

2020 Activity Report

29th Activity Report



BfDI

Federal Commissioner
for Data Protection and
Freedom of Information



29

Table of Contents

1. Introduction

2. Recommendations

- 2.1 Summary of recommendations for the 29th Activity Report
- 2.2 Recommendations made the 28th Data Protection Activity Report and the 7th Freedom of Information Activity Report—implementation status
- 2.3 Key recommendations from previous activity reports—implementation status

3. Committee

- 3.1 Conference of Independent Federal and State Data Protection Supervisory Authorities (Data Protection Conference)
 - 3.1.1 Resolution on the Patient Data Protection Act (Patientendaten-Schutz-Gesetz, PDSG)
 - 3.1.2 Implementing constitutionally compliant register modernisation
 - 3.1.3 Data sovereignty
 - 3.1.4 Video surveillance guidance
 - 3.1.5 Requirements for secure e-mail communication
 - 3.1.6 DSK 2.0 initiative
- 3.2 European Data Protection Board
 - 3.2.1 Report from the Key Provisions Expert Subgroup
 - 3.2.2 Evaluation of the GDPR: the first round is complete
 - 3.2.3 Face recognition – benefits and limitations
 - 3.2.4 Approval and publication of the (German) accreditation criteria for monitoring bodies pursuant to Article 41 of the GDPR

4. Main topics

- 4.1 Coronavirus
 - 4.1.1 The Federal Government's Corona-Warn-App
 - 4.1.2 The data donation app
 - 4.1.3 Coronavirus measures and projects
 - 4.1.4 Amendments to the Infection Protection Act
 - 4.1.5 Protective mask only against data?
 - 4.1.6 Messenger and video conferencing systems — a blessing and a curse in coronavirus times
 - 4.1.7 Delivery of parcels under pandemic conditions
 - 4.1.8 Federal emergency or bridging assistance programmes in connection with the coronavirus pandemic
 - 4.1.9 Corona-related changes in employment services

4.2 The Patient Data Protection Act

4.3 Implementation of the Schrems II Judgment of the European Court of Justice

5. Legislation

5.1 Register modernisation

5.2 Administrative digitalisation is progressing

5.3 IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0)

5.4 Amendment of the Federal Intelligence Service Act

5.5 Legislative procedure for amending the law on the protection of the constitution

5.6 The regulation on ‘apps on prescription’

5.7 Data Transparency Regulation (Datentransparenzverordnung)

5.8 The basic pension is coming—but will it be compliant with data protection law?

5.9 The Digital Family Benefits Act (Digitale Familienleistungen-Gesetz)

5.10 Current legislation and other regulations in the telecommunications sector

6. Security

6.1 Police 2020

6.2 Uniform case processing system

6.3 The ruling of the Federal Constitutional Court on strategic foreign telecommunications reconnaissance

6.4 The Haber procedure

6.5 Security screening of applicants to intelligence services

6.6 Passenger name records—how much data collection is justified to fight terrorism?

6.7 PCJA Directive still not fully implemented

6.8 Redesign of the FIU 2.0 information network

6.9 Data protection breach in the area of customs investigation

6.10 Employee data protection in the Customs Administration

6.11 Data protection breaches at the Federal Police

6.12 Protected border-crossing records

7. Other individual topics

7.1 Data protection supervision in the parliamentary area

7.2 Interdisciplinary Advisory Board for Employee Data Protection

7.3 Registers in the healthcare sector

7.4 Improve, but please do it right—the second decision of the Federal Constitutional Court on providing information about inventory data

7.5 Anonymisation—positioning between the GDPR and the TKG

7.6 Unencrypted tax data

- 7.7 Federal IT consolidation
- 7.8 Microsoft, data protection and digital sovereignty
- 7.9 Artificial intelligence—progress
- 7.10 Certification and accreditation—initial procedures start
- 7.11 Video identification procedure—current fundamental decision of the BfDI with a spill over effect for many areas
- 7.12 Impact of Brexit
- 7.13 New developments in research with health data
- 7.14 Rectification of diagnostic data
- 7.15 Sickness benefit case management—no consensus on the scope of the health insurance providers' data collection powers
- 7.16 Division of responsibilities in the telecommunications sector
- 7.17 Cyber attacks on the Institute for Federal Real Estate (Bundesanstalt für Immobilienaufgaben)

8. Freedom of Information Act (Informationsfreiheitsgesetz)

- 8.1 Individual topics
 - 8.1.1 Freedom of information in the pandemic
 - 8.1.2 What is actually a trade secret?
 - 8.1.3 Access to records detailing processing activities
 - 8.1.4 Federal Freedom of Information Act does not apply to the Association of German Cities (Deutscher Städtetag)
- 8.2 Case law
 - 8.2.1 Dispute over the publication of an opinion on glyphosate: justified protection of intellectual property or censorship?
 - 8.2.2 What applies? The Political Parties Act or the Freedom of Information Act?
 - 8.2.3 Social media and freedom of information
- 8.3 Statistics on freedom of information

9. Controls and effects

- 9.1 Questionnaire checks for authentication at call centres
- 9.2 Hand scanner questionnaire check
- 9.3 Change of official Data Protection Officer in the Federal Ministry of Defence
- 9.4 Advisory and inspection visits on the application of the Freedom of Information Act
- 9.5 Controls in the security sector
 - 9.5.1 Checks and complaints in the area of the Federal Office for the Protection of the Constitution
 - 9.5.2 Anti-terror file checks
 - 9.5.3 The case processing system at the Federal Criminal Police Office
 - 9.5.4 International BKA data transfers
 - 9.5.5 General contribution on Security Clearance Act checks carried out

10. Internal developments within the BfDI

10.1 Courses for action by the BfDI if legislation is contrary to European law

10.2 Ruling of Bonn Regional Court confirms the BfDI's legal opinion

10.3 Staffing developments in 2020

10.4 New premises

10.5 Press and public relations

10.6 The BfDI's work in figures

11. BfDI as the single point of contact (SPOC)

11.1 Strengthening the One-Stop-Shop

11.2 Statistical insight into the work of the SPOC as part of the cooperation and coherence procedures at a European level

1 Introduction

2020 - what a year! Coronavirus and the impact of coronavirus crossed over into all areas of life, set the political agenda as well as the economic one, put us into two unprecedented lockdowns and introduced us to endless video conferences. Some fundamental rights, including data protection, have been restricted to help fight the pandemic.

Social distancing, less contact points, working from home, home schooling the kids or keeping them otherwise occupied while still managing to do 'normal' work—all of these demands were placed on many employees and were put into practice in 2020. The home office became the norm in my department too, and thanks to almost all desktop PCs being replaced with laptops—something that happened in 2019—and authorities switching to e-files, we were able to continue our work almost without restriction, apart from on-site inspections.

This was also urgently required, because the Federal Government further increased its number of bills, which was already high last year. In the healthcare sector in particular, three pandemic control laws were introduced in addition to the 'Patient Data Protection Act' (Patientendaten-Schutz-Gesetz, PDSG), which already required a great deal of consultation, and in some cases left hardly any time for review and consultation.

In particular, the PDSG regulates the long-planned electronic health record (EHR) and the introduction of electronic prescriptions. Despite long and intensive consultations with the Federal Ministry of Health, it has unfortunately not been possible to design the EHR for all persons covered by statutory health insurance in such a way that it both brings the health benefits and meets the requirements of the General Data Protection Regulation (GDPR) from day one (see 4.2). It is precisely because the EHR will contain a lot of particularly sensitive patient data that protecting this data is especially important. I must insist on further improvements here in line with the GDPR.

The monitoring of the Register Modernisation Act (Registermodernisierungsgesetz, RegMoG), which was introduced into the Bundestag at the end of 2020, was similarly consultation-intensive and ultimately unsatisfactory. The law provides for the tax identification number to be used in future as a personal identifier for more than 50 databases and registers of the federal and state governments. In terms of data protection law, more sensible alternatives that also fully guarantee functionality, such as area-specific personal identification numbers, were only insufficiently reviewed or not reviewed at all. It is precisely because the Federal Constitutional Court (Bundesverfassungsgericht) has repeatedly declared that the introduction of personal characteristics are unconstitutional in recent years that I expect current plans will not be able to withstand a constitutional appeal. The project of reducing bureaucracy for citizens and administration, which is worthy of support, thus runs the risk of being postponed further into the future (see 5.1 and 5.2).

The effects of the ruling of the European Court of Justice (ECJ) on international data traffic from July 2020 cannot be postponed. With its 'Schrems II' Judgment, the court not only declared the regulations of the 'Privacy Shield' invalid—it also clarified once again that, in principle, there must be a level of data protection equivalent to that of the EU for data transfers to third countries. In this respect, standard data protection clauses, for example, must be supplemented by 'additional measures' if, for example, security agencies in the recipient country are able to gain extensive access to the data transferred (see 4.3). To assist data controllers affected by the immediate effect of the Judgment, the European Data Protection Board is providing immediate initial guidance and assistance. However, due to the gravity and scope of the effects of the ruling, its consequences are sure to keep us busy for years to come.

One issue I hope we don't have to deal with for years to come is the Corona-Warn-App (CWA). Partially because everyone hopes we can tackle coronavirus as quickly as possible, and partially because the work invested in

this project in 2020 always had to be done under great time pressure. I am therefore also pleased that the CWA can serve as a positive example of how the consistent involvement of a data protection supervisory authority throughout the development process has made it possible to launch an outstanding product in terms of data protection law (see 4.1.1). Not least because of its data protection-friendly design, the CWA has met with a high level of acceptance among the population and had already been downloaded more than 24 million times by the end of 2020.

And that is exactly why I'm surprised and irritated by the current discussion about the app's alleged lack of functionality. In particular, the claims made by many parties that strict data protection requirements would prevent any meaningful further development of the CWA are simply wrong and are often based on a lack of understanding of how the app works and its technical possibilities. The fact is that none of the suitable and technically feasible proposals brought into the discussion to date have failed because of data protection. I would therefore like to see a more differentiated and, above all, more informed debate here that supports useful and effective further development. Even if the CWA cannot be the sole solution, it offers excellent conditions for stopping chains of infection more quickly and thus making a significant contribution to combating the pandemic.

Beyond coronavirus, the BfDI was also involved in many topics in 2020, the effects of which don't just cover very specific areas and legal issues, such as the amendment of the Federal Intelligence Service Act (Bundesnachrichtendienstgesetz; see 5.4), the Bundestag's necessary data protection regulations (see 6.1) or developments in the field of artificial intelligence (see 6.9). A whole series of issues also related to topics that can have a direct noticeable impact on individual citizens, such as procedures for sickness benefit management (see 6.14), the unencrypted sending of sensitive data by e-mail (see 6.6) and requirements for the data protection-compliant implementation of private video surveillance (see 3.1.4).

Another important area of my work is shown in this report for the first time together with data protection—freedom of information. Coronavirus also impacted my work here—the modalities and costs of repatriating German citizens during the first lockdown were the subject of numerous queries. Many people sent questions about pandemic management to the Robert Koch Institute or the Federal Ministry of Health, where I had been asked to mediate.

Finally, this year's activity report once again impressively demonstrates that data protection and freedom of information are cross-cutting issues that are of greater

or lesser importance in almost all areas of life. Most importantly, it shows that the work to assist citizens in safeguarding and enforcing their fundamental right to informational self-determination continues to grow. Fortunately, the increase in the number of jobs over the past three years has made it possible, among other things, to further intensify the provision of advice and information to the bodies I supervise. This meant that I was able to implement the 'raise awareness, advise, monitor' work assignments set out in the GDPR and the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) better than ever before. And as such, in addition to the positive examples mentioned in the activity report, where advice has led to data protection-friendly solutions and the solid implementation of the right to freedom of information, there are many other cases where our recommendations have been followed up and implemented by companies and public authorities.

I do not do this work alone, and instead am able to rely on a strong, motivated and committed team of 251 employees—as of the end of 2020. I would like to take this opportunity to express my sincere appreciation for the (extra) work they have done and to thank them for their great cooperation, even and especially under the more difficult conditions this year.

Prof. Ulrich Kelber

2

Recommendations

2.1 Summary of recommendations for the 29th Activity Report

I also recommend that the bodies under my oversight involve me early on in time-critical projects. This means that data protection and thus also the protection of data subjects' rights can be adequately taken into account from the outset. (Nos. 4.1.4, 4.1.8, 4.1.9)

I recommend that the Federal Council (Bundesrat, BR) elect a deputy for the joint representative pursuant to Section 17 (1) of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). (No. 11.1)

I recommend that the modernisation of the register should be based on several area-specific identifiers instead of a single personal identification number. At the very least, the 4-corner model should be used for each data transmission and a strict purpose limitation for the use of the ID number should be established. The data cockpit should be further developed into a real inventory data information system in the near future. (No. 5.1)

I recommend that the bodies under my oversight carefully review their data transfers to third countries in light of the requirements of the ECJ's Schrems II Judgment and make any necessary adjustments. (No. 4.3)









I recommend that the laws, projects and measures that were developed and implemented under high pressure and within short deadlines during the coronavirus pandemic are deliberately and carefully reviewed once the pandemic is over. (Nos. 4.1.3, 4.1.4)







I recommend that 'digital health applications' are transmitted to users in the secure telematics infrastructure or on machine-readable data storage devices. In addition, an app store should be newly created for the provision of 'digital health applications' in the telematics infrastructure and operated by silent stakeholders in the healthcare system. (No. 5.6)

I recommend clarifying that the exercise of data protection rights should not lead to the sentence being aggravated in disciplinary proceedings. (No. 6.10)




I recommend that European data protection law be implemented immediately and in full. This should not be used as an excuse to introduce controversial regulations with new powers of intervention for security agencies. (No. 6.7)

2.2 Recommendations made the 28th Data Protection Activity Report and the 7th Freedom of Information Activity Report—implementation status

	Recommendation	Implementation status
	I recommend that the seven data protection requirements of the 'Hambach Declaration on Artificial Intelligence' should be observed in the diverse implementation of AI. (No. 3.1 of the 28th AR)	AI is evolving rapidly. It is good that the (public) discourse around the legal, economic and social implications of AI is in full swing. Data protection is an important success factor here. I will continue to follow developments in this area closely and continue to advocate for privacy-compliant AI that serves people.
	I recommend supporting the position of national data protection supervisory authorities as well as the European Data Protection Board (EDPB) in the evaluation of the GDPR. This applies in particular to meaningful relief for small and medium-sized enterprises with respect to the bureaucratic procedural effort to be made and the demand for a tightening of the current legal framework for profiling. (No. 4.1 of the 28th AR)	The Commission's Evaluation Report is available (COMMUNICATION FROM THE COMMISSION COM(2020) 264 final). The Federal Government played an active role in council during the evaluation process. As a result, the COM did not consider direct measures to amend the GDPR.
	I recommend implementing differentiated role and rights management for the electronic health record from the very beginning. (No. 4.2.1 of the 28th AR)	It is true that the Patient Data Protection Act with its numerous regulations on the telematics infrastructure and the electronic health record (EHR) has come into force. However, the EHR will launch on 01/01/2021 without the possibility of document-specific access control. Only from 01/01/2022 onwards will 'front-end users' be able to control document-specific access authorisations; all other insured persons will only be able to permanently control access authorisations via document categories.
	Instead of transferring registers to the Federal Institute for Drugs and Medical Devices, I recommend creating an independent register authority in the healthcare sector. (No. 4.2.2 of the 28th AR)	This recommendation has not yet been followed up.
	I recommend that the proposals of the Data Ethics Committee should be enshrined in law. (No. 4.6)	As far as can be seen, no steps have been taken to implement this so far. An initial attempt to introduce a personal information management system (PIMS) in the draft of the Telecommunications-Telemedia-Data Protection Act was withdrawn at the outset.
	I recommend adapting the Telecommunications Act (Telekommunikationsgesetz, TKG) and the Telemedia Act (Telemediengesetz, TMG) to the GDPR. (No. 5.2 of the 28th AR)	At the end of 2020, the Federal Government submitted a bill to modernise telecommunications and telemedia law.
	I recommend declaring a security law moratorium and launching an evaluation process for the powers of intervention granted to security agencies in order to identify potential deficiencies in enforcement. (No. 5.3 of the 28th AR)	This recommendation has not yet been followed up.
	I recommend that the modernisation of the register should be based on several area-specific identifiers instead of a single personal identification number. (No. 5.5 of the 28th AR)	My concerns were largely not taken into account in the legislative process which is still ongoing. The recommendation will therefore also be updated and set out in detail in a new recommendation (see above).

	Recommendation	Implementation status
	I recommend that video surveillance systems based on biometric facial recognition should not be used in public spaces. (No. 6.2 of the 28th AR)	So far, a corresponding provision has not been included in the Federal Police Act (Bundespolizeigesetz, BPolG).
	I recommend that an explicit and comprehensive legal basis should be created for the 'Haber procedure'. (No. 6.5 of the 28th AR)	This recommendation has not yet been followed up.
	I recommend that, with respect to services under the Online Access Act (Onlinezugangsgesetz), citizens should be given a user-friendly option to track and control the data processing processes that take place. (No. 8.2 of the 28th AR)	The draft of the Register Modernisation Act provides for a data cockpit, which envisages transparency with respect to transfers between the registers covered by the RegMoG. I am also committed to expanding the data cockpit into a true inventory data information system.
	I recommend that the bodies under my oversight should only send personal data by e-mail in encrypted form as a matter of principle. (No. 8.3 of the 28th AR)	Unfortunately, there is still far too little use of encrypted e-mail communication. In particular, my criticism of a tax code provision on this matter did not result in any improvement.
	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. (No. 8.7 of the 28th AR)	This recommendation has not yet been followed up.
	<p>I recommend that the legislator further develop the Freedom of Information Act (Informationsfreiheitsgesetz) in the direction of a transparency law.</p> <p>a) This transparency law should impose a much stronger and more extensive obligation on authorities to make proactive disclosures.</p> <p>b) A transparency law should also oblige the Federal Government to set up and operate a central federal portal for the bundled proactive provision of information. Here, previously unpublished information should be made available to everyone, and suitable information should be made available to individual interested parties on request (the 'access for one—access for all' principle).</p> <p>c) The portal should also make electronic applications and decision-making straightforward. This should make it easier to find information whilst at the same time reducing administrative.</p>	<p>The federal legislator has not yet followed up on my recommendation to develop the Freedom of Information Act into a transparency law.</p> <p>However, there are initiatives in the area of open data: in December 2020, the Federal Ministry of the Interior, Building and Community and the Federal Ministry of Economics and Technology submitted the draft bill for the Second Open Data Act (Zweites Open-Data-Gesetz) and the Data Use Act (Datennutzungsgesetz).¹</p> <p>Firstly, the bill is intended to extend the Federal Government's open data regulation (Section 12a of the E-Government Act [E-Government-Gesetz]). More public administrative data should be made discoverable via the central access point GovData and metadata should be stored there.</p> <p>Secondly, the Data Use Act is intended to transpose Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information into national law. The further legislative process remains to be seen.</p>









¹ Draft Act amending the E-Government Act and introducing the Public Sector Data Utilisation Act (Gesetz für die Nutzung von Daten des öffentlichen Sektors), source: <https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/referentenentwurf-zweites-open-data-gesetz-und-datennutzungsgesetz.pdf>






	Recommendation	Implementation status
	I recommend that the legislator expand my role as the Federal Freedom of Information Commissioner.	My ordering and sanctioning powers under freedom of information law have not yet been extended in line with my data protection powers.
	<p>a) In this context, it should be possible for me to issue binding orders and further sanctions analogous to my powers under data protection law. This would mean that applicants would no longer have to rely solely on the path of judicial legal protection, which is often time-consuming and cost-intensive.</p> <p>b) Like my predecessors, I recommend to the legislator that my duties and powers are extended, particularly with respect to environmental and consumer information law. In this way, I would be able to meet the undisputed need for advice and support for both applicants and the authorities.</p>	<p>A corresponding legislative procedure has been initiated.</p> <p>In the meantime, the Federal Government's draft bill 'Draft Act amending the Environmental Damage Act, the Environmental Information Act and other environmental regulations' ('Entwurf eines Gesetzes zur Änderung des Umweltschadensgesetzes, des Umweltinformationsgesetzes und weiterer umweltrechtlicher Vorschriften') dated 11/11/2020 is available¹:</p> <p>In December 2020, the Environment Agency (Umweltbundesamt) published the study 'Evaluation of the Environmental Information Act (Umweltinformationsgesetz, UIG) - Analysis of the Application of the Regulations of the UIG and Development of Optimisation Potential for Unhindered and Easy Access to Environmental Information' ('Evaluation des Umweltinformationsgesetzes (UIG) - Analyse der Anwendung der Regelungen des UIG und Erschließung von Optimierungspotentialen für einen ungehinderten und einfachen Zugang zu Umweltinformationen')². It can be inferred from the expert opinion that there was a recommendation to extend the ombudsman and supervisory competences of the BfDI to the UIG (see p. 159 f. of the study) and the supervisory tasks to the BfDI (see p. 167).</p>
	I recommend that the legislator should critically examine the exemptions in the Freedom of Information Act for redundancy and continued need.	Due diligence is still pending.







¹ Source: BT printed matter 19/24230: <https://www.bmu.de/gesetz/entwurf-eines-gesetzes-zur-aenderung-des-umweltschadensgesetzes-des-umweltinformationsgesetzes-und-w/>

² Source: <https://www.umweltbundesamt.de/publikationen/evaluation-des-umweltinformationsgesetzes-uig>

2.3 Key recommendations from previous activity reports—implementation status

	Recommendation	Implementation status
	I recommend that the legislator should include remedial powers for the BfDI in the new Federal Police Act (Bundespolizeigesetz, BPolG). These should at least correspond to the powers already contained in the new Federal Criminal Police Office Act (Bundeskriminalamtgesetz, BKAG). (No. 1.2 in the 27th AR)	The draft for a new BPolG that I have before me provides for remedial powers for the BfDI. However, the requirements are more stringent than those provided for in the Directive. For example, an order should only be possible after a complaint has been made. It also lacks the explicit option to issue an erasure order. As such, this increases the risk that effective remedial action will be possible.
	I recommend that the legislator should also introduce sanctioning powers for the BfDI in the area of intelligence services. (No. 1.2.1 in the 27th AR).	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I recommend that the legislator should clarify that fines for GDPR breaches can also be imposed on statutory health insurance providers if they act as commercial enterprises. (No. 1.1 in the 27th AR)	The legislator rejects this. We therefore see cases where data protection breaches have been deliberately committed in order to achieve an economic advantage.
	I recommend that staffing levels within job centres should be increased to the point that they can free up their data protection officers, ensuring that they can comply with their legal requirements. (No. 3.2.1 in the 27th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I recommend that the Federal Government should revise the Passenger Data Act (Fluggastdatengesetz, FlugDaG) in light of the ECJ's requirements on the EU-Canada PNR agreement and advocate for a revision of Directive (EU) 2016/681 in Brussels. (No. 1.3 in the 27th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	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 also recommend that the BfDI's supervisory authority should be comprehensively recognised, including when the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) maintains shared files with foreign intelligence services, and this should be clarified by law if necessary. (No. 9.1.5 in the 27th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I recommend that the newly developed standard contract for commissioned processing should be used throughout the federal administration for contracts for commissioned processing. The standard agreement is published on my website. (No. 9.2.6 in the 27th AR)	Fortunately, the standard contract is increasingly being used on a larger scale.
	I recommend that police authorities should have access to meaningful documentation when accessing Eurodac and the Visa Information System (VIS). (No. 9.3.5 in the 27th AR)	Measures to optimise documentation have been promised by the responsible bodies and these measures seem likely to result in improvements. However, my follow-up checks have still revealed deficiencies in this area, which need to be improved by the responsible bodies. I will continue to critically monitor the implementation of the documentation improvement.

	Recommendation	Implementation status
	In view of their limited practical value, I recommend that the legislator should abolish the anti-terrorism file (Anti-Terror-Datei, ATD) and the right-wing extremism file (Rechtsextremismus-Datei, RED). (No. 9.3.5 in the 27th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I recommend that the Code of Criminal Procedure (Strafprozessordnung, StPO) should be revised. In particular, the collection and use of data that has been gathered by informants for police-related or intelligence-related purposes should be regulated in such a way as to create legal clarity during criminal proceedings. Cooperation with the authorities ensuring the protection of the Constitution should in any case be regulated more stringently and in greater detail. The case law of the Federal Constitutional Court must be implemented in this respect. (No. 11.1.2 in the 27th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I strongly advise that the e-Privacy Regulation should be adopted as soon as possible. The current application of national rules adopted on the basis of Directive 2002/58/EC no longer adequately reflects current developments and creates legal uncertainty for all parties concerned. This particularly applies to the relationship between the German Telecommunications Act (Telekommunikationsgesetz, TKG) and the GDPR. (No. 15.1.2 in the 27th AR)	In the EU Council, no progress could be made under Germany's Presidency of the Council either, and thus still no general approach could be found.
	I advise federal public authorities to critically question the need to use social media. Important information should not be provided exclusively through social media. Sensitive personal data should not be posted on social media—public authorities should not post such data themselves, nor should they encourage citizens to do so. For confidential communication, there are appropriate more secure communication channels that should be referenced, such as SSL-encrypted forms, encrypted e-mails or De-Mail. (No. 15.2.7 in the 27th AR)	No improvements were observed in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I recommend that federal agencies that operate a Facebook fan page should consider whether doing so is absolutely necessary for the performance of their duties or whether they cannot choose to use more privacy-friendly communication channels—at least until the situation has been clarified by law. (No. 15.2.8 in the 27th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.

	Recommendation	Implementation status
	I recommend to the legislators at federal and state level that they should embrace the spirit and letter of the new European data protection rules when adapting national data protection law in order to ensure the largely uniform application of future European data protection. (No. 1.1, 1.2 in the 27th AR)	The legislator largely implemented the regulatory mandates and scope from the GDPR through the Data Protection Amendment and Implementation Act (Datenschutz-Anpassungs- und Umsetzungsgesetz) and the Second Data Protection Amendment and Implementation Act (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz). The legislator partially complied with my recommendations in both acts. However, I continue to be critical of some regulations, such as the restriction of supervisory powers for persons subject to professional secrecy, the regulations on video surveillance, some of which are contrary to European law, or restrictions on data subject rights that are too far-reaching in certain areas. The upcoming evaluation of the BDSG should focus on these points.
	For the future, I recommend that the German Bundestag should draw up its own data protection regulations in compliance with GDPR requirements. (No. 14.1.1 in the 27th AR)	The Bundestag is currently considering the creation of its own data protection regulations.
	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. (No. 3.1, 3.2.1 in the 26th AR)	In summer 2020, the Federal Ministry of Labour and Social Affairs (Bundesministerium für Arbeit und Soziales, BMAS) convened the interdisciplinary Advisory Board on Employee Data Protection. The advisory board's work is still ongoing. The advisory board's recommendations are expected in the first half of 2021. The advisory board's work was the first step towards employee data protection law.
	I recommend to the legislator that the legal bases for the powers of intervention of security agencies and intelligence services should be drafted in line with the requirements of the Federal Constitutional Court on the BKAG in a constitutional way, i.e. that the relevant regulations should also be amended accordingly. (No. 1.3 in the 26th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I recommend that the legislator should create legal provisions for the implementation of mortality registries for research purposes. (No. 9.2.3 in the 26th AR)	No changes were identified in the current reporting period. For the current status, please refer to the comments made in the last AR.
	I recommend that the legislator should create clear guidelines in the area of IT systems to make these systems as secure and resilient as possible, while ensuring the highest possible level of protection for personal data. (No. 10.2.11.1 in the 26th AR)	The ITSecurity Act 2.0 was adopted by the cabinet on 16/12/2020 and is now under discussion in the Bundestag. Care must also be taken to ensure that data protection concerns are given the best possible consideration in the further legislative process too.

3

Committee

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

The Data Protection Conference (Datenschutzkonferenz, DSK) is tasked with protecting fundamental data protection rights, achieving uniform application of European and national data protection law and jointly advocating for its further development. In 2020, chairmanship, which rotates on an annual basis, was held by the Saxon State Data Protection Commissioner Andreas Schurig.

Due to coronavirus, all of the DSK's preliminary, intermediate and main conferences took place as video conferences. Nine resolutions on current legislative projects and six resolutions, e.g. on the use of Google Analytics, were adopted. In addition, current guidance, for example on video conferencing systems, as well as application notes on accreditation and on the standard data protection model, were developed.

3.1.1 Resolution on the Patient Data Protection Act (Patientendaten-Schutz-Gesetz, PDSG)

The Conference of Independent Federal and State Data Protection Supervisory Authorities (Data Protection Conference) has dealt with the Patient Data Protection Act (Patientendaten-Schutz-Gesetz, PDSG) several times, which accelerates digitalisation in the healthcare sector. As a result of its deliberations, the DSK has published a resolution (see 4.2).

Although monitoring the legislative process for the PDSG as a federal law falls within my sole area of responsibility, it was necessary to develop a uniform data protection law opinion on the PDSG with the state data protection commissioners. This is because the PDSG contains requirements for all statutory health insurance providers, i.e. for both the health insurance providers under my supervision and those under the supervision of the state commissioners. The joint positioning took

place at the working level in the EHC sub-working group of the 'Health and Social Affairs' working group as well as through coordination at the level of heads of authorities. I presented the results of this work at a federal press conference, which was also attended by three state commissioners. As things progressed, the DSK passed a resolution on the PDSG, in which the regulations of the bill that are problematic in terms of data protection were addressed and solutions pointed out. This was intended to bring about necessary improvements to the PDSG in terms of data protection law before the last round of consultations in the Federal Council, unfortunately without success. Therefore, in order to fulfil their supervisory obligation after the PDSG enters into force, the data protection supervisory authorities must consider imposing supervisory measures on data controllers to maintain or restore data protection compliance.

Cross-reference: 4.2 Patient Data Protection Act

3.1.2 Implementing constitutionally compliant register modernisation

The DSK has clearly spoken out against the misappropriation of the tax ID to a personal identification number.

In the resolution 'Implementing constitutionally compliant register modernisation!' of 26 August 2020, the DSK clearly positioned itself against the Federal Government's plan to expand the tax ID to a cross-register classification feature (personal identifier). In doing so, the DSK referred to its previous resolution on this subject dated 12 September 2019.

The DSK refers to the always extremely critical assessment of the Federal Constitutional Court towards the introduction of such personal identifiers. Like the highest German court, the DSK also sees the risk of abuse as a threat to fundamental rights. The draft of the Register Modernisation Act does not sufficiently compensate for this. The possibility of combining data to form a personality profile is not effectively prevented and it can

be expected that the tax ID will gradually be used as an identification number in business life as well.

The DSK criticises that much more data protection-friendly alternatives, such as 'sector-specific' personal identifiers, are not taken into account. These procedures are suitable in practice, but are apparently not being adopted to due (relatively minor) economic considerations and because of a self-imposed need for urgency.

The resolution of 28 August 2020 can be found at www.bfdi.bund.de/entschließungen

Cross-reference: 5.1 Register modernisation

3.1.3 Data sovereignty

Data sovereignty has been established as a guiding concept for digital policy. It shapes debates on future data strategy at a European and national level. But the use of the term often remains vague. It is not a suitable alternative concept to the constitutional right to informational self-determination. Nor should it be established as a fighting term against the existing legal concept of data protection. A DSK resolution defines what should be understood by this in terms of data protection and formulates concrete demands.

The term 'data sovereignty' initially gained importance in connection with the ideas of 'data ownership' which emerged shortly after the adoption of the General Data Protection Regulation (see the 27th AR, 1.5., p. 34). It is not a legal term—it comes from political debate. It is now frequently used in discussions on European and national data strategies. The Federal Government's key issues paper for a data strategy views 'digital sovereignty' as being secured through the guarantee of improved access to data. Data sovereignty thus refers more to an economic policy geared towards securing the autonomy and independence of institutions and European digitalisation. The Gaia-X project, which was initiated by the Federal Government and is geared towards a European cloud infrastructure, is cited as one example in particular. In this context, the Federal Ministry of the Interior, Building and Community is also planning a Centre for Digital Sovereignty (Zentrum Digitale Souveränität, ZenDis), which will focus on the topic of open source software in public administration.

This institutional understanding, which is geared towards protection against unilateral dependencies, also finds support in terms of data protection policy. Thus, in a resolution of September 2020, the Data Protection Conference commits itself to freedom of choice and full control by public administration controllers over the means and procedures used in digital processing. The federal, state and municipal governments are called upon to only use hardware and software in the long term

that leaves exclusive and complete control to controllers responsible for data processing, guarantees transparency of security functions and allows use without profiling and misuse by third parties. Digital sovereignty objectives and criteria would already have to be taken into account in all procurement and award procedures in the short term. Preference should be given to open source products, and services and products should be selected with a view to privacy by design, privacy-friendly default settings and individual configurability.

However, the term is still used in the debate on individual consumer rights. Some lobbyists are more interested in replacing the immaterial right to informational self-determination with the economic autonomy of the individual with buzzwords such as 'data donation' and 'data as payment'. The underlying, property-analogous understanding of data and the supposedly indivisible dominion over data concerning oneself is misguided. Because economically, it is more about the exploitation of information than about data, and often even about the exploitation of communications concerning several persons and the targeted acquisition of knowledge about individual persons or groups of persons. Here, it is more true than ever that such intangible goods need special protection and that maximum privacy protection can only be achieved with a differentiated data protection concept. A general change in data protection towards data sovereignty, which some even advocate for, is therefore neither to be expected, nor would it be appropriate in view of the necessary protection of citizens' rights in digitalisation.

3.1.4 Video surveillance guidance

The Data Protection Conference (Datenschutzkonferenz, DSK) presents guidance on issues relating to private video surveillance.

On 3 September 2020, the DSK presented guidance on video surveillance by non-public bodies. This guidance is largely based on the Guidelines 3/2019 of the European Data Protection Board (EDPB) on data processing using video equipment (see no. 3.2 of the 28th AR) and supplements them with specific processing situations in Germany. This includes sections on neighbourhood CCTV, the data protection assessment of door and bell cameras, drones, wildlife cameras and dashcams.

The guidance also comprehensively presents basic data protection considerations relating to video surveillance, as well as some practical guidance. As an example, the appendix contains a sample of information signs and a checklist for the most important points to be checked prior to carrying out video surveillance.v

The guidance can be found on my website at www.bfdi.bund.de/orientierungshilfen, under 'Guidance on video surveillance by non-public bodies' dated 04/09/2020.

3.1.5 Requirements for secure e-mail communication

Unfortunately, confidential end-to-end communication via e-mail is still not widely accepted because it is still not easy to manage. It is therefore all the more important to encrypt e-mails at least at a transport-level for service providers, therefore protecting them from being viewed or manipulated by third parties at transport stages. In this respect, the guidance issued by the DSK in 2020 contains corresponding provisions on communication with service providers.

The guidance indicates the requirements applicable for sending and receiving e-mail messages by controllers, their processors and public e-mail service providers in transit. Risks to which dormant data such as e-mails already received are exposed or which arise from further processing such as automatic forwarding are not taken into consideration. These requirements are based on the provisions of Articles 5(1) (f), 25 and 32(1) of the GDPR. The guidance is state of the art at the time of publication as a basis for specifying requirements. The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has also addressed the issue of encrypted e-mail communication at the transport level in a new technical guideline and has issued specifications (BSI TR-03108 Secure E-Mail Transport https://www.bsi.bund.de/DE/Publikationen/Technische-Richtlinien/tr03108/tr03108_node.html)

The guidance was created at my suggestion. The basic idea was to arrive at a uniform view of encryption at a transport level in order to provide companies in the telecommunications industry with corresponding uniform specifications. The guidance now reflects a coordinated body of opinion among the states and the Federal Government on email encryption and sets a benchmark for confidential communications at the transportation level. It can be downloaded at www.bfdi.bund.de/orientierungshilfen.

3.1.6 DSK 2.0 initiative

The DSK has decided to set up a 'DSK 2.0 Working Group' at management level, which is to evaluate the cooperation between independent federal and state data protection supervisory authorities, including the DSK's working methods, and, if necessary, to draw up proposals for a reorganisation.

Within the context of the political debate surrounding the centralisation of data protection supervision and due to constantly new questions when it comes to data protection law with ever faster developing technology, the DSK 2.0 working group is to review the DSK's current

working methods and the cooperation between the supervisory authorities. It is intended to identify potential improvements so that cooperation can continue to be successful and self-determined.

Citizens, companies and associations rightly expect that, even under the federal structure of data protection supervision in Germany, comparable matters are treated equally and that procedures are designed to be efficient and transparent.

I therefore advocate within the framework of the DSK 2.0 working group that

- faster and more efficient decision-making processes are established for the DSK;
- DSK resolutions become more binding;
- supervisory practice is further harmonised; and
- liaison between the working parties of the DSK and the working parties of the European Data Protection Board is optimised.

It is expected that this work will be completed by the 101st Data Protection Conference in spring 2021.

3.2 European Data Protection Board

In the reporting period, the European Data Protection Board (EDPB) further intensified its work on the uniform application of the General Data Protection Regulation (GDPR) throughout Europe. Guidelines were adopted and opinions issued in this regard. Cross-border cooperation has also been further strengthened.

The EDPB is an independent European body that contributes to the consistent application of data protection rules across the EU and promotes cooperation between EU data protection authorities. I have already explained these tasks in more detail in my two previous activity reports. As the joint representative of all German supervisory authorities, I am a member of the Board.

The EDPB's work was dominated by the impact of the COVID-19 pandemic after the first two meetings in January and February. All other meetings took place in the form of video conferences as remote meetings. In the process, the EDPB significantly increased the total number of meetings and held a total of 27 conferences, some of which lasted two days.

The focus of the work continued to be on the development of guidelines pursuant to Article 70 GDPR for the uniform implementation of the GDPR in Europe. In addition, the Board also adopted opinions in the consis-

tency mechanism under Article 64 GDPR and took a first formal decision in the dispute resolution procedure on a cross-border complaint procedure (consistency mechanism). It also dealt with current data protection policy issues at international and EU level, including data processing in the aftermath of the COVID-19 pandemic.

In terms of content, the EDPB's work in the second half of the year was significantly influenced by the outcome of the Schrems II Judgment (ECJ, Judgment of 16 July 2020, Case C-311/18). This Judgment has reshaped the requirements for data transfers to third countries (see 4.3)¹.

This was followed by elaborations on various details of the data transfer. For example, the **recommendations on the use of supplementary measures**² provide a roadmap of the steps data exporters need to take to determine whether they need to take additional measures. This is a prerequisite for being allowed to transfer data outside the EEA in accordance with EU law.

The EDPB has also adopted a strategy for 2021 to 2023.

Guidelines

In the reporting period, the EDPB adopted numerous guidelines, which I regularly contributed to the drafting of as a rapporteur or co-rapporteur. Some of these have been subject to public consultation to ensure transparency and participation.

- As an example, '**Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications**' clarify the relationship with the envisaged e-privacy regulation and issues related to the processing of personal data for new purposes.
- **Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies** deal with international data transfers between public bodies for various administrative cooperation purposes under the GDPR. However, the guidelines do not apply to transfers in the field of public security, defence or state security.
- **Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak** aim to shed more light on the most pressing issues in this context, including the legal basis, the establishment of appropriate safeguards for such processing

of health data and the exercise of data subjects' rights (see also 6.13).

- **Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak** clarify the conditions and principles for the proportionate use of location data and contact tracking tools for two specific applications: these apply to the use of location data to support the response to the pandemic by modelling the spread of the virus so that the overall effectiveness of containment measures can be assessed. They are also used for contact tracing to inform individuals that they have been in close proximity to a person who has subsequently been confirmed as a carrier of the virus. The aim is to break the chains of infection as early as possible.
- **Guidelines 5/2020 on consent under Regulation 2016/679** focus on the changes that have occurred as a result of the GDPR. They provide practical guidance on how to comply with the GDPR's requirements on consent based on Opinion 15/2011 of the Article 29 Working Party (EDPB predecessor). Among other things, there was a need for clarification regarding the validity of consent when interacting with 'cookie walls' and regarding consent when scrolling (see also 3.2.2).
- **Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR** aim to provide further guidance on data protection aspects in the context of the PSD 2 (Payment Services Directive 2), in particular on the relationship between the relevant provisions of the GDPR and the PSD 2. The substantive focus of these guidelines is on the processing of personal data by account information service providers (AISPs) and payment initiation service providers (PISPs).
- **Guidelines 7/2020 on the concepts of controller and processor in the GDPR** have the main objective of clarifying the meaning of the terms, the different roles and the allocation of responsibilities between these parties (see also 3.2.1).
- **Guidelines 8/2020 on the targeting of social media users** are intended to clarify the division of roles and responsibilities between social media platforms and companies or other organisations using targeting features of these social media platforms, against the background of several ECJ judgments (ECJ, Judgment of 5 June 2018, Case C-210/16 and

¹ Statement on the Judgment of the European Court of Justice in Case C-311/18 - Data Protection Commissioner v Maximilian Schrems and Facebook Ireland of 17 July 2020 (<https://www.bfdi.bund.de/edsa-stellungnahmen>)

² Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_de)

Judgment of 29 July 2019, Case C-40/17). They should also illustrate the impact of the respective data processing operations on the (fundamental) rights and freedoms of data subjects using practical examples.

- **Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679** provide guidance on what constitutes a ‘relevant and reasoned objection’ by affected supervisory authorities to proposed decisions by lead supervisory authorities in cross-border supervisory cases. They also clarify how to proceed and what to consider when evaluating an objection.

Opinions in the consistency mechanism/decision in the cooperation procedure

Under the consistency mechanism, the EDPB issued 28 opinions. These largely concern binding internal data protection rules submitted by Member States (Article 47 of the GDPR), standard contractual clauses (Article 48[8] of the GDPR) or the accreditation of certification bodies (Article 43[3] of the GDPR) or bodies for monitoring compliance with codes of conduct (Article 41 of the GDPR).

In my last activity report, I pointed out that no draft decision had yet been issued by lead national supervisory authorities in any major cross-border case involving leading global tech companies. A first such draft is now available and has already become the subject of an objection procedure under Article 60(4) of the GDPR, in which German supervisory authorities have also been involved. The EDPB formally ruled on such an objection for the first time in November 2020.

EDPB Strategy 2021-2023

In addition to its programme of work, the EDPB has established a strategy for 2021 to 2023. This is based on four pillars: The first pillar involves **advancing harmonisation and facilitating legal conformity (compliance)**. To this end, the EDPB aims at maximising consistency in the application of data protection rules and limiting fragmentation among Member States. The second pillar **aims to support effective enforcement and efficient cooperation between national supervisory authorities**. To this end, internal processes are to be optimised, specialist knowledge pooled and improved coordination promoted, among other things. The third pillar formulates a **fundamental rights approach to new technologies**. For example, this includes the evaluation of new technologies such as AI, biometrics or profiling. The fourth pillar is **the global dimension**. The EDPB is

committed to promoting the high level of EU data protection beyond the borders of the EU in the development of global standards. I have already set the course for this by being elected to the Executive Committee of the Global Privacy Assembly (GPA),³ Accordingly, the Chair of the EDPB and several members have expressed their support and stressed the importance of close cooperation with the GPA.

Cross-references: 4.3 Schrems II, 3.3 Global Privacy Assembly

3.2.1 Report from the Key Provisions Expert Subgroup

In 2020, the EDPB’s Key Provisions Expert Subgroup (KEYP) continued to address important fundamental questions on the interpretation of the GDPR. It was able to finalise the discussions on the guidelines on the concepts of ‘controller’ and ‘processor’, as well as revising the guidelines on consent concerning ‘cookie walls’ and ‘scrolling as consent’. Work continues on other important dossiers.

Guidelines 07/2020 on the concepts of controller and processor

For the application of the GDPR, it is of key importance whether a party acts as sole controller, joint controller or processor. The guidelines therefore provide important guidance on how to distinguish between these. This guidance is complemented by practical cases of application (Part 1 of the guidelines).

The second part of the guidelines takes a closer look at the relationship between joint controllers and between controllers and processors, with particular reference to the legal implications of this. The appendix to the guidelines is likely to be of particular interest to practitioners. This contains a flow chart to allow the parties involved to review their role.

The public consultation on the guidelines ended in October 2020 and the final text is expected to be published in early 2021.

Updated Guidelines 05/2020 on consent under the GDPR

Following preparatory work by the KEYP, the EDPB has adopted a revised version of the guidelines on consent under the GDPR with regard to consent for the use of websites. Firstly, the EDPB clarified that merely scrolling or continuing to surf a website is not effective consent in any case. Here, there is a lack of a clear affirmative action. Secondly, the guidelines now contain a clear indication that access to an online service may not be made dependent on permission to use cookies (‘cookie walls’). In the case of websites which, due to their struc-

3 ‘BfDI elected to Executive Committee of the Global Privacy Assembly’, press release of 16 October 2020 (www.bfdi.bund.de/pressemitteilungen)

ture, force tracking on users in this way, consent is not voluntary. Exceptionally, cookie walls are permissible if a comparable service is also offered without tracking, for example as a service subject to payment.

As a member of the EDPB, I agreed with the revision of the guidelines and hope that controllers will draw the right conclusions from this and finally offer privacy-friendly alternatives. The cookie issue also plays a role in the legislative process for the e-Privacy Regulation (see 5.10). The revised guidelines on consent are available in English on the EDPB's website and will also be available on the DSK's website once they have been translated into German.

Ongoing work

According to the EDPB's work plan, guidelines on data subjects' rights will be developed in the KEYP. The first step is the right of access under Article 15 of the GDPR. The dossier is intended to provide assistance with the numerous issues that are very important in practical application. This concerns the scope of the right to copy (Article 15 [3] of the GDPR) as well as exceptions and limitations to the right of access (Article 15 [3] of the GDPR, Article 12 [5] of the GDPR). In the reporting period, initial drafts were discussed and preliminary decisions were taken on a number of issues. The adoption of the guidelines on data subjects' rights/the right of access, in which I am involved as co-rapporteur together with the State Representative for Data Protection in North Rhine-Westphalia (Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, LDI NRW), is expected in 2021.

In the meantime, a working group has also started its work within the KEYP to draft guidelines on the legal basis of 'legitimate interest' under Article 6 (1) (f) of the GDPR. These guidelines are receiving a great deal of attention from the professional community. The underlying GDPR standard was largely openly formulated and sometimes misleadingly interpreted as an 'elastic clause'. It has even been used as a supposed legal basis for particularly risky data processing operations, which is, however, incompatible with this standard. Together with the State Representative for Data Protection in Baden-Württemberg (Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, LfDI Baden-Württemberg) and the State Representative for Data Protection in Mecklenburg-Western Pomerania (LfDI Mecklenburg-Western Pomerania) I am involved in the drafting as co-rapporteur. The guidelines on legitimate interest will replace the 2014 Working Paper 217 of the Article 29 Working Party (Opinion 6/2014). I will do my utmost to ensure that the guidelines address the existing problems in practice as concretely as possible and that

this legal basis does not prove to be an arbitrary catch-all for otherwise untenable data processing operations.

Cross-reference: 5.10 Current legislation and other regulations in the telecommunications sector, e-Privacy Regulation

3.2.2 Evaluation of the GDPR: the first round is complete

The European Commission had to carry out an evaluation of the GDPR by the deadline of 25 May 2020. It consulted the EDPB for this purpose. Overall, the Commission takes a positive view of the GDPR. Nevertheless, it sees a need for improvement in practical implementation.

In accordance with Article 97 (1) of the GDPR, the European Commission submitted a report to the European Parliament and the Council on the evaluation and review of the GDPR. To this end, it requested information from the EDPB pursuant to Article 97 (3) of the GDPR. The DSK forwarded to the EDPB its progress report on the application of the GDPR, the content of which I already presented in detail in my last activity report (see no. 4.1 of the 28th AR).

On 18 February 2020, the EDPB adopted the joint response article to the evaluation of the GDPR. It stresses the importance of the GDPR for the protection and strengthening of the fundamental right to data protection within the EU. Overall, the EDPB considers the GDPR to be a successful set of regulations that are uniform throughout Europe. Although it does not see any need for short-term revision at present, it does identify the need for improvement in a number of areas. For example, it stresses the need to cut red tape for small and medium-sized enterprises (SMEs). It also requires supervisory authorities to be adequately equipped with the necessary resources for the effective implementation of the One-Stop-Shop mechanism. With regard to international data flows, the EDPB stresses the importance of the European Commission's adequacy decisions. It calls on the Commission to revise the decisions on EU standard contractual clauses for data transfers to third countries.

In its Evaluation Report of 24 June 2020, the European Commission assesses the GDPR as an overall success. The essential objectives of the GDPR have been achieved. The Commission supports the call for supervisory authorities to have adequate resources, both financially and in terms of staffing. The reduction of bureaucratic burdens for SMEs whose data processing operations do not involve high risks should at least be reviewed. The expandability of the right to data portability (up to real-time data exchange) as a central data subject right is also flagged. The Commission sees the continuing fragmentation within the scope of the GDPR due to the use of opening clauses by national legislators as problematic.

No current need for change

Overall, the European Commission sees no need to adapt the GDPR through concrete amendments. The next evaluation is scheduled for 2024 in accordance with Article 97 (1) of the GDPR. In the meantime, supervisory authorities must continue to contribute to the necessary debate on data protection policy.

I also believe that extensive legislative changes to the GDPR are premature at this point in time. The EDPB develops guidelines on various topics, which I am heavily involved. This is intended to ensure the uniform application of the law in the regulatory area of the GDPR, avoiding a European patchwork quilt of regulations. Overall, the GDPR is a major step forward for data protection in Europe. The new set of rules has also proved its worth throughout the coronavirus pandemic. Even beyond European borders, the GDPR serves as a modern basis for the adaptation of data protection law. Despite the great progress made, I do see a need for improvement in the practical implementation of the GDPR. This is particularly true in the area of cooperation between data protection supervisory authorities in cross-border proceedings. Differences in national administrative procedures should not hamper the effective enforcement of the GDPR against data protection breaches by companies that operate internationally.

3.2.3 Face recognition – benefits and limitations

What happens to a society when its members are regularly checked by the police when in public spaces? In squares, train stations and transport hubs, every day? Without there being cause for this?

This scenario is not a description of conditions in distant, authoritarian countries. It happens in Europe. It happens in Germany. Security agencies in Europe, the Federal Government, and states are looking to take advantage of biometric facial recognition. There are discussions about using more and more surveillance cameras for this purpose. These are already set up for people in numerous public places and stations (see no. 9.3.3 of the 27th AR and no. 6.2 of the 28th AR).

For the security agencies, this allows them to compare faces of passers-by in real time, i.e. 'live', against wanted lists. They can gather details about the circumstances of suspects, carry out undercover investigations and make arrests.

Such an approach raises fundamental issues. The live comparison described is the same as a police check carried out for all persons passing by or staying in a certain place. It would be the same if every person had to give their fingerprint when entering a train station so that

this can be checked against police lists. Then everyone is a suspect. The only way they aren't is if they're not a hit when compared against the lists. The presumption, vouched for by the Federal Constitutional Court, that citizens are fundamentally righteous is being turned on its head.

The application of such technology directly affects the privacy of the individual. But technology also threatens a functioning democracy. For many people, the assumption that they can move about anonymously in public spaces is a basic prerequisite for participation in demonstrations, political engagement and the formation of opposition. The knowledge that you are constantly being recorded by the state has an intimidating and discouraging effect. Self-determination and diversity suffer as a result. However, these are fundamental requirements for a functioning free democratic community based on plurality and its citizens' ability to be involved in this.

EDPB guidelines

I welcome the EDPB's decision to develop guidelines on the use of facial recognition technology by law enforcement agencies. This includes not only the aforementioned live monitoring, but also other applications. I am pleased to be able to play a leading role in the guidelines as one of the rapporteurs.

Opinion on Clearview AI

Law enforcement agencies can also use the Internet to identify people. Companies specialising in this field use their facial recognition software to analyse huge amounts of photos that people have shared on social networks, for example. But photos on employer websites are also used. Numerous security agencies around the world have already used such services.

The events surrounding the company Clearview AI led to an enquiry by several members of the EU Parliament. A joint opinion was then drawn up in the EDPB, in which I participated as rapporteur.

In its opinion, the EDPB points out that such data processing differs substantially from intra-agency image comparisons. Private companies carry out the data reconciliation here—as auxiliaries, essentially. The way in which the data pools are created and their legality is also unclear. I am critical of the processing of data obtained in this way in a third country, such as the USA.

The EDPB calls for a policy debate on the role of technologies such as facial recognition, in particular their impact on fundamental rights. I strongly agree with this assessment.

3.2.4 Approval and publication of the (German) accreditation criteria for monitoring bodies pursuant to Article 41 of the GDPR

The German accreditation criteria for monitoring bodies of codes of conduct have been approved by the EDPB and have been published on the DSK's website.

Pursuant to Article 57 (1) (p) of the GDPR, each supervisory authority in its territory must draw up and publish the requirements for the accreditation of a body for monitoring compliance with codes of conduct pursuant to Article 41 of the GDPR. Prior to this, they had to be approved by the EDPB within the framework of a consistency mechanism pursuant to Article 64 (1) (c) in conjunction with Article 41 (3) of the GDPR. Codes of conduct 'specify' the GDPR, which in part contains very abstract regulations and a large number of general clauses. Codes of conduct can be used here as an aid to interpretation.

The consistency mechanism and the associated EDPB opinion on the national draft accreditation requirements serve the uniform application of Articles 40 and 41 of the GDPR by all EU Member States, pursuant to Article 63 of the GDPR.

I had already helped develop the European 'Guidelines 1/2019 on codes of conduct and monitoring bodies under Regulation (EU) 2016/679'. These guidelines are intended to provide practical advice and interpretative guidance on the application of Articles 40 and 41 of the GDPR and to explain the rules and procedure for the submission, approval and publication of codes of conduct at a national and European level. Among other things, the guidelines state that a code of conduct (for the non-public sector) should specify an accredited monitoring body. In addition to the competent data protection supervisory authority, the latter monitors whether members who have signed up to the code of conduct comply with its provisions.

The German accreditation criteria for monitoring bodies of codes of conduct were approved by the EDPB. They are published on the DSK website.

I also contributed to the EDPB's opinions on the accreditation criteria for monitoring bodies of codes of conduct of ten other EU Member States.

3.3 Global Privacy Assembly

In 2020, the Global Privacy Assembly (GPA)—known as the 'International Conference of Data Protection and Privacy Commissioners' until 2019—addressed, among other things, the challenges of the COVID-19 pandemic for data protection. For the first time, a German representative, the BfDI, was elected to the 'Executive Committee' of the GPA.

Like many other international organisations or associations, the GPA, with over 120 data protection authorities from around the world, was affected by the COVID-19 pandemic. This was evident in the functioning of the GPA itself as well as in the treatment of technical issues. It had already become clear in the spring of 2020 that the conference in Mexico City planned for the autumn could not take place as scheduled. However, with the support of the Secretariat, and particularly under the guidance of the GPA Chair—my UK colleague, Elizabeth Denham—the GPA managed to respond swiftly and successfully to the data protection challenges the pandemic brought with it.

The Executive Committee issued two statements on ensuring data protection even under pandemic conditions. These are a general statement issued in March 2020 and a statement on privacy-compliant contact tracing issued in May 2020. In addition, the Executive Committee, as the GPA's steering body, established a COVID-19 Taskforce, which worked throughout the year on ensuring privacy under the special conditions of the pandemic.

I was happy to participate in this task force, contributing in particular my experience from data protection monitoring for the German Corona-Warn-App. In the context of the fight against the COVID-19 pandemic, it was noticed quite early, first in Asian countries such as Singapore, South Korea and Taiwan, that applications for mobile devices could be considered as suitable tools for contact tracing. The development of corresponding software applications was then started immediately. The accumulated expertise of the COVID-19 Taskforce was eventually incorporated into a comprehensive 'Best Practice Compendium' which was made available to GPA members.

I am pleased that our annual meeting of GPA members in autumn 2020 could still take place as a joint video conference thanks to the efforts of the GPA Chair and Secretariat. The first meeting of this kind took place in Bonn in 1979 under the name of the 'International Data Protection Conference'.

Preparing for such a digital global event entails considerable practical difficulties. A suitable time has to be found for participants from Chile in the west to New Zealand

in the east, because it is always very early or very late somewhere.

The 2020 Virtual Annual Meeting didn't just address the COVID-19 pandemic. Resolutions were also adopted on important issues for the future, such as AI (artificial intelligence) and facial recognition. In both cases, the GPA requires transparency for data subjects on the nature and scope of the processing of personal data. There should also not be any decisions made about people that are purely machine decisions. This is important not only to protect personal data, but also to avoid discrimination inherent in the system.

The GPA has continued on its path towards a more structured organisational form. Its members have allowed the Executive Committee to submit resolutions or decisions for adoption outside the annual meeting in the future. This should enable the GPA to better respond to current issues and events relevant to data protection as an organisation.

I was elected to the GPA's Executive Committee at the meeting as the first German member. I would like to express my sincere thanks for the broad support I received from my GPA colleagues in this unanimous election. Over the next two years, I will bring both the broad experience of German data protection authorities and seek to link the GPA Executive Committee with the EDPB. In doing so, I would like to also contribute to the further harmonisation of data protection at global level.

The current plans are to hold the 2021 conference in Mexico as an in-person event. I would like to thank my colleague in Mexico for his willingness to host the GPA conference again one year later.

The GPA's statements, resolutions and further documents can be found at www.globalprivacyassembly.org.

Cross-references: 3.2 EDPB, 4.1.1 Corona-Warn-App

4

Main topics

4.1 Coronavirus

The coronavirus pandemic shaped the entire of 2020—including data protection. Advice and information weren't just necessary and time-consuming in connection with the development of apps, but also for the privacy-compliant design of laws and regulations or the use of video conferencing systems. Below are some of the advice points on pandemic response.

4.1.1 The Federal Government's Corona-Warn-App

The Federal Government's Corona-Warn-App (CWA) was released by the Robert Koch Institute (RKI) on 16 June 2020, after just over two months of development. As a contact tracing app, it allows encounters between app users that may be relevant for infection to be collected in a privacy-friendly way, using Bluetooth. If there is a positive COVID-19 test result, users can very quickly alert their contacts via the Corona-Warn-App without having to disclose their identity. Those alerted then have the option of contacting doctors and health authorities to get themselves tested. By behaving with proper caution, the contact persons who receive a warning are making an effective contribution to the prevention of further infections.

I have been involved in the CWA project in an advisory capacity from the very beginning and am also responsible for data protection supervision in the RKI project.

Data protection as a success factor

To be effective, the CWA relies on the support of large sections of the population. Data protection is an essential factor for such digital solutions to be accepted. The comparatively high number of a good 25 million downloads shows that this is also the case with the CWA. For example, its French counterpart, which takes a less privacy-friendly approach with centralised data processing, is already considered a failure, with only about 2 million downloads and even lower usage.

Such a centralised approach, like in France, was first discussed in Germany and other countries through the

multinational PEPP-PT initiative (Pan-European Privacy-Preserving Proximity Tracing). However, following critical review by academia, civil society and data privacy advocates, the implementation of this approach was ultimately rejected by the Federal Government at the end of April 2020. Instead, the decentralised approach now used was consistently implemented from this point onwards. The project was flanked by sensible measures, such as development in an extremely transparent open source process. The general criticism of the use of the Google/Apple Exposure Notification protocol provided by Apple and Google, particularly the accusation of unauthorised collection of data, has so far not been supported by comprehensible evidence. Overall, it can be said that the CWA represents the fundamentally privacy-friendly implementation of the decentralised contact tracing approach.

Problematic media disruption

The positive impression of the core application in the form of the CWA is unfortunately contrasted by the problem-laden operating environment, which is indispensable for practical use. It was already clear at the launch of the CWA that not all of the participating laboratories would be able to make their test results available to app users due to the lack of the necessary technical equipment.

Thus, users whose tests were evaluated by these laboratories could not use the privacy-friendly workflow for providing results in the CWA and could not directly alert their contacts in the event of a positive result. Instead, an alternative process using 'tele-TANs' had to be established for these cases. In order to receive this tele-TAN, users who tested positive had to contact an activation hotline.

This undesirable media disruption in app use poses a data protection risk, especially since the hotline briefly holds personal data to identify callers.

In the context of data protection supervision, I have therefore paid particular attention to the early review of

this hotline. In doing so, I found minor deficiencies in access control.

Fortunately, the RKI succeeded in remedying these deficiencies in a timely manner. However, the problem of the lack of laboratory connections has not yet been resolved. The media disruption, which is problematic from a data protection point of view, persists.

A view to the future

At the time of going to press, there was still no end in sight for the COVID-19 pandemic. Recent criticism of the CWA's lack of capabilities and features was partly justified, but often due to ignorance of the deliberately chosen objective and the limits of the technical possibilities of the chosen approach. For example, the CWA was deliberately developed for the purpose of data-saving contact tracing. Therefore, contact tracking was not planned and is not technically feasible in this app. Notwithstanding this, there is of course potential for further development with respect to the CWA. Ideas like cluster detection are useful and possible. It is just a shame that I, as the competent data protection supervisor, only learned of many of these considerations late and from the press. Here, timely involvement from those responsible in the planning stage would have been more appropriate.

When the COVID-19 pandemic ends, as will the use of the CWA. The lessons learned on how to implement such solutions on a voluntary basis in an effective and privacy-friendly way should be taken into account in any future projects.

Further information on the subject can also be found in the EDPB's Guidelines of 21 April 2020, available at www.bfdi.bund.de/guidelines.

4.1.2 The data donation app

The Robert Koch Institute (RKI) uses the Corona Data Donation app to analyse data provided on a voluntary basis from fitness trackers of now more than 500,000 citizens. To this end, the RKI also processes data concerning health in particular, which is considered to be a special category of personal data. Using the knowledge gained from analysing this data, the RKI intends to optimise the prediction of diseases such as COVID-19. This should allow better management of containment measures taken to fight against the current pandemic.

Amidst the debate on the introduction of a corona tracing app, the RKI released the Corona Data Donation app on 7 April 2020. With the surprising release of this additional app, the RKI caused confusion not only among the general public.

I was also involved with just a few days notice. In my initial assessment, I was able to advise the RKI on some aspects that are key for data protection. However, a final version of the Corona Data Donation app was not made available to me until it was released in April.

With the release of this first government coronavirus app, the RKI met with wide resonance from civil society. I expressly welcome this dedication, such as the investigation by the Chaos Computer Club (CCC). Deficiencies identified in the process always serve to improve the situation and, not least, provide additional insights for data protection supervision work.

To this day, I am still accompanying the RKI in this project as part of my data protection supervision. Various aspects of data processing were reviewed. Any deficiencies identified were immediately discussed with the RKI and often remedied at very short notice. Corrective measures under Article 58 of the GDPR was not required by the editorial deadline.

As with my initial assessment, further analysis and evaluation showed that the interface between the RKI's systems and the fitness tracker providers is the biggest problem in terms of data protection. The privacy-compliant collection of fitness tracker data from the systems of the various providers presented the RKI with major challenges in terms of data minimisation. However, this is absolutely necessary to be able to keep the central promise of pseudonymity for Corona Data Donation app users.

Regardless of specific shortcomings, the question of whether data processing actually fulfils its actual purpose always arises in such a project of an experimental nature. If it does not, processing must be stopped. Therefore, I indicated at the time of release that I expected regular evaluations. The RKI's statements made available to me so far do not yet allow a final evaluation in this respect.

4.1.3 Coronavirus measures and projects

Data protection in the age of coronavirus: how can data protection be prevented from becoming a prominent victim of the pandemic? Trust is fundamental for acceptance by users of digital applications. Therefore, I advise on the development and origin of such applications, but I am not a approval authority.

The Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) developed and funded a number of projects to help manage the coronavirus pandemic. As early as spring, the project manager responsible at the BMG approached me and asked for my support. As I have a great interest in ensuring that the protection

of personal data is kept in mind in view of the special circumstances and the great time pressure, I gladly agreed to give priority to the respective measures and projects.

Symptom diary

One of the projects was the symptom diary—a web-based application to facilitate the management of contacts by health authorities, made available to them free of charge by the BMG. Contacts in quarantine receive a daily link and then fill out the online questionnaire about their symptoms themselves, meaning time-consuming telephone calls are no longer required. I advised the BMG and worked with them to improve the documents. For example, an additional reporting feature that generates statistical evaluations for the data collected was dropped after I expressed doubts about the effectiveness of the anonymisation provided for this purpose and demanded appropriate safeguards.

However, a conclusive or binding assessment was prevented by the fact that concrete integration into the IT structure was also important. In addition, the respective state data protection commissioners are responsible for data processing in municipal health authorities. However, I could not comply with the urgent wish—expressed not only here—to issue ‘approval’, because this is not part of my legal duties and rights. The BfDI is not an approval authority, because this would, for example, also require a technical review of all the components used in a solution.

DEMIS-SARS-CoV-2

I advised the BMG and the Robert Koch Institute (RKI) on the launch of the German Electronic Reporting and Information System for Infection Prevention (Deutsche Elektronische Melde- und Informationssystem für den Infektionsschutz, DEMIS) in an initial expansion stage (DEMIS-SARS-CoV-2). I already closely accompanied this software in the early days of its development in 2013/2014. DEMIS is intended to serve the purely electronic processing of notification obligations provided for in the Infection Protection Act (Infektionsschutzgesetz, IfSG), but also provides for further features with central data storage and access options for the respective authorities. The legal basis for DEMIS is Section 14 of the IfSG. However, the regulation envisaged here with more detailed provisions for implementation is not yet available. DEMIS is therefore not yet fully operational. Certain functions are likely to create areas of shared data protection responsibility which require specific arrangements. However, to be able to use a secure transmission channel for reporting the large number of infected persons as quickly as possible in the pandemic, the system was put into operation early—with limited scope. The data protection responsibilities can be assigned more easily

for these functionalities. In this way, the data can be transmitted in encrypted form from the laboratories to the health authorities and on to the RKI. According to a predefined structure, test results and other information are collected, assigned in the system to the responsible health authority and then reported to them. A special pseudonymisation procedure is used to identify duplicate reports. This is significant progress over the previous fax transmission method, both in terms of speed and data protection. The obligation initially introduced in the IfSG to report those tested negative should also have been fulfilled via DEMIS. I had already pointed out to the RKI that I did not consider the reports to be admissible. Even before the operation of DEMIS-SARS-CoV-2, the obligation was sensibly removed from the law.

SORMAS@DEMIS

In connection with DEMIS, the BMG and RKI also advised on the SORMAS software which has various modules. SORMAS stands for Surveillance Outbreak Response Management and Analysis System and was developed by the Helmholtz Centre for Infection Research (Helmholtz-Zentrum für Infektionsforschung, HZI) to record cases and contacts. The BMG wanted to make this software available to health authorities free of charge to support their work. The SORMAS-ÖGD version was also previously used to manage cases in some health authorities—SORMAS -L (for local). In addition to a reporting feature, it also contains an interface for a quarantine diary feature. With efficient contact management, the connection of SORMAS to DEMIS facilitates the determination of contact chains, including across municipal borders, as health authorities are also networked with each other—SORMAS X (for eXchange). Another module is used for overarching data analysis—SORMAS XL (for eXtra Laxer)—but at the time of going to press, it is not yet in use as I had raised concerns about the unclear legal basis. I welcome the fact that the applications are hosted by the Federal Information Technology Centre (Informationstechnikzentrum des Bundes, ITZBund), as this removes any concerns about data being held by private companies. To meet the legal requirements, the respective health authorities must now conclude commissioning agreements with ITZBund.

The problem that I am not legally responsible for evaluating the software in its specific use in health authorities was also something that came up in this consultation. In this case, in consultation with the BMG and the HZI, I involved the state data protection commissioners in the consultation and coordinated a joint data protection assessment by the competent data protection supervisory authorities in the states. Ultimately, together with the data protection authorities of the federal states, I agreed to the start of operation ‘with reservations’, since

the BMG had given assurances that it would also initiate necessary data protection improvements during operation. In addition, the previous practice of case processing in health authorities was often neither efficient nor privacy-compliant, and there was a lot of political pressure to use the new system.

KaDoIn research project

Another request for advice from the BMG related to KaDoIn, an application designed by the Hannover Medical School (Medizinische Hochschule Hannover, MHH) for the card-based documentation of index patients. KaDoIn is used to read the location data from the smartphone of an infected index patient, visualise it using Google Maps, process it in a structured way and compare it with the location data of potential contact persons. As part of a study funded by the BMG, the MHH investigated how this can support contact tracing by health authorities. The concern about inadmissible tracking was quickly dispelled, as the data is prepared locally in the browser and provided in a structured format. The user—i.e. the index patient—makes their own decision as to the data they select and send to the health authority. Participation in the study was voluntary, so I did not see any significant obstacles under data protection law.

Cross-reference: 4.1.4 Amendments to the Infection Protection Act

4.1.4 Amendments to the Infection Protection Act

The Infection Protection Act (Infektionsschutzgesetz, IfSG) was amended in three ‘stages’ due to the pandemic. In this context, the extension of both the reasons for and the scope of reporting obligations for diseases and pathogens significantly interfered with the fundamental right to informational self-determination. Transparent justifications and a discussion of the data protection requirements would have been necessary, but were repeatedly lacking. The insufficiently justified obligation to report the negative test results was wisely removed.

After the obligation to report diseases and pathogens under the Infection Protection Act was extended to COVID-19 and SARS-CoV-2 through a regulation issued in January 2020, the Infection Protection Act was amended in March, April and November. Technical votes and political decisions were made in the shortest possible time. It was not just the number of laws and regulations processed by the Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) that rose to record-breaking heights as a result of the pandemic. The time allowed for referral was also extremely short. At the same time, the BMG did not allow the participation periods provided for

in the Joint Rules of Procedure of the Federal Ministries for the many other laws and ordinances not based on ‘coronavirus’ for no discernible reason.

First Pandemic Protection Act

With respect to the (First) Act on the Protection of the Population for an Epidemic Situation of National Importance, there was an advance warning on Friday afternoon that the draft would be published on Saturday, 21 March 2020, with a deadline for comments of four (!) hours. In addition to far-reaching powers of intervention and ordinances for the BMG, obligations for carriers and airlines were provided for. I raised substantial doubts as to the constitutionality, in particular as to the appropriateness of some of the measures. Even during a pandemic, fundamental rights should not be suspended. Unfortunately, most of my concerns were not addressed. Neither the necessary improvement of the justification nor the evaluation demanded by me, nor the necessary erasure specifications nor the target-oriented data protection law monitoring of cross-border research projects centrally by me were provided for. The Act also amended the International Health Regulations Implementation Act. The Passenger Information System requests now provided for therein violate the EU Directive on PNR data.¹ After the Bundestag passed the law on 25 March 2020, and the Federal Council approved it on 27 March, it entered into force on 28 March 2020 (see my opinion of 3 April 2020 www.bfdi.bund.de/stellungnahmen)

Second Amending Act

The draft of the Second Act for the Protection of the Population in the Event of an Epidemic Situation of National Scope was sent out on the afternoon of 20 April 2020 with a request for comments by 22 April 2020. This bill also contained far-reaching changes to the IfSG. Not all of them were urgent: without reference to the current situation, the obligation to report new, previously unknown diseases by name has already been extended to suspected cases. However, the newly introduced obligation to report negative test results to the Robert Koch Institute (RKI) specifically related to SARS-CoV-2 and SARS-CoV. However, the justification for this was based solely on statistical considerations. The fact that the reports to the RKI were to be submitted pseudonymously and therefore had to comply with the requirements of the GDPR was not taken into account in the law and its justification. The Infection Protection Act serves to avert danger, specifically to protect against infection with an infectious disease. However, those who test negative are not contagious. I therefore considered notifications in this form to be unnecessary and therefore inadmissible.

¹ Article 1 (2) of Directive (EU) 2016/681 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.

Unfortunately, the provision nevertheless remained in the law initially. The immunity passport did not make its way into the law. An immunity passport would contain health-related information—a doctor's assessment of immunity. This would make it substantially different from the vaccination certificate, which documents the fact of vaccination. As far as the vaccination certificate is concerned, inspection may only be requested in certain cases. As immunity with respect to SARS-CoV-2 had not yet been scientifically clarified in April, the regulation was withdrawn again. In my view, it would be incompatible with the right to informational self-determination if proof of immunity were to be used generally as an 'admission ticket'. Conversely, this would lead to discrimination against those who could not provide such evidence. This law came into force on 23 May 2020.

The procedure for this legislation showed that the pandemic also caused great uncertainty in the government. There was a lack of reliable scientific knowledge on infection routes and risks, the probability of contracting the disease and the risk of re-infection, and targeted treatment using medication. This uncertainty evidently should be addressed with the comprehensive, legally mandated nationwide state collection of personal health data. The question of whether regional surveys or surveys based on consent in the context of clinical and scientific research projects could also have led to sufficient findings was not discussed.

Third Pandemic Protection Act

The Third Act on the Protection of the Population for an Epidemic Situation of National Importance was submitted on the evening of 14 October 2020, with a comment period that ended on 16 October 2020. An amended and partially supplemented version was sent on the morning of Friday 23 October, with a deadline of 6 p.m. on the same day. These extremely short deadlines made proper processing difficult. As the pandemic had already existed for several months at that point in time, this haste was not appropriate in my view, but could at least have been mitigated by involvement in the deliberations even before an agreed draft was produced. Once again, various reporting obligations and transfers of personal data have been introduced or extended. It was not taken into account that the processing of health data, i.e. particularly protected personal data, constitutes an interference with the fundamental right to informational self-determination. These must therefore be carefully justified and accompanied by specific measures to protect sensitive data. In particular, a refinement of the information on the place of residence of infected persons was foreseen, without taking into account that this would increase the risk of re-identification. This is because this regulation does not only apply to COVID-19, but also to other,

rarer pathogens. In addition, it was stipulated without sufficient justification that pseudonymous reports on vaccination and vaccination consequences must now be addressed to two different bodies—the Robert Koch Institute and the Paul Ehrlich Institute. This leads to the data doubling in size, which I take a critical view of. The obligations on entry have also been extended: instead of the disembarkation card, which has to be completed by passengers on the basis of international health regulations and then forwarded to the competent health authority, a digital entry declaration is now envisaged, in which individual travellers must also provide information about themselves and their stay.

It is also interesting to compare the wording of the previous disembarkation card and that for COVID-19: in the previous one there are explanations of the basics of data processing. Then data about the person, fellow travellers and whereabouts are requested. The COVID-19 version, on the other hand, drastically points out the obligation to complete the form and the threat of a fine if false information is provided. Then additional health information is requested, namely symptoms and testing. This meant that increased requirements had to be met in terms of the security of data processing, which I had to take into account when advising on technical implementation for the digital transmission of disembarkation cards.

The Third Pandemic Protection Act was again problematic with regard to the regulations concerning obligations and powers for transport companies and the Federal Police in connection with entry. A regulation may provide for transport companies being required to be provided with evidence of registration requirements, vaccinations and health status and for transport companies in turn being required to provide data on passengers. The Federal Police should monitor compliance with the obligations under the ordinance and report violations. The justification here once again fell well short of the requirements of the Joint Rules of Procedure of the Federal Ministries. The encroachments on fundamental rights are not sufficiently weighed up and justified. In particular, the appropriateness and necessity of the measures are not demonstrated. In the context of the EU, a distinction between cross-border and domestic travel requires special justification. There is no mention of the specific safeguards required by Article 9 (1) of the GDPR for the processing of data concerning health. Further requirements for transport companies, i.e. private companies, are missing. Regulations must be put into place for whether and how they are permitted to collect data and how long, to what extent and with what safeguards they are permitted to store it. However, I was able to chalk up the fact that with this law, the obligation

to report the negatively tested was removed again before its implementation had begun, as a success.

4.1.5 Protective mask only against data?

Shortly before Christmas, the Federal Minister of Health wanted to do something good and have protective masks distributed free of charge by prescription via pharmacies to those particularly at risk. Some pharmacists saw this as an opportunity to access their customers' data for other purposes.

At the start of December, the Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) issued the Ordinance on the Entitlement to Protective Masks to Avoid Coronavirus SARS-CoV-2 Infection—Coronavirus Protective Mask Ordinance (Verordnung zum Anspruch auf Schutzmasken zur Vermeidung einer Infektion mit dem Coronavirus SARS-CoV-2 - Coronavirus-Schutzmasken-Verordnung, SchutzmV), which entitles persons over the age of 60, as well as anyone who has certain diseases or certain risk factors for COVID-19 to be severe, to three FFP2 protective masks or masks of similar quality. Distribution is via pharmacies. For the distribution, clause 1 of Section 4 (1) of the SchutzmV stipulates that those entitled to protection should prove their age by 'presenting their identity card'. As I have been able to gather from some of the complaints of data subjects, some pharmacists immediately copied customers' identity cards in this regard. There is no justification or legal basis for this. In addition, some pharmacists only wanted to hand out a protective mask, which was actually to be given away free of charge, if the data subjects had previously filled out an application for a customer card and agreed that their data could be transferred to third parties (for marketing purposes). The protection masks, which are actually free of charge based on the BMG's intentions, would therefore be paid for with the data of those entitled to the free masks.

I have asked the BMG to intervene and ask pharmacies to act in accordance with the regulation. As I am not the competent data protection supervisory authority for pharmacies, I have passed on the specific complaints to my colleagues in the federal states, advising to check whether fines are to be imposed here under the GDPR.

4.1.6 Messenger and video conferencing systems — a blessing and a curse in coronavirus times

Video conferencing systems and messenger apps have seen a huge increase in importance since the coronavirus pandemic began, as conferencing, working from home mobile working would be much harder without them. Unfortunately, not all systems are safe in terms of data protection.

Working from home and mobile working can contribute to reducing the number and duration of direct contacts in situations such as the coronavirus pandemic, thus reducing the risk of infection. The widespread availability of high-capacity mobile or fixed-line connections means that a large proportion of meetings and events that were previously held as face-to-face events can now be held virtually instead. However, the principles of data protection must be observed, which proves to be problematic with many technical solutions.

Initial great uncertainty

When contact restrictions started in spring 2020, many companies and government agencies were forced to quickly create a functioning communications infrastructure to make working from home and mobile working something that worked on a scale that was previously almost unimaginable. At this stage in particular, in addition to purely practical challenges, there was a great deal of uncertainty as to which of the solutions available companies and authorities would be able to use. There could be no neglect when it came to protecting personal data concerning employees and customers. On the other hand, there was an increased willingness—whether conscious or unconscious—to put this protection aside for the time being.

Opportunities and risks when using video conferencing systems

Especially in a situation like the coronavirus pandemic, video conferencing systems give people the opportunity to significantly reduce the number and duration of direct contacts if employees increasingly work mobile or work from home, or if business trips to on-site appointments are replaced by video conferences. However, these benefits are also accompanied by a number of risks. These concern both the persons participating in a video conference and persons about whom personal data is exchanged, for example by means of messenger, or spoken about in a video conference. Here, it is important to protect the privacy of employees (and their families, if applicable) who participate in video conferences from home, and also to ensure that sensitive content is protected in the same way it is in a face-to-face meeting. If a system is used which the data controller does not operate itself, but which is operated by a service provider who may be based outside Europe, it must also be ensured that any 'data collection' by the service provider takes into account the data protection requirements applicable in Europe.

Notes on selection and operation

In early April 2020, I posted guidance on my website on how to select and securely operate messenger and video conferencing services. I placed particular emphasis on the aspects of transparency, security and controllability. The responsibility for the privacy-compliant use of a service lies largely with the users, even if a service is used that is operated centrally by a provider. I also provided users with a set of guiding questions to help them evaluate and select appropriate offerings.

Guidance from the Data Protection Conference

Over the year, the Conference of Independent Federal and State Data Protection Supervisory Authorities (Data Protection Conference) developed guidance on the use of video conferencing systems, which was published in October 2020. This guidance is supplemented by a checklist which helps controllers to not disregard any relevant aspects when selecting and using video conferencing systems. The guidance explicitly addresses employee data protection, which plays an important role, especially when video conferencing systems are used when working from home or in mobile work.

Circular to the federal administration on WhatsApp

After I received individual tips at the start of the coronavirus crisis criticising the use of WhatsApp by federal administration agencies, I clarified in a circular to all top federal agencies in April 2020 that federal agencies should refrain from using WhatsApp. The transmission of metadata to WhatsApp and, in a second step, also to Facebook, always provides a contribution to profiling by Facebook. This is unacceptable for public authorities, which are particularly bound by compliance with the law and have the function of a role model in this context.



Use of a publicly available service or in-house operation?

A central question in the use of video conferencing or messenger systems is the choice between using a commercial, publicly available service and operating a corresponding system in-house. While the in-house operation of a system gives controllers full control over practically all data protection-relevant parameters on the one hand, it also places complete responsibility for secure and high-performing operation on them on the other. The technical and organisational effort required to set up and operate an in-house service is considerable. The use of publicly available, commercial offers, on the other hand, is often quicker to implement and involves less effort.

However, it is precisely offers that can be used particularly quickly and easily that are often particularly problematic. These centrally operated services only require only the installation of an app on a mobile device or a client application on a notebook. However, it is usage data could possibly also be collected by the relevant providers, from which profiles can be created that may be used for their own purposes. The providers are called upon to provide more transparency here. If a service gives the option to share files or to record conversations or sessions, this is always problematic if the corresponding content is stored on the provider's infrastructure, possibly unencrypted. Transparent information must also be provided on the question of whether or how data streams are protected on the way from the clients to the server.

4.1.7 Delivery of parcels under pandemic conditions

The coronavirus pandemic has greatly increased the volume of parcel deliveries. With the requirement of contactless delivery, some variants of handover documentation collided with data protection requirements in the early days.

The delivery of parcels, the volume of which had increased dramatically as a result of shop closures, also had to be adapted to the required distancing rules. Deliveries with a signature on a hand scanner and the associated device and pen had to be replaced. As such, parcel service companies in Germany adjusted their processes in the spring: from then on, instead of having the items acknowledged by signatures, the deliverers were to, for example, photograph the signature of the person receiving the parcel.

Several citizens reported to me that in addition to their signature on the package, their ID was also photographed as part of the delivery process. In individual cases, employees of parcel service companies photographed the recipient with their parcel for documentation purposes and transferred these images to the company's own systems.

The incidents reported to me were usually confirmed by the parcel service companies concerned when the facts of the case were clarified, naturally combined with confirmation of the erasure of the personal data which was collected unlawfully. Photographs of identity cards or pictures of recipients undoubtedly go far beyond what is permitted by law. Collecting and storing them is a clear violation of the GDPR.

This also applies to postal service workers: appropriate training and sensitisation of employees with respect to the legal requirements prevents data protection violations.

4.1.8 Federal emergency or bridging assistance programmes in connection with the coronavirus pandemic

At various points, I was involved in the implementation of the Federal Government's programmes to overcome the negative economic impact of the coronavirus pandemic. This has shown how important it is for my institution to be involved in data protection issues at an early stage.

The Federal Government responded quickly to the economic impact of the coronavirus pandemic with financial stabilisation measures for the economy. To this end, existing mechanisms have been expanded or new programmes launched, such as the stabilisation measures under the Large State Guarantee Programme (Großbürgschafts-Programm) and the Economic Stabilisation Fund (Wirtschaftsstabilisierungsfonds). In addition, a programme of bridging aid was set up for small and me-

dium-sized enterprises that had to cease all or most of their business operations in the wake of the coronavirus crisis. A common feature of all these programmes is that personal data of a wide variety of persons involved in the procedures is regularly processed during the relevant application procedures.

Precisely because of the need for rapid implementation and the complex data protection issues that have to be taken into account, I would have liked to see early involvement in these projects so that the procedures could be placed on a sound basis in terms of data protection law. However, this was not consistently the case.

As a positive example, I would like to highlight the new bridging aid programme for small and medium-sized enterprises that have had to cease all or most of their business operations in the wake of the coronavirus crisis. The Federal Ministry of Economics and Technology (Bundesministerium für Wirtschaft und Energie, BMWi) approached me at an early stage to obtain my expertise in the planned procedural steps. The administrative implementation of this programme should be carried out by the states as closely as possible to citizens. Therefore, I regularly informed my colleagues in the states about the programme, so that a complete follow-up by the competent data protection authorities could be ensured. In addition, I was able to advise the BMWi not only on data protection issues in connection with the involvement of the tax authorities and auditors, but also on the 'Bridging aid online application' procedure platform that was set up. To this end, the BMWi presented a comprehensive data protection concept, a list of processing activities and a data protection impact assessment, all of which showed a pleasing level of awareness with regard to the consideration of necessary aspects of data protection law.

By contrast, I only became aware of the stabilisation measures under the Large State Guarantee Programme and the Economic Stabilisation Fund when they were already being implemented by the BMWi. In particular, I would have liked to have been able to comment from the outset on the involvement of third parties as mandataries in the application processes to be carried out. I do not understand the delimitation of responsibilities under data protection law chosen here, which deviates from the decision-making power of the individual parties in the application procedure. However, a clear allocation of responsibilities is particularly important for the effective exercise of data subjects' rights. I am therefore still in further coordination talks with the BMWi on this point.

4.1.9 Corona-related changes in employment services

A hasty legislative procedure regarding simplified access to benefits under Book II of the Social Code (Sozialgesetzbuch Zweites Buch, SGB II; Social Protection Package I) leads to uncertainty with respect to data protection issues.

In order to cushion the social and economic consequences of the measures to contain the coronavirus in the spring of 2020, the Social Protection Package I introduced regulations to facilitate access to basic security benefits under the SGB II, with validity for funding periods from 01/03/2020. According to the justification given for the Act (BT printed matter 19/18107), the aim of the Act was to make benefits available quickly and unbureaucratically in a simplified procedure in order to be able to support data subjects in a timely manner. No one should face existential hardship because of the economic impact of this crisis. The simplified procedure was necessary to support the work capacity of job centres. The legislative procedure was fast-tracked. The consultation of associations normally provided for in the legislative process did not take place; I was involved, but with such a short deadline that I was unable to examine the draft law in a comprehensive way. Although I recognise the urgency of the proposed legislation in a crisis situation, I believe that this expedited procedure overstretches the principles of the rule of law, particularly as there could also be early and thus parallel participation in such cases. I refer to the critical statement of the Deutscher Sozialgerichtstag (German Social Court Conference) of 25 March 2020 on the draft law, which I endorse on this point.

One of the provisions of Social Protection Package I is that assets are not taken into account for a period of six months, but this does not apply if the assets are substantial. It is presumed that there are no substantial assets if the applicant declares so in the application. It remains unclear to what extent it follows from the legal provision that no assets are to be taken into account that no assets verification should take place at all. The explanatory memorandum to the Act does not provide any specific details either. The aim of the legislative proposal was to make the often complex and time-consuming asset verification process quick and unbureaucratic, without generally dispensing with asset verification.

This issue, which is in itself a matter of legal performance, has serious implications for data protection law. The regulation led to uncertainty among some claimants, as some job centres nevertheless continued to request documents required to verify the existence of income and assets. In particular, as before, the submission of bank statements for the last few months was requested. If, however, asset verification is fundamentally inadmis-

sible, the regular request for account statements is also not compatible with the data protection principle of data economy. Job centres may only process data required to carry out their legal tasks.

This led to considerable uncertainty and an increased volume of enquiries sent to me. The information provided on the website of the Federal Ministry of Labour and Social Affairs (Bundesministerium für Arbeit und Soziales, BMAS) was not suitable for removing this uncertainty. In principle, in my view, the job centres were right to require the submission of documents justifying entitlement, such as bank statements for the last three months. The purpose of the amendment to the law made by the social package is not to generally exclude the asset verification as such. It is simply a question of simplifying administrative procedures so that benefits can be paid more quickly. Reviewing bank statements for the last three months does not significantly delay the administrative procedure. Moreover, this is necessary in order to be able to verify, at least to a limited extent, the information provided in the application procedure, despite simplified asset verification. In addition, bank statements are not only needed to verify assets, but also to prove what income has accrued to the claimants. In fact, the Federal Employment Agency (Bundesagentur für Arbeit) points out the obligation to submit account statements despite the simplifications (<https://www.arbeitsagentur.de/corona-faq-grundsicherung-arbeitslosengeld-2>). A clearer legal regulation as well as a more detailed explanation of the regulations by the BMAS or the Federal Employment Agency and the job centres could have helped to avoid these uncertainties.

4.2 The Patient Data Protection Act

The Patient Data Protection Act (Patientendaten-Schutz-Gesetz, PDSG) entered into force on 20 October 2020. It contains extensive regulations on the electronic health record (EHR) and violates the General Data Protection Regulation (GDPR) through its specific form of access management. I also take a critical view of the alternative access to the EHR by means of mobile devices (smartphone, etc.), i.e. without using the electronic health card (EHC), as well as regulations on electronic medical prescriptions (ePrescriptions, or 'eRezept' in German). The ePrescription is the first 'mandatory application', i.e. the PDSG contains specifications that are mandatory for all persons covered by statutory health insurance. Another important provision in the PDSG allows insured persons to release data in the EHR for research. Within this context, there is a lack of important

specifications that must be made by the legislator—and not in downstream processes.

Digitalisation in the healthcare sector will be further advanced through the PDSG. The telematics infrastructure (TI) concept developed for this purpose is intended to ensure data protection and data security. In the justification to the PDSG, the legislator rightly emphasised the preservation of patient sovereignty as one of the most important requirements. Despite this central premise of the PDSG, the goal of informational self-determination



The telematics infrastructure (TI) networks all parties in the healthcare system in the area of statutory health insurance and ensures the secure exchange of information across sectors and systems. It is a closed network to which only registered users (persons or institutions) with an electronic health professional and practice card have access. In order to meet all data protection requirements and, in particular, to protect patients' medical data, the telematics infrastructure relies on strong information security mechanisms.

for insured persons is missed, especially in probably the largest project of the law, the EHR.

Law establishes responsibility under data protection law

TI applications and components are planned, developed and operated by a large number of contributors. It is therefore important to clearly allocate responsibility under data protection law. Only in this way can data subjects exercise their rights and authorities exercise their supervision effectively. Therefore, in September 2019, the Conference of Independent Federal and State Data Protection Supervisory Authorities (Datenschutzkonferenz, DSK) adopted a resolution on its view of data protection responsibility in the TI (see no. 4.2.1 of the 28th AR). Accordingly, gematik, as the central and planning body of the TI, bears sole responsibility under data protection law for the central zone of the TI and joint controllership for the decentralised zone. The PDSG now explicitly regulates responsibilities. In contrast to the view of the DSK, however, the legislator limits the responsibility of gematik (see Section 307 (5) of SGB V). gematik is only responsible under data protection law insofar as it determines the means of processing personal data and there is no responsibility on the part of the other—solely responsible—parties (see Section 307 (1) to (4) of SGB V).

gematik must set up a coordinating body that provides information on responsibilities to data subjects. The standardisation of complete responsibility under data protection law for data processing in the TI and the establishment of a coordinating body for the provision of information to data subjects are to be welcomed in principle. However, the legally regulated sole responsibility of the providers of applications also harbours problems, as the example of the EHR shows.

Electronic health record violates the GDPR

EHR access management standardised in the PDSG violates the GDPR and the fundamental rights of the persons insured. For example, when the EHR launches on 1 January 2021, insured persons will not have full sovereignty over their own data concerning health. This means, for example, that in 2021 insured persons will be unable to restrict their doctor's access to individual documents required for treatment. The insured person only has the choice of either granting service providers (e.g. doctors) authorisation to access all stored data (findings, diagnoses, therapy measures, etc.) and all documents they have personally entered into the EHR, or denying this authorisation altogether. So the all-or-nothing principle applies. This means that any person who is granted access to a medical document or a document personally posted by the insured person can view all the information in the EHR in each case, even if this is not necessary for the treatment in question. The PDSG only provides for an improvement from 2022 onwards. However, this only applies if you are using a mobile device (e.g. smartphone, tablet). From this point on, document-specific access could then be granted via smartphone or tablet.

This does not cover the large group of people who do not own a device or do not want to use one. These insured persons will continue to have their patient sovereignty restricted. You can only grant limited access rights to categories of documents with the service provider, e.g. in the medical practice. Alternatively, they may grant rights of representation to a representative using a suitable technical device. Only the representative can then grant document-specific authorisations for these persons. This means that insured persons must disclose to the representative all health information held in their EHR, including intimate information. In addition, the representative does not help insured persons who, for security reasons, for example, deliberately do not want to use a smartphone or tablet to manage their EHR—and thus no corresponding device belonging to a representative.

Another critical aspect in terms of data protection law is that the large number of people who do not have or do not want to use their own device will not be able to view their own EHR, which they will have to manage them-

selves, in the long term. They will therefore be excluded from using the EHR in this way. Thus, this group of people also cannot benefit from the advantages of an EHR in healthcare.

These serious restrictions on patient sovereignty contradict elementary requirements of the GDPR and thus violate European law which is directly applicable in Germany. I have repeatedly pointed this out from an early stage, including during the legislative process. My proposed solutions were not taken into account or were removed from the bill in the parliamentary proceedings. This concerns, for example, the installation of point-of-sale terminals in health insurance provider offices, which insured persons that don't have their own device and those who do not wish to use their own device could use to access to their EHR within the secure TI environment.

By discriminating against and treating this large group of insured individuals unequally, the PDSG creates a two-tier society in the EHR.

The federal and state data protection supervisory authorities have also publicly expressed this criticism in a resolution adopted in September 2020.

Another central point of criticism under data protection law is the EHR authentication procedure of the with own terminals, which does not meet the requirements of the GDPR. Because health data is particularly sensitive, access to the EHR always requires highly secure authentication procedures that must always be in line with the latest state of the art. The 'alternative insured person identity' procedure, through which insured persons can log in to their EHR without using the EHC, is based on a signature service and does not fully meet these security requirements. In order to ensure that data protection is complied with, the highest possible level of security must also be guaranteed for this alternative authentication. This guarantee is also the responsibility of health insurance providers. Because of this shortcoming, too, supervisory measures may have to be taken against health insurance providers to ensure that they are replaced by a more appropriate procedure.

In the second/third reading of the PDSG on 3 July 2020, Federal Minister of Health Spahn correctly emphasised in the Bundestag that '(...) data protection is important for data as sensitive as data concerning health, and data protection of the highest level. There is nothing more sensitive for the individual, nothing more personal, more intimate than the data about one's own health and especially a possible illness. That is why we are setting data protection standards at the highest level in this Patient Data Protection Act (...)'.

Also and in particular in my role as data protection

supervisory authority, I am obliged to work towards the elimination of GDPR violations.

Implementation of the EHR exclusively according to the requirements of the PDSG is contrary to European law and therefore requires the imposition of supervisory measures. Accordingly, in November 2020, I sent a formal warning to the statutory health insurance providers under my supervision for offering an unlawful EHR to persons insured with them.

Health insurance providers face a dilemma due to the sole responsibility for the EHR assigned to them by the legislator. If they refuse to implement the EHR in accordance with the requirements of the PDSG, they will be threatened with heavy fines laid down by law in the PDSG. If, on the other hand, they implement the law that is contrary to European law, i.e. if they offer their policyholders an EHR that is contrary to European law, they will come under the scrutiny of supervisory authorities. Ultimately, only the legislator can remedy this situation.

The first mandatory application: the electronic medical prescription

The PDSG introduces a new application with the regulations in Sections 360 and 361 of SGB V. Medical prescriptions must be transmitted electronically via the TI from 1 January 2022. The ePrescription (or 'e-Rezept' in German) is thus a mandatory application—and the first medical one ever.

Prescriptions within the scope of SHI-accredited healthcare should always be stored in a central repository in the TI. Patients will then only be able to choose whether they want to receive access information in electronic form or—along the lines of a train or airline ticket—as a paper printout with a code block to be redeemed at a pharmacy.

As with the EHR, there will be a two-tier society with the ePrescription. Anyone who does not want to or cannot use the ePrescription app will not have direct access to the data stored about them or to their prescriptions.

For authentication in the ePrescription app vis-à-vis the ePrescription server, the PDSG does not provide for the use of an alternative procedure without an EHC. Users will therefore link their EHC to the terminal device via near field communication (NFC). Here, a contactless data exchange takes place over a short distance of a few centimetres. As part of the introduction of the ePrescription application, an identity provider will be set up in the TI—a service that will initially only authenticate users and confirm identification for the ePrescription, but could later potentially do so for all TI applications. Thus, the central topic of authentication is to be outsourced from the applications. This is advantageous for the introduction and security evaluation of authentication



Resolution of the Conference of Independent Federal and State Data Protection Supervisory Authorities—01/09/2020

Patient Data Protection Act: without any data protection improvements for the insured person, this is contrary to European law!

On 3 July 2020, the German Bundestag passed the Patient Data Protection Act (Patientendaten-Schutz-Gesetz, PDSG) in defiance of criticism voiced by the independent federal and state data protection supervisory authorities. Criticism is directed in particular at access management, which is only designed in a rough, granular way, authentication for the electronic health record (EHR) and the representative solution for insured persons who do not have a suitable device.

The PDSG is scheduled for final consideration by the Federal Council on 18 September 2020.

Central legal regulations are in conflict with elementary requirements of the EU General Data Protection Regulation (GDPR). Contrary to the current draft, insured persons must already be given full sovereignty over their data when the EHR is introduced on 1 January 2021. This also corresponds to the requirements formulated by the legislator itself in the PDSG to preserve patient sovereignty via the insurance-managed EHR without restrictions and to design the use of the EHR for all insured persons in accordance with data protection.

The bill does not achieve these goals. When the EHR is launched, all users will be forced into an ‘all-or-nothing’ approach with regard to the data stored by healthcare providers (doctors, etc.) in the electronic health record, as no document-level control is envisaged for this data in 2021. This means that parties to whom the insured persons grant access to their data will be able to see all the information contained therein, even if this is not necessary for the specific treatment situation.

Just one year after the launch of the EHR, i.e. from 1 January 2022, only insured persons who use devices (smartphone, tablet, etc.) suitable for accessing their EHR will be able to independently carry out document-specific control and rights assignment in relation to such documents.

All other insured persons who do not own appropriate devices or do not want to use them for security reasons to protect their sensitive health data (i.e., ‘non-front-end users’) will not be granted these rights beyond the 1 January 2022 deadline. From 1 January 2022, the PDSG in this respect only allows non-front-end users a representative solution. They can then exercise their rights by means of a representative and their mobile device. However, in the case of representation, insured persons would have to grant their representative full access to their health data.

Another point of criticism is the authentication procedure for the EHR and the ‘guarantee of the necessary high level of data protection’. Since the data in question is health data and thus highly sensitive personal information, the requirements of the GDPR stipulate that authentication must ensure the highest possible level of security in line with the state of the art. This applies in particular to authentication procedures without the use of the electronic health card. If alternative authentication methods are used that do not meet this high standard, this constitutes a breach of the GDPR.

In its opinion on the PDSG of 15 May 2020 (BR printed mater 164/1/20, see no. 21. on Article 1 no. 31 [Section 334 et seq. of SGB V-E9]), the Federal Council pointed out to the Federal Government considerable concerns with regard to the conformity of the PDSG with the GDPR. Its criticism essentially refers to the lack of detailed access management on launch of the EHR and the resulting restriction of the data sovereignty for the insured person. It has called on the Federal Government to comprehensively review in the further legislative process in particular the regulatory proposal on the offer and establishment of the EHR (Section 342 of SGB V) with regard to data protection concerns.

Also in light of this, the independent state and federal data protection supervisory authorities call on the Federal Council, on the occasion of its deliberation scheduled for 18 September 2020, to call on the Mediation Committee in order to obtain necessary improvements to the PDSG under data protection law during the legislative process.

means. In order to make use of these advantages in a privacy-compliant manner, I call for the processes for introducing authentication means to be developed in advance for the entire TI and for the criteria for classifying the security levels to be defined in a transparent way. Such central functionality for TI security must also be regulated across the board and must not merely be an annex to ePrescription development.

With ePrescriptions, another paradigm shift is also taking place: gematik is developing the ePrescription app and will make it available. gematik's task is therefore not limited, as is the case for the EHR, to drawing up specifications and security requirements according to which manufacturers must offer TI components or services. gematik itself becomes the manufacturer and thus also responsible for data protection. This has the consequence that gematik is required to check and approve its own developments. In this respect, there is at least a risk of potential bias. As part of the legislative consultations, I was at least able to achieve that an external security report must be commissioned by gematik and this must be checked and confirmed by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) before the app is allowed to go into operation.

The availability requirements for the ePrescription are of course very high and also of central importance. During the design process, I had pleaded for a decentralised solution. This could have been made more robust with respect to central services failing. In the assessment—including, among other things, the protection against manipulation and prescription trading—the valid specified central solution ultimately prevailed.

In all of the aspects mentioned, the importance of my repeatedly and early expressed demand to anchor the central aspects of the application of the ePrescription in the law is shown. For a compulsory application such as the ePrescription, the legislator must make central decisions and provide guard rails in the law without committing to a specific technology. Unfortunately, this was not implemented, so central questions are now decided downstream by gematik, in particular within the framework of the technical specifications. Among other things, the PDSG lacks regulations on purpose limitation, data storage and technical principles and control options for all insured persons. Thus—and within the context of the outstanding importance of the application for healthcare security—the regulations for the introduction of the electronic prescription do not have sufficient legal clarity and need to be supplemented. Only with regard to the standardisation of a regulation on the storage period of ePrescriptions did the legislator follow my petition in the PDSG. The concrete design of the ePre-

scription application must also be measured against the requirements of the General Data Protection Regulation. In addition to data security measures, the focus of the review will also be on ensuring availability.

Release of EHR data for research, Section 363 of SGB V.

Another important new provision in the PDSG allows insured individuals to release data stored in their EHR for medical research. I was already able to achieve significant improvements here in the departmental consultation, such that from 2023, this valuable and coveted health data can be used in a way that complies with data protection requirements. Research with health data is of considerable importance to society. On the other hand, this data is particularly sensitive. Processing of it is subject to special requirements and protective measures in accordance with Section 363 of SGB V. These include disclosure being voluntary and only permissible at the instigation of the insured person and with their explicit consent, which may be withdrawn at any time. The scope can also be freely determined and limited to selected documents. In addition, data is transmitted pseudonymously and encrypted in order to protect the data subjects.

The regulation contains two different ways of release for research, which differ with regard to their evaluation under data protection law: on the one hand, it is possible to release the data to the Research Data Centre (Forschungsdatenzentrum, FDZ) at the Federal Institute for Drugs and Medical Devices (Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM), which then makes the data available for research purposes; on the other hand, it is planned to release the data directly to the research community.

Research Data Centre

When released to the FDZ, the data is stored there and made available for research once the prerequisites have been checked. The procedure is based on the specifications for the use of healthcare data that is held at the FDZ on the basis of the data transparency regulations of Sections 303a et seq. of SGB V. These provisions were rewritten by the Digital Healthcare Act (Digitale-Versorgung-Gesetz) in December 2019, which I reported on in my 28th Activity Report (no. 5.6, p. 45).

This results in a regulated application procedure with explicitly named authorised users and specifically named permissible purposes. The FDZ examines the suitability and necessity of the requested data in terms of scope and structure in relation to the intended purpose. It is also important for the protection of the data that authorised users are obliged to maintain secrecy and are liable to prosecution in the event of infringement. However, I

was able to get a reduced group listed as eligible to use EHR data compared to data transparency: only persons whose tasks actually include research.

In accordance with the provisions of the data transparency regulations in Section 303a et seq. of SGB V, data is also transmitted via a trust centre.

In principle, this concept of release to the FDZ complies with data protection requirements. Unfortunately, the Federal Ministry of Health has not followed up my previous suggestions to establish the FDZ at an independent agency. Due to the importance of medical research and the high sensitivity of the medical data concerned, an independent body should be entrusted with this task in order to gain the trust of insured persons in this way.

Direct release for scientific research

Unfortunately, when releasing directly to research, there are no requirements other than consent. From a data protection perspective, I also take a critical view of the concept of consent being overstretched. Consent for 'specific areas of scientific research', as provided for in Section 363 (8) of SGB V, is only permissible under certain conditions. In principle, voluntary consent can only be given if the purpose of processing is specifically described. Broad consent is only exceptionally provided for in the GDPR if a precise description is not possible. But even then, the purpose must be described as precisely as possible. Further explanations by the DSK on the requirements for broad consent can be found in its decision of 5 April 2019, which I reported on in my 28th Activity Report (no. 4.5.1, p. 34). Despite my advice, however, the necessary requirements are missing from the statutory scheme. In the consultations on technical implementation, I will continue to advocate that improvements and measures for the procedural safeguarding of data transmission be implemented in order to achieve release and use that is permissible under data protection law.

Amendment of Section 68b of SGB V

Section 68b of the SGB V was also amended by the PDSG. This standard, which was already created by the Digital Healthcare Act (Digitale-Versorgungsgesetz, DVG), opens up the possibility for health insurance providers to promote healthcare innovations. To this end, they may evaluate insured-related data they have lawfully collected and stored to the extent necessary. Prior to this, the data must be pseudonymised and—as far as possible—anonymised. Data transfer to third parties is excluded.

According to the original version of the DVG, health insurance providers were only allowed to evaluate insured person data and provide information and individual offerings if the insured person had previously consented to this in writing or electronically. With the PDSG, this

consent requirement has now been replaced by a right of objection with regard to the evaluation of data and the submission of individual healthcare offerings, which only relates to the specific submission of offerings.

I am extremely critical of this change. With the complete abolition of the consent requirement and the lack of an objection option with regard to data evaluation, vulnerable groups among the persons insured are particularly exposed to evaluations by health insurance providers. In my opinion, genuine voluntary participation in the healthcare offerings should be linked to the fact that the insured persons can decide in advance against the inclusion of their data in the evaluation for the purpose of offer submission.

During the legislative process for the PDSG, I did not have the opportunity to comment on the version of Section 68b of SGB V that is now in force. This amendment was only adopted after the departmental vote in the final phase of the parliamentary proceedings. For this reason, I have subsequently expressed my concerns to the BMG in order to achieve a privacy-compliant adaptation of Section 68b of SGB V in one of the ongoing legislative processes. Furthermore, I reserve the right to take supervisory measures against health insurance providers with regard to the concrete implementation of procedures, insofar as these do not comply with the General Data Protection Regulation.

Information texts according to Section 343 of SGB V - agreement with the BfDI

The PDSG also introduced a new Section 343 into SGB V. This obliges health insurance providers to provide comprehensive, suitable information material in a precise, transparent, comprehensible and easily accessible form, in clear, simple language, without any barriers, before they offer their insured persons an electronic health record in accordance with clause 1 of Section 342 (1) of SGB V.

The information must detail:

- all relevant circumstances of data processing for the establishment of the electronic health record;
- the transmission of data to the electronic health record;
- the processing of data in the electronic health record by healthcare providers, including the related data processing operations in the various components of the telematics infrastructure; and
- the controllers responsible for data processing under data protection law.

The National Association of Statutory Health Insurance Funds (Spitzenverband Bund der Krankenkassen, GKV-SV) has been obliged under Section 343 (2) of SGB V to

assist the health insurance providers in fulfilling their information obligations by producing suitable information material—including in electronic form—and making it available to health insurance providers for mandatory use. It shall prepare such information in agreement with me, with an agreement to be reached no later than 30 November 2020 (Section 343 [2] of SGB V).

Following in-depth consultations, the GKV-SV presented a version of the information texts to which I declared my agreement in good time before the deadline.

Cross-reference: 5.7 Data Transparency Regulation (Datentransparenzverordnung)

4.3 Implementation of the Schrems II Judgment of the European Court of Justice

The Schrems II Judgment of the European Court of Justice (ECJ) has caused quite a stir: from the declaration of invalidity of the Privacy Shield, to standard contractual clauses that will generally no longer be readily applicable, to the 'additional measures'. The massive impact on international data transfers to third countries is clearly of note for controllers and processors and entails high implementation requirements, not least for supervisory authorities.

The Schrems II Judgment

I had already reported on the ongoing 'Schrems II' proceedings in my last activity report (ECJ: Case C-311/18)¹. The case concerned whether the applicable standard contractual clauses were sufficient for the transfer of personal data to the US. Standard contractual clauses are the most widely used instrument used in practice to demonstrate the appropriate safeguards necessary for a transfer to a third country. It was also expected that the ECJ would rule on the effectiveness of the Privacy Shield².

On 16 July 2020, the ECJ finally delivered the landmark Schrems II Judgment, in which it declared the provisions of the Privacy Shield invalid. For data transfers to the USA, the abolition of the Privacy Shield meant a drastic change. Furthermore, the ECJ has once again clarified that personal data of EU citizens may only be transferred to third countries if they enjoy an essentially equivalent level of protection in this third country as in the EU. In

doing so, the ECJ did not fundamentally question the instrument of standard contractual clauses. However, the court stated that these would have to be supplemented, where necessary, by 'additional measures' so that the data enjoys substantially equivalent protection in the third country as in the EU. For the US, the ECJ has already found that standard contractual clauses cannot provide this equivalent level of protection without additional measures. Similarly, the impact of the judgment on other third countries as well as on other transfer instruments under Article 46 of the GDPR, e.g. binding corporate rules—BCRs, which have already been transparently elaborated by the European Data Protection Board (EDPB), should not be underestimated. In addition to the publications already released, the EDPB will publish further details on the impact of the judgment on the BCR (Art. 46 [2] [b] of the GDPR) and the ad-hoc contractual clauses pursuant to Article 46 [3] [a] of the GDPR as soon as possible.³

Implementation

The ECJ also made a clear assignment of tasks. Companies and public bodies are obliged to check the lawfulness of data transfers to third countries on their own and to adapt them if necessary. They are advised and monitored by supervisory authorities when doing so.

Immediately after the judgment, I began working with my colleagues at a national and European level to develop guidance for data controllers and processors (data exporters).

Furthermore, on 8 October 2020, I addressed an information letter on the 'Impact of ECJ Case Law on International Data Transfers' to federal public agencies as well as companies subject to my oversight and additionally published it on my website.⁴ In it, I summarised the key statements of the judgment and clarified how my department intends to meet ECJ requirements. I therefore drew the attention of the data exporters to their obligation to check the transfer of data to third countries and also drew attention to when there was an obligation to notify me. I will evaluate the responses from companies and public authorities under my supervision to the information letter and subsequently ask them specifically about direct data transfers in specific areas. Furthermore, the implementation of the Schrems II Judgment will be a regular focus of future advisory and inspection visits.

On my website, I also support data controllers and processors with up-to-date information on the subject,

1 The ECJ's Schrems II Judgment of 16 July 2020, Case C-311/18

2 Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the EU-US Privacy Shield.

3 Schrems II recommendations from the EDPB v. 10 November 20, available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

4 Information letter from the BfDI, available at: <https://www.bfdi.bund.de/rundschreiben>

e.g. a summary of the key statements of the Schrems II Judgment, a checklist on transfers to third countries and links to relevant websites (e.g. the EDPB website).⁵

In the EDPB, with my cooperation and that of other German supervisory authorities, it was possible to develop rapid assistance for data exporters just a few days after the judgment was announced. Part of this includes frequently asked questions (FAQs) on the judgment of the Court of Justice of the European Union in Case C-311/18—Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems.⁶ It also includes recommendations on ‘additional measures’ (‘Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data’)⁷ which were adopted in the EDPB on 10 November 2020. The recommendations are intended to help data exporters determine whether they need to add additional measures to their data transfers. The recommendations also provide practical examples of transmission scenarios.

The Schrems II Judgment meant that the ECJ presented data exporters, but also data protection supervisory authorities, with no small task. The work on implementing the Schrems II requirements is likely to keep everyone busy at a national and European level for some time to come. I will continue to support and promote the implementation of the ECJ’s Schrems II Judgment, in particular by advising companies and public authorities that transfer data to third countries.

⁵ Information on the BfDI website, available at: https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/Auswirkungen-Schrems-II-Urteil.html

⁶ FAQs adopted by the EDPB on 23 July 2020 available at: https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_en

⁷ Schrems II recommendations from the EDPB v. 10 November 20, available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

5

Legislation

5.1 Register modernisation

Register modernisation is a central building block for future-oriented modern administration. However, the use of the tax ID as a uniform and overarching personal identifier, which has been planned so far in the draft of the register modernisation law, faces considerable constitutional concerns and thus fundamentally calls the project into question.

I already commented on the modernisation of the register in my last two activity reports (see no. 5.5 of the 28th AR and no. 9.2.2 of the 27th AR) and made it clear how important it is for the necessary further digitalisation of the administration to be designed in a constitutional way. Last but not least, data protection also benefits from modern infrastructures and procedures.

However, with a uniform, cross-sector personal identifier such as the tax ID, which is provided for in the 2020 draft Register Modernisation Act (Registermodernisierungsgesetz, RegMoG), which currently being discussed by the Bundestag, the legislator is missing the opportunity to design an identifier in such a way that it meets the requirements of modern administration and protects the population and peoples' constitutional right to informational self-determination. Instead of broad approval for what is potentially a major step forward in digitalisation, which was quite tangible due to the very early involvement of the Data Protection Conference and my authority in the preparation of the draft law, the project now faces fundamental criticism from many sides.

In its resolutions of 12 September 2019 and 26 August 2020, the Data Protection Conference expressly warned against using the tax ID as a personal identifier in this way and completely detaching it from its original purpose. The Federal Council (BR printed matter 563/20) and the Bundestag's Academic Services (Wissenschaftliche Dienste des Bundestages; WD 3 - 3000 - 196/20) also recognised the constitutional danger posed by the draft of the RegMoG submitted. Even previous use in the tax area would no longer be secure.

In this sense, I have tried in my statements on the draft law (see, among others, my statement to the Bundestag's Committee on Internal Affairs of 21 October 2020 www.bfdi.bund.de/stellungnahmen) to raise awareness of the urgency of a secure and constitutional design. What is clear is that the functioning modernisation of registers will not be possible without a legally secure and unambiguous identification of individual persons. But a universal identifier like the tax ID, which carries the high risk of being thrown out by the Federal Constitutional Court following years of litigation, has the potential to set digital administration in Germany back years. Even if it should endure in one form or another, how would this damage trust in this tool? This is also because when the tax ID was introduced in 2007, the explicit assurance was given that it would in any case be limited to the tax area and never used as a general personal identifier.

Need for improvement

That is why, in my view, the current draft needs to be improved in the following areas:

the draft must move away from the idea of expanding the tax ID to become a uniform, cross-domain personal identification number, especially since the tax ID does not offer sufficient protection against misuse. There are more modern alternatives with area-specific identifiers or further cryptographic methods.

The law must also guarantee robust purpose limitation for the identifier: it may only be used to establish identity for the provision of digital administrative services. This has not been ensured in the draft so far, precisely because according to the general regulations of the GDPR, purpose-changing uses can be found and the identifier can therefore spread uncontrollably. First in public administration, then eventually in society and the private sector.

The bill also does not yet take sufficient precautions to ensure that the exchange of data between different administrative areas is adequately protected against misuse, identity theft and profiling. The '4-corner model'

is a good approach though, using encrypted 'double envelopes' and using a third party for transmission authorisation. However, this alone is not sufficient to adequately contain all relevant risks. The model can be circumvented with abusive intentions and also does not adequately protect against the aggregation of personal data by external attackers. In addition, contrary to the announcements made by the coalition committee on 3 June 2020, the 4-corner model is to be used solely for cross-sectoral transmission, disregarding the state of the art. Since it is already apparent that only a few large administrative areas will be formed, the 4-corner model will therefore not be used at all for a large proportion of data transmissions.

Consequently, the tax area must not be excluded from the necessary security measures. With the introduction of the planned identifier, this area will ultimately also use a general personal identifier; the singular tax ID in the previous sense will essentially cease to exist.

Finally, data protection must also be further developed for administrative digitalisation. The data cockpit included in the draft is an important and good first step in creating transparency. However, the further development of this tool should be considered from the outset in order to ultimately bring citizens on an equal footing with the state. If the state can retrieve data in a matter of seconds, then data subjects must not only be able to understand this, but must also be able to take the reins on this. Only the possibility of being able to retrieve one's own data from state registers and databases ultimately creates a kind of equality.

Cross-reference: 3.1.2 Implementing constitutionally compliant register modernisation

5.2 Administrative digitalisation is progressing

The digitalisation of administrations at a federal and state level is being prioritised and vigorously pursued in politics. The coronavirus pandemic has further accelerated this development.

The Act on the Digitalisation of Administrative Procedures in the Granting of Family Benefits (Gesetz zur Digitalisierung von Verwaltungsv Verfahren bei der Gewährung von Familienleistungen, DigFamG) also amended the Online Access Act (Onlinezugangsgesetz, OZG). These are intended to increase the willingness of citizens and companies or other legal entities to use administrative services digitally rather than using the traditional analogue method. The coronavirus pandemic is not only

accelerating this development. It is also showing how important it is to create this digital offering.

It is important to me that the use of digital administrative services remains voluntary, i.e. that their use of them is not something that is forced. It must still be possible in the foreseeable future to carry out administrative business in the same way on site. Citizens must have free choice in this regard. In addition, they must be able to transparently trace who is processing their personal data, for what purpose, how, where and for how long, at any time. One tool that could support them in this respect is the planned data protection cockpit (see no. 5.1 Register modernisation).

Interoperability of citizen accounts

With the OZG, the Federal Government has created the prerequisites for networking the administrative portals of the Federal Government, the states and the municipalities. Citizens should be able to access all online administrative services via an administrative portal of their choice without having to identify themselves more than once (single sign-on, SSO). To allow the necessary interoperability of the services offered by the Federal Government, the states and the municipalities, the Federal Government and the states have concluded an administrative agreement which provides for the operation of the services and components required for interoperability by a body at the Free State of Bavaria. At my instigation and that of my colleagues in the states, this agreement also includes regulations on the exercise of joint controllership for the processing of personal data pursuant to Article 26 of the GDPR. This means, for example, that data subjects can always find a contact person to exercise their data subject rights.

Interoperability of user accounts requires a binding framework for assessing the trustworthiness of identification systems that provide access to all federal, state and municipal services. This legal framework was established at a European level through Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions (eIDAS Regulation). In accordance with the eIDAS Regulation, the OZG provides for the use of means of identification for the trust levels 'low', 'substantial' and 'high'. So far, only the ID card with an eID function is suitable for the 'high' level. In addition, the possibility of using ELSTER software certificates to prove identity in the user accounts of both natural persons and organisations will be created for a limited period of time. Until 30 June 2023, ELSTER software certificates will be recognised for the trust level 'substantial'. It is encouraging that the ELSTER software certificate offers a means of identification for the trust

level ‘substantial’, which so far is the only one for this trust level.

In accordance with the eIDAS Regulation, rules have also been established to identify persons and organisations from EU Member States and for identification by recognised private providers. During the reporting period, the first German provider of an identification system was recognised by the Federal Government. Providers of private identification systems for SSO purposes give their account providers the option of using a pseudonymised digital advertising identity to address account users personally with the user’s consent. Such a digital advertising identity is comparable to smartphone advertising IDs and enables the profiling of user behaviour across user accounts. Users of means of identification under private law must be informed in a clear and comprehensible manner about the consequences of consenting to the generation of a pseudonymised digital identity for personalised advertising.

Federal portal and federal user account

I welcome the fact that, at my instigation, the DigFamG has also regulated the responsibilities for the federal portal and the federal user account in the E-Government Act and created legal bases for the processing of personal data in the federal portal and for access rights. This provides legal certainty and clarity for users, e.g. on where they can assert their data subject rights. However, with respect to further planned federal portal features, such as an application overview, I see there being a need for appropriate processing authorisations being standardised before they go live.

Cross-reference: 5.1 Register modernisation

5.3 IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0)

Cyber and information security are essential anchors of trust when it comes to digitalisation. However, the goal of improving the protection of society and the economy in the digital world pursued in the amendment to the IT Security Act must take data protection requirements into account.

IT security was and is a sore point for digitalisation and also for the protection of personal data. Data protection and IT security are inevitably intertwined. Ultimately, IT security should exclude misuse, unauthorised access and unauthorised use of personal data, so that IT security risks are always data protection risks as well.

The initial draft of the IT Security Act 2.0 was sent on to me at a departmental level in spring 2019. Originally planned new regulations in criminal law and criminal

procedure law, which in my view were excessive and therefore to be viewed critically in terms of data protection, were no longer pursued in a new draft.

In the legislative process as a whole, it is particularly important to me that the joint controllership and partnership between the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) and my department is strengthened. In this context, a valid information basis is a central prerequisite for the effective completion of tasks by both sides. It is therefore important that the BSI, which is to be expanded into an important information hub for IT security, continues to actively inform me about identified security risks and incidents in information technology.

One of the critical aspects of the bill is the extension of the storage of log data from three to twelve months. It is argued that this extension is essential for effective protection and detection of cyber attacks. This is because cyber attacks typically span a longer period of time and only with existing log data is it possible to reconstruct the attack and repair the damage as best as possible. The motivation for the longer retention period is understandable, but in my view it does not justify its significant extension and raises questions of proportionality. In addition, I have pleaded at various points for the IT Security Act to clarify which specific personal data is processed for which purposes.

For the BSI, the IT Security Act entails a considerable increase in responsibility and tasks. Correspondingly, the additional workload of my department for advising, monitoring and reviewing data protection requirements will also increase significantly when implementing the BSI’s new reviewing, requesting and monitoring powers.

My opinion dated 18 December 2020 can be found at www.bfdi.bund.de/stellungnahmen

5.4 Amendment of the Federal Intelligence Service Act

The Federal Constitutional Court (Bundesverfassungsgericht, BVerfG) has obliged the legislator to amend provisions of the Federal Intelligence Service Act (Gesetz über den Bundesnachrichtendienst, BNDG) on the ‘foreign telecommunications reconnaissance’ by 31 December 2021 (see 6.4). In view of the considerable relevance to fundamental rights, the vote on the draft bill took place under unreasonable time pressure.

In my first statement on the draft bill, I expressed my criticism of the tight timetable for departmental consultation. The timetable declared by the Federal Chancellery in the departmental meeting on 7 October 2020—just over a week after the draft bill was sent to the departments—to

introduce the Federal Intelligence Service Act (Bundesnachrichtendienst-Gesetz, BNDG) to the cabinet within just one month, blatantly violated the requirements of the Joint Rules of Procedure of the Federal Ministries and the requirement of early involvement of my department. It was impossible to examine the complex set of rules with the necessary care and depth within such a short period of time. Even if the Federal Chancellery later modified its timetable and the cabinet did not adopt the draft until 16 December 2020, a total consultation period of just three months for a total of four different draft bills, some of which have been substantially amended in terms of content, each with a few days for comments, is simply unreasonable. In order to avoid constitutional risks, it would also have been urgently necessary to adhere to the principle of 'thoroughness before speed'. I am also critical of the fact that no comments from the other departments involved were made available to me. An essential discussion with other participants was thus not possible.

Criticisms

My substantive criticism of the draft bill concerns the planned changes in the supervision of the Federal Intelligence Service (Bundesnachrichtendienst, BND) and various substantive regulations.

A major point of criticism in terms of substantive law lies in the insufficient implementation of the restrictions on data transfers by the BND to other domestic and foreign public and non-public agencies as stipulated by the BVerfG. My concerns about the intended design of the transmission regulations were partially taken into account by the Federal Chancellery and the transmission regulations were partially improved as a correction to the comprehensive data collection of the strategic foreign telecommunications reconnaissance. Nevertheless, other important aspects for the further design of transmission restrictions remained unconsidered, although the provisions are, according to the requirements of the BVerfG, crucial to create a counterbalance to the extensive, unprovoked data collection in the context of the strategic foreign telecommunications reconnaissance.

Among the concerns I have expressed is the bill's provision for the possibility of transmitting data collected by the BND for the purpose of providing political information to the Federal Government, domestic intelligence services or police forces for intelligence-gathering purposes. According to the intention of the BVerfG ruling, such data should only be collected for the purpose of providing political information to the Federal Government and, in principle, may only be transmitted directly to the Federal Government for this purpose. The view taken by the Federal Chancellery that domestic intelligence ser-

vices or police forces should be allowed to receive this data for their own onward transmission to the Federal Government in my view goes too far. This extension of the transmission powers introduced with the second draft bill represents a deterioration of data protection in relation to the first draft bill and meets with considerable constitutional concerns.

However, the need for changes in other intelligence service laws (e.g. the law on the protection of the constitution [Bundesverfassungsschutzgesetz, BVerfSchG]) on transmission regulations resulting from the BVerfG ruling was not the subject of this legislative procedure. The BND's authorisation bases for transmissions outside the BNDG were not adapted, like the general transmission regulations in the BNDG, which is likely to lead to the general transmissions not being constitutional in the BNDG in any case.

It should be emphasised that in other areas, such as the protection of confidentiality, my suggestions have been used as an opportunity for legislative improvements. The standards for the protection of confidentiality in the case of strategic foreign telecommunications reconnaissance and the intervention in information technology systems for the early detection of risks were initially to be understood in such a way that only professionals (e.g. journalists, lawyers) were covered by the protection of confidentiality, but not the communication relationship involving the conversation partners as such. This has been rectified in the bill. However, there is no general provision apart from the special regulations on strategic foreign telecommunications reconnaissance and interference with information technology systems.

The authority of the BND, standardised for the first time in the amendment, to intervene in information technology systems abroad to collect data through 'hacking' and the authority to forward this data to the domestic services as well as police and prosecution authorities is also considerably questionable from a constitutional point of view. My concerns about such particularly intensive data collection interventions and the associated transmission requirements were not taken into account by the Federal Chancellery.

New supervisory authority

Finally, the regulations for the implementation of the requirements made by the BVerfG for the independent objective legal control of the measures of the BND in the area of strategic foreign telecommunications surveillance are of particular relevance. Although a completely independent supreme data protection supervisory authority exists in Germany with my authority, which has a high level of expertise and many years of experience in data protection and thus intelligence service control

of the BND and the domestic intelligence services of the Federal Government, the Federal Government intends to create a new supreme federal authority, the 'Independent Control Council' ('Unabhängige Kontrollrat'). On the one hand, the purpose is to ensure a court-like control with final decision-making powers, which the essential procedural steps of strategic foreign telecommunications surveillance are subject to. In addition, it will be responsible for carrying out random administrative checks on the legality of the entire strategic monitoring process. The area of administrative control overlaps with my supervisory responsibility, since I already fully control the BND's data processing in the area of strategic foreign telecommunications reconnaissance.

With the merger of quasi-judicial and administrative control under the roof of a new supreme federal authority, synergy effects are not used which would have arisen had administrative legal control been transferred to me, as envisaged by the BVerfG as one solution variant. Instead of using existing control structures with experienced staff in my authority, which have proven their worth in the area of Federal Intelligence Service supervision, a new supervisory authority, which functions with detailed work but is inexperienced in intelligence control, is to be set up with considerable funds in the shortest possible time by the end of the year 2021. Since this is also still to be settled at the BND locations in Berlin and Pullach, possibly directly on its premises, doubts also arise as to the distance demanded by the BVerfG. These doubts are reinforced by the fact that the new control body can transfer the staff administration to the Federal Chancellery and thus to the authority superior to the BND, which the planned Independent Control Council will probably be forced to do due to the fact that it lacks its own structures. As a result, the existence of yet another supervisory authority makes the control landscape in the area of intelligence services even more confusing. Without comprehensive powers of cooperation among the control authorities, BND control is inevitably made more difficult. For this reason, too, the cooperation between the Independent Control Council and my authority must be legally structured in such a way that a substantive exchange on the specific controls may and must take place. Here, the bill does not yet meet all expectations and should be urgently improved in the parliamentary proceedings.

Cross-reference: 6.3 Foreign telecommunications reconnaissance ruling

5.5 Legislative procedure for amending the law on the protection of the constitution

The current legal situation in the law on the protection of the constitution does not currently permit source telecommunication surveillance in the intelligence sector or an intensification of cooperation between the constitution protection authorities and the Military Counterintelligence Service (Militärischer Abschirmdienst). This is to be changed by an amendment to the law.

Through a cabinet resolution of 21 October 2020, the Federal Government introduced a bill to amend the law on the protection of the constitution into the German Bundestag. From a data protection perspective, I have already commented on the draft (my document of 4 November 2020 can be found at www.bfdi.bund.de/stellungnahmen). At the time of going to press, the parliamentary deliberations have not yet been completed.

The object of the proposed legislation is, in particular, to grant the intelligence services the authority to conduct source telecommunication surveillance as well as to technically expand the exchange of information between the constitutional protection authorities and the Military Counterintelligence Service by expanding the options for joint data storage.

Last but not least, the constitutional court judgements of the past year on foreign telecommunications intelligence (BVerfG, judgement of 19 May 2020 - 1 BvR 2835/17) and on providing information about inventory data (BVerfG, judgement of 27 May 2020 - 1 BvR 1873/13, 1 BvR 2618/13) have once again made it clear that the scope and extent of the need for reform in the law on the protection of the constitution are dramatic. The regulatory system, density and depth of the relevant provisions generally lack the necessary consistency and quality to authorise the intelligence services to take measures that encroach on fundamental rights in accordance with constitutional law.

Instead of improving these deficits, the bill would put further strain on the already unconstitutional legal situation. The introduction of such a far-reaching and momentous measure as source telecommunication surveillance in particular requires a comprehensive, stringent and resilient overall legal concept that takes into account all of the Federal Constitutional Court's requirements.

The intensification of the exchange of information between the constitutional protection authorities and the Military Counterintelligence Service, which is certainly correct in principle, cannot be implemented in accordance with the constitution on the basis of the current

bill. The basic prerequisite for intensifying and expanding cooperation between domestic intelligence services is the existence of legal transmission regulations between the authorities concerned that conform with the constitution. The transmission regulations of the Federal Protection of the Constitution Act and the Military Counterintelligence Service Act are in fundamental need of reform following the release of the findings of the Federal Constitutional Court in its decision on foreign telecommunications reconnaissance at the latest.

The legislator should therefore currently concentrate exclusively on reforming the law on the protection of the constitution from the ground up in line with the constitutional requirements. Only after this has been fully achieved should it consider expanding intelligence data processing or even intelligence powers on the basis of a conscientious evaluation of the need for and the effectiveness of intelligence powers. In doing so, it must also pay particular attention to whether any extensions of powers are really necessary or whether it is not rather the case that police and prosecution authorities already cover the state's needs with their existing powers.

Cross-references: 5.3 Amendment of the Federal Intelligence Service Act, 6.3 FMA ruling

5.6 The regulation on 'apps on prescription'

Patients rightly expect prescribed health apps to keep their data confidential. To ensure this, the regulations in the Digital Health Applications Ordinance (Digitale-Gesundheitsanwendungen Verordnung, DiGAV) must be improved—self-declaration by the manufacturers cannot suffice here.

The DiGAV came into force in April 2020. It is intended to set out in detail the provisions of the act for better healthcare through digitalisation and innovation (Digital Healthcare Act [Digitale-Versorgung-Gesetz, DVG]—see no. 5.6 in the 28th Activity Report) on digital healthcare applications (DiHAs), in particular Sections 33a and 139e of the Fifth Book of the German Social Code (SGB V). Section 33a of SGB V introduced an entitlement for people with statutory health insurance to be provided with DiHAs, which can be prescribed by doctors and psychotherapists and are reimbursed by the health insurance provider. The prerequisite for this is that the respective DiHA has successfully passed a test procedure set by the Federal Office for Drugs and Medical Devices (Bundesamt für Arzneimittel und Medizinprodukte, BfArM) and is listed in a directory of reimbursable digital health applications. Details of this 'fast track procedure', of rapid access by DiHAs to the primary healthcare market, are included in the DiGAV.

I already expressed my fundamental concerns about the procedures for ensuring a sufficient level of data protection and data security for the DiHAs to the Federal Ministry of Health and the German Bundestag's Committee on Health during the legislative process for the DVG. Unfortunately, they were not taken into account in the DiGAV either and continue to apply without restriction.

For example, I have repeatedly highlighted privacy concerns about the distribution of health apps through platforms owned by Apple and Google. The problem with downloading DiHAs via commercial app stores is that third parties may be able to obtain sensitive health data as well as the app store operators (e.g. via a depression app or similar—metadata can be very sensitive in these cases). Digital health applications should therefore not be transmitted via 'publicly available digital distribution platforms' such as those of the US companies. Instead, an app store should be created in the telematics infrastructure, operated by parties in the healthcare system who are subject to the legal duty of confidentiality. Of course, even while using the DiHA, there is a risk that the manufacturers of the mobile devices or other third parties may obtain sensitive health data and create health profiles, for example, by integrating tracking or analysis tools.

Confidentiality and accountability not assured

Transparency for users is a very important aspect, especially when users' voluntary, informed, explicit consent is the legal basis for the use of the DiHA. The DVG, the DiGAV and the BfArM guidelines on the 'fast track procedure' under Section 139e of SGB V state in abstract terms that data protection and data security must be observed. However, it is problematic that only a self-declaration by the DiHA manufacturers is envisaged, which does not actually have any legally binding effect, and as such, it cannot be reliably demonstrated that data protection requirements, which are required in Section 139e of SGB V and in the DiGAV, are actually complied with.

In addition, there are no clarifying regulations on responsibility under data protection law. The purposes for which and the conditions under which the manufacturer may process data collected through the DiHA are set out in Section 4(2) of the DiGAV. However, other parties may also have access to sensitive health data—depending on the specific context of use of the DiHA, this could include physicians or other healthcare providers. Often, a DiHA manufacturer cannot reliably answer many questions in its 'data protection self-declaration' to the BfArM. This does not guarantee transparency for the user. Rather, users would need to be fully informed in advance about which individuals/entities would have access to which of their health data through them using

the DiHA. Unfortunately, neither the DVG nor the DiGAV provide for a contact person for data subjects' rights who could provide comprehensive information in the specific context of use. Clarifications that I had requested were not provided.

I sincerely hope that future laws and regulations to further digitalise healthcare will address these deficiencies.

5.7 Data Transparency Regulation (Datentransparenzverordnung)

The Data Transparency Regulation specifies the requirements in the SGB V and makes more detailed stipulations for data processing in the Research Data Centre. Unfortunately, there are no rules on the implementation of the right to object.

The amended Data Transparency Regulation of 19 June 2020, which came into force on 11 July 2020, specifies the tasks and procedure for data transparency in accordance with Sections 303a to 303e of SGB V. As a result of the Digital Healthcare Act of 9 December 2019, which I reported on in my 28th Activity Report (no. 5.6, p. 45), the data transparency procedure has undergone a number of changes, meaning that the regulation has also had to be rewritten. The Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) involved me at an early stage, but in the end the deadlines set for me were again very short: the draft itself was finally sent to the departments for comment with a deadline of just 12 calendar days.

Overall, the wording of the draft showed that data protection was in principle given a high priority. I expressly welcome this, since the demonstrably careful handling of the sensitive health data concerned here is essential for acceptance among the population. This is necessary because, due to data transparency regulations, the data supplied to the Research Data Centre (Forschungsdatenzentrum, FDZ) is the account data for more than 70 million persons covered by statutory health insurance. In addition, the scope of data had been extended by the DVG. Transparency vis-à-vis data subjects is enhanced by the fact that the individual categories of data are now mentioned in the regulation and are not hidden behind references to other standards.

This regulation also stipulates that the Federal Institute for Drugs and Medical Devices (Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM) will maintain the research database and that the Robert Koch Institute, as a trust centre, will ensure that the data is pseudonymised. The research database is of particular importance because of the volume of data and its sensitivity. It would

have been all the more important to allocate tasks in this context not in a regulation but by law. I have therefore suggested—unfortunately so far in vain—that a corresponding amendment to Section 303a of SGB V be made in the near future.

The designation of the BfArM as the owner of the research database is problematic, since the BfArM is also part of the group of authorised users specifically named in the law who are provided with data after a corresponding application has been examined. Thus, the BfArM could decide on its own application. This lacks the necessary independence, which is indispensable for an orderly procedure that also duly respects data protection aspects. The regulation solved this incompatibility by stipulating that the BfArM itself cannot receive data. I view this regulation with a certain degree of scepticism, as it counteracts the BfArM's right of use granted by law. For this reason, too, I will carefully examine the processing of applications at the BfArM in due course.

New objection system required

In addition, I had recommended to provide rules for the implementation of the right of the data subject to object pursuant to Article 21 (6) of the GDPR, even if the conditions are likely to exist only in a few specific cases. The right exists independently of any implementation regulation. For reasons of legal clarity, however, a procedure should be specified here, since the objection should reasonably not be lodged with the FDZ itself, but with the respective health insurance provider. Unfortunately, this recommendation was not implemented. This is regrettable, as it could have alleviated the concerns of citizens about mandatory government data collection and retention, which I am aware of due to various submissions. The BMG has signalled that it will soon establish an orderly objection procedure outside of the Data Transparency Regulation. I will continue to monitor the progress of these efforts. The BMG did not take up my request to provide for a general right of objection.

Cross-reference: 7.3 Healthcare registers

5.8 The basic pension is coming—but will it be compliant with data protection law?

The financial improvement brought about by the introduction of the basic pension is welcome from a social perspective. However, the planned form of entitlement verification interferes with the right to informational self-determination.

Those who have paid into the statutory pension scheme over many years with below-average income are to be

better protected in old age from a financial perspective. This is the aim of the Basic Pension Act (Grundrentengesetz) on 1 January 2021.

I was involved in the legislative process. However, my data protection objections were not taken into account.

The Basic Pension Act provides for the use of the tax identification number outside the taxation procedure by the statutory pension insurance institutions. Within the context of the constitutional court's case law on the creation of a uniform personal identifier, this is problematic with respect to constitutional law. This applies all the more as the Federal Government is currently planning to introduce the tax identification number as a uniform personal identifier for all citizens as part of the register modernisation (see 5.1 Register modernisation).

It is not just the income of the person entitled to the pension, but also that of the person living with him or her in a marriage or civil partnership that is used to calculate the basic pension. Statutory pension insurance institutions are therefore granted the authority to also query the tax identification number of the spouse or civil partner at the Federal Central Tax Office and to use it for an automated data comparison with the tax authorities when checking income. In addition to the problem described regarding the use of the tax identification number outside of the taxation procedure, this data comparison violates the principle of first collection under data protection law and thus encroaches on the rights to informational self-determination of third parties.

Cross-reference: 5.1 Register modernisation

5.9 The Digital Family Benefits Act (Digitale Familienleistungen-Gesetz)

Digital family services as the first step for comprehensive administrative digitalisation? Less paperwork, just with more data protection.

The act on the digitalisation of administrative procedures when granting family benefits (Digital Family Benefits Act) of 3 December 2020 promises less paperwork for important family benefits such as parental allowance, child benefit or child supplement. The digitisation of these applications should be the start of comprehensive administrative digitalisation. I welcome this in principle. However, administrative digitalisation has been fast-tracked. Tight schedules were the order of the day in this ambitious legislative process from the very beginning.

As a result, the digitalisation of parental allowance, child benefit or the application for a birth certificate is voluntary, essentially presupposes the consent of the applicants and—which must remain the case—represents an alternative alongside the paper application, which is still an option.

I fully support the goal of the Digital Family Benefits Act to be the start of the digital application process in social law. This also applies to the consent option found here. However, consent within the meaning of the GDPR means 'informed consent'. The citizen must know what kind of data processing they are consenting to. This will be important in the implementation of the law. In many areas of social law, the principle of direct collection also applies, i.e. data must be collected directly from the data subject. The law clearly deviates from this, albeit for the convenience of the applicants concerned. Transparency and control by citizens over their own data and the possibility to view the status of the respective procedures at any time are therefore essential. As such, 'trustworthy communication' between different authorities must not lead to the authorities knowing more about citizens through digitalisation than they are aware of. The most important thing here is implementation in practice, which I will continue to monitor critically.

Digitalisation of other administrative procedures

The act created further data protection regulations for the user account and for the processing of personal data in the federal administration portal by amending the Online Access Act (Onlinezugangsgesetz, OZG) and the E-Government Act (E-Government-Gesetz, EGovG) (see no. 5.2). These framework conditions—which can also be used for the digitalisation of other administrative procedures—are, without exception, characterised by voluntary participation by citizens and a high level of data security. I was able to provide a lot of momentum for the legislative process here, and this was followed up by the legislator.

In the act itself, I had also demanded that, insofar as the transmission paths and other aspects relevant to data protection are regulated between the Pension Insurance Data Office (Datenstelle der Rentenversicherung, DSRV) and the authorities responsible according to Section 12 (1) of the Federal Parental Allowance and Parental Leave Act (Bundeselterngeld- und Elternzeitgesetz, BEEG), a stipulation should also be made to reach an agreement with me (Section 108a [4] of SGB IV). The fact that this suggestion was not followed is regrettable. The act creates the legal basis for data transfers for using the rvBEA procedure¹ to query remuneration data from employers,

¹ 'rv' stands for 'Rentenversicherung' (pension insurance); 'BEA' stands for 'Bescheinigungen elektronisch anfordern und annehmen' (request and accept certificates electronically)

including for parental allowances (Section 108a of SGB IV, Section 9 [2] of the BEEG). The competent state parental allowance offices will be given the opportunity to use the DSRV's data retrieval and transmission procedure. As a result, applicants no longer have to submit the required remuneration certificates from their employer themselves; instead, the DSRV electronically queries remuneration data from the employers on behalf of the state parental allowance offices and then forwards this data to the parental allowance offices. I will offer my advice on the framework agreement, which is still to be agreed and which will regulate the modalities of this—legally unique—contract awarding.

I expressly welcome the fact that the competent parental allowance office only commissions the retrieval and transmission of the remuneration statements in accordance with Section 108a of SGB IV if the applicants have consented to both data retrieval and data transmission for their remuneration statement data.

All of this shows that the digitalisation of complex administrative procedures, in which various public and private agencies from federal and state governments are involved in addition to the citizens, is not a simple and quick task, but it is also one that can be solved. Administrative digitalisation and the associated—highly desirable—simplification of administration must not be at the expense of citizens' rights and opportunities for participation and control. Digitalisation should instead be used to increase transparency and participation opportunities for citizens.

I will constructively provide support for further legislative projects on the digitalisation of application procedures in social law that will follow in the next few years.

5.10 Current legislation and other regulations in the telecommunications sector

Several laws in the telecommunications sector need to be aligned with European law in a timely manner. However, as things stand at present, this will not be done in time. The ePrivacy Regulation also continues to be a long time coming.

In my last AR (no. 5.2), I already complained that numerous laws have still not been adapted to be in line with the General Data Protection Regulation (GDPR). The ePrivacy Regulation has also been poorly implemented for years. In particular, the provisions on cookies do not comply with European law. I have repeatedly called on the legislator to take final action here. The persistence of legal uncertainty is intolerable for businesses and supervisory authorities. In July 2020, the Federal Government

first presented a draft for an amendment to the Telemedia Act. In the future, this will be called the 'Telecommunications Telemedia Data Protection Act' (Telekommunikations-Telemedien-Datenschutz-Gesetz, TTDSG). It is gratifying that the legislator has taken a first step here. Unfortunately, the draft has significant flaws. I have commented on this and made recommendations.

Telecommunications Modernisation Act

The Telecommunications Modernisation Act (Telekommunikationsmodernisierungsgesetz, TKMoG) implements numerous requirements from the European 'Electronic Communications Code' in national regulations, in particular the Telecommunications Act (Telekommunikationsgesetz, TKG). The objectives of the code are to develop and exploit very high capacity networks, to ensure sustainable and effective competition and to ensure the interoperability of telecommunications services. It also aims to ensure the accessibility and security of networks and services and to promote the interests of end users. Citizens should be provided with affordable, high-quality telecommunications services. As part of the transposition into national law, the central concept of telecommunications services is also significantly expanded. This was previously defined in Section 3, No. 24 of the TKG (old) and will be legally anchored in the new provision of Section 3, No. 55 of the Telecommunications Act (Telekommunikationsgesetz, TKG) in the future. Therefore, messenger services, e-mail services and videoconferencing services in particular will now also be covered by the concept of telecommunications services. Thus, in the future, my data protection supervision could also extend to these services. According to Section 9 of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), the BfDI is responsible for the supervision of companies that process data concerning natural or legal persons to provide telecommunications services.

Unfortunately, there is no telling when the laws will come into effect.

ePrivacy Regulation

I have already reported in detail on the revision of the ePrivacy Regulation, which is to be replaced by an e-privacy regulation that is directly applicable in the Member States (see no. 17.2.4.1 of the 26th AR, no. 15.1.2 of the 27th AR and no. 5.2 of the 28th AR). While the European Commission already presented the draft ePrivacy Regulation on 10 January 2017 and the European Parliament adopted the draft report of the lead LIBE Committee on 26 October 2017, negotiations in the Council of the EU have not made an decisive progress since mid-January 2017. The original goal of having the ePrivacy Regulation enter into force at the same time as the GDPR on 25 May 2018 has therefore already been missed by more than

two and a half years. The German Council Presidency wanted to achieve a 'general orientation' of the Council in the second half of 2020 so that the trilogue negotiations with the European Parliament and the European Commission necessary for adoption could finally begin. However, the negotiations in the Council continued to drag on, even under the German Presidency, so final adoption can probably be expected in 2021 at the earliest.

I was able to successfully lobby the Federal Ministry for Economic Affairs and Energy to remove provisions on data retention and the processing of communications metadata for other purposes without the consent of end users from the draft regulation. My concerns about the general lowering of the level of data protection, on the other hand, unfortunately went unheard, as did my demand that data protection supervision of compliance with the ePrivacy Regulation should be left to the data protection authorities on a mandatory basis in accordance with the Commission's draft. Thus, in some Member States, there is a risk of fragmentation of the supervisory landscape and additional, unnecessarily complex coordination mechanisms between the different supervisory authorities in the European Data Protection Board (EDPB). This will make it more difficult to enforce data subjects' rights.

6

Security

6.1 Police 2020

Through the 'Police 2020' project, police authorities at federal and state level want to redesign the police IT landscape. The system will be split into different 'domains' covering the whole range of police work. They concern both individual transactions and information which the police authorities intend to retain for future use in analyses and data comparisons. I still lack reliable documentation on the basis of which I could assess the system or individual subsystems.

The Police 2020 Project Group at the Federal Ministry of the Interior, for Construction and Home Affairs (BMI) gave me a verbal presentation on the status of the project in December 2019. It agreed to involve me in the future. Following this meeting, the BMI sent me an initial 'technical development plan'.

However, this document does not constitute an adequate basis for carrying out a robust examination under data protection law. The project is divided into various sub-projects, most of which are apparently to be developed in the states and then later transferred to the information network managed by the Federal Criminal Police Office (Bundeskriminalamt, BKA). In several cases, I have only learned from third parties that significant parts have progressed in planning that directly or indirectly affect the Police 2020 project or one of its intermediate steps.

For this reason, after consulting with the federal state data protection commissioners, I first wrote a letter of principle to the BMI. On this basis, the Data Protection Conference has adopted a resolution to this effect.¹

In terms of content, I welcome the fact that the development plan identifies data protection as one of its key objectives. However, the plan does not describe in detail how this objective is to be achieved. It is necessary to first define the legal limits and possibilities before the system as a whole and individual subsystems are put into development. The conception or programming of

individual modules should not begin before fundamental data protection issues have been clarified.

Comprehensive review required

This first requires a comprehensive data protection review for existing data, systems and practices. The 'technical development plan' is oriented towards police interests. It has not taken into account the findings of the numerous data protection checks and consultations carried out in recent years. I suggest that this should first be done through an independent evaluation.

Legal guard rails

The documents available to date do not address the legal framework. Only one innovation is mentioned: the principle of hypothetical data recollection. This principle is indeed important. However, it is by no means the only legal and constitutional requirement to be observed. The Federal Criminal Police Office Act and the state police laws provide numerous legal guidelines that must be taken into account in the Police 2020 concept. The responsible bodies must adequately check and document whether and how these are complied with—before planning and commissioning a system in detail. So far, this has not been fulfilled.

Separation of purpose

The 'development plan' reads: 'At its core, incident and case processing, evaluation and analysis, and evidence management are moving to a unified police case management system.' On the basis of this statement, it is unfortunately to be feared that in future there will no longer be sufficient differentiation between the various purposes, but that all stored data will be subsumed under the generic term 'police processing'.

But the important thing is: when the security authorities process personal data, a specific purpose must always be defined. In particular, data stored for a specific task or for documentation purposes may not be transferred across the board to a data repository which at the same

¹ You can find the 16 April 2020 resolution at www.bfdi.bund.de/entschluesungen

time serves to prevent danger or criminal prosecution. However, this is the case when all data is used in a blanket manner in an evaluation and research platform. How this is to be technically delimited in the future is not known to me, but it is fundamental for data protection evaluation.

Evaluation and analysis

With the new 'data house' in Police 2020, the security authorities are creating a technical basis for comprehensive computer-based analyses of personal data. These heavily interfere with fundamental rights and must therefore be limited both from a legal and a technical perspective. To base them merely on general clauses does not do justice to the fundamental right to informational self-determination.

So far, it is unclear what exactly is planned. On the one hand, it was emphasised in the verbal presentation of the technical development plan there was no intention to use 'artificial intelligence'. On the other hand, the development plan provides for what appears to be a fairly extensive 'Domain 2' for evaluation and analysis.

Basic data protection modules

In addition, greater attention should be paid to data protection opportunities, for example through basic modules specifically designed for data protection.

The Police 2020 programme offers the opportunity to implement new basic technical functionalities for data protection as 'basic services'. For example, a 'basic separation of purposes service', a 'basic data quality service' and a 'basic supervision and control service', containing logging services in particular, are required.

Proof of concept (POC) data consolidation sub-project:

At the start of 2019, I was still invited to join the project's legal working group on a Police 2020 sub-project—planned data house testing. I have informed the BMI of considerable data protection objections to the project. Since then, I have not been invited back to this WG. In December 2019, BMI verbally assured me of my future participation in the legal WG again. Contrary to this promise, I have not yet received an invitation and have not participated in any other way.

This surprises me insofar as in the Federal Government's answer of 6 August 2020 to a minor question, it was still stated that the BMI, the BKA and the Federal Government/state committees were in a regular contact with me on the planning of the POC data consolidation. My comments would be carefully examined and included in further deliberations on the POC (BT printed matter 19/21510).

In the meantime, the ministry has informed me that it is no longer responsible for the project because this is purely a state matter, but at the same time, the project will be integrated into Police 2020 at a later date if necessary. Therefore, it is not comprehensible to me whether and why the ministry is now relinquishing responsibility.

PIAV-S sub-project

PIAV-S stands for the strategic use of data in the Police Information and Analysis Network (PIAV). PIAV is intended to expand the exchange of information and intelligence between federal and state police forces. It is intended to help set priorities and advise police and political management and decision-making levels. To this end, it is to provide selected personal, case and factual data from police authority incident or case systems and facilitate a daily updated, location-related and person-related count of criminal offences. PIAV-S thus differs qualitatively from the police crime statistics, which only record offences after the police investigation has been completed.

The BKA talks about one type of data processed. However, my initial assessment is that this is pseudonymised, i.e. personal data. I am in discussion with the BKA to clarify this point. If it is only a matter of pseudonymisation, which still allows the police to use the individual data, I do not see any legal basis in federal law for the data transfer from the states to the BKA and the storage in PIAV-S. Therefore, there is still a considerable need for clarification in this matter.

6.2 Uniform case processing system

The uniform case processing system (UCPS) at the BKA consolidates all decentralised case processing systems of the Federal Police (Bundespolizei, BPOL), the BKA and state police forces. In a first step, the systems of the BPOL, the BKA and the police forces of Brandenburg, Baden-Württemberg, Hesse and Hamburg were put on a common basis.

In 2019, an interim solution to the UCPS was started with the BKA as the central IT service provider. With the start of operations, I received written documents going beyond a general presentation for the first time; only shortly before the editorial deadline for the activity report did I receive further documents.

The multi-client interim solution is based on the BKA's individual case processing systems, the Federal Police and the participants of the 'CRIME cooperation' (police forces of Brandenburg, Baden-Württemberg, Hesse and Hamburg). These use system variants from one and the same manufacturer. The finished solution, the UCPS, is

to become a uniform platform for all participants in the future.

However, the documents sent to me only describe the requirements from the user's point of view, and not the finished system, so I was unable to make a data protection assessment. In particular, there is a lack of documentation that accurately describes the purpose and legal bases of the system. Therefore, I currently see the following problems:

firstly, the legal basis of the UCPS and the purpose for which it is operated is not documented. If the UCPS is to be operated not just for the purposes of criminal proceedings, but also for threat prevention, this would also have further implications, for example, for access authorisation. The processing purposes under data protection law are to be separated in this case (see no. 9.5.3 on the CPS).

Secondly, a data protection impact assessment is still missing. Because the UCPS, as a multi-client-capable system, unites all data in one data warehouse and does away with decentralised data storage at a federal and state level, the risks in terms of data protection and IT security increase. I was at least promised the preparation of the data protection impact assessment.

Thirdly, no comprehensive erasure concept has yet been presented that describes how the erasure of data, for example from case processing on site, affects the system at a state and federal level or vice versa. Instead, it only describes how a user carries out erasure in their system. In addition, new words such as 'anlöschen' (delete) and 'Löschvormerkung' (delete flag) are created instead of using standard data protection terms such as Löschen (erase) and Sperren (suppress).

Cross-references: 6.1 Police 2020, 9.5.3 Case processing system

6.3 The ruling of the Federal Constitutional Court on strategic foreign telecommunications reconnaissance

The ruling of the Federal Constitutional Court (Bundesverfassungsgericht, BVerfG) on the constitutionality of the regulations in the Federal Intelligence Service Act (Bundesnachrichtendienst, BNDG) on foreign telecommunications reconnaissance was eagerly awaited. I was invited as an expert witness in the court proceedings and was able to provide insight into the data processing practice of the Federal Intelligence Service (Bundesnachrichtendienst, BND) from my control experience. The ruling, which declared the regu-

lations on strategic foreign telecommunications reconnaissance in the BNDG to be unconstitutional, at the same time contains detailed requirements for a constitutional design of strategic foreign telecommunications reconnaissance and clarifies the framework for the necessary independent, objective legal control of the data processing procedures in the BND.

The human rights organisation Reporters sans frontières and other complainants had filed a constitutional complaint against the new version of the BNDG from 2016 and the surveillance measures threatening them as part of the BND's strategic foreign telecommunications surveillance. Among other things, the complainants argued that the secrecy of telecommunications under Article 10 (1) of the Basic Law (Grundgesetz, GG) and the freedom of the press under clause 2 of Article 5 (1) of the GG also protect against access by German state authorities abroad to the contents and metadata of electronic communications. The background to this was the concern in the complainants made that data from communications requiring special protection, e.g. in journalistic research work with informants, could be passed on by the BND to other intelligence services worldwide in line with common practice.

In addition to the question of the binding nature of German state authority to fundamental rights when acting abroad towards foreigners, the court was faced with the task of identifying the constitutional limits within which strategic foreign telecommunications reconnaissance can be permissible and proportionate as an instrument with considerable scope. In doing so, the court emphasised that global and unrestricted foreign intelligence is constitutionally impermissible. According to the BVerfG, as a particularly intrusive instrument of reconnaissance, it requires substantial restrictions to sufficiently limited and differentiated purposes, which the legislator must determine. Accordingly, only purposes aimed at the protection of high-ranking common goods, the violation of which would cause serious damage to external and internal peace or to the legal interests of individuals, can be considered. Another essential question is whether the BND is in a position to technically implement the limits of such a permit. Obtaining this knowledge about the technical capabilities of the BND was therefore one of the challenges of the proceedings, which the BVerfG met by questioning the BND itself as well as independent experts and specialists. As such, I also had the opportunity to answer questions from the court and share my impressions of the control practice.

Another focus of the proceedings concerned the question of which constitutional requirements are to be placed on the control of surveillance measures within the framework of strategic foreign telecommunications reconnaissance. In my experience, the possibility of a



The core statements of the judgement (judgement of the First Senate of 19 May 2020 - 1 BvR 2835/17) can be summarised as follows:

- The areas of protection of the secrecy of telecommunications under Article 10 (1) of the Basic Law (Grundgesetz, GG) and of the freedom of the press under clause 2 of Article 5 (1) of the GG also extend to measures taken by German authorities against foreigners abroad, i.e. also to measures of the BND's strategic foreign telecommunications reconnaissance.
- Strategic foreign telecommunications reconnaissance is an exceptional power with a considerable scope and intensity of intervention, which can be designed in a proportionate and constitutional manner, taking into account the criteria for limiting data collection and processing outlined by the BVerfG. According to the court, this particularly includes accompanying regulations on the use of filtering techniques, permissible monitoring purposes, the design of the monitoring procedure, focussed handling of search terms, limits to the stockpiling of traffic data, methods of data evaluation, the protection of confidentiality relationships and the core area of private life design as well as the specification of erasure obligations, and the requirements for independent objective legal control.
- If data from strategic foreign telecommunications reconnaissance is processed by the BND, data relating to the core area of private life may not be processed at all and data of persons in particular need of protection (e.g. whistleblowers, dissidents) or from communication relationships requiring special protection (e.g. between lawyer and client, journalist and informant) may only be processed in exceptional cases standardised by law.
- To ensure that all data collection and processing within the scope of strategic foreign telecommunications reconnaissance is carried out in line with constitutional law, it is also necessary to design and use the data processing systems and other data processing processes in a manner that complies with constitutional limits.
- The transfer of data from strategic foreign telecommunications reconnaissance to other authorities at home and abroad is subject to strict conditions. As a rule, specific dangerous situations for specific, higher-ranking legal interests must be factually identifiable, otherwise disclosure is inadmissible. The purposes permitting a transfer are to be standardised, and the implementation of a transfer is to be made accessible to independent control.
- Additional conditions must be met when transferring data to foreign intelligence services. According to the requirements of the BVerfG, the transfer of data abroad is only permitted if the handling of the transferred data there does not undermine the guarantees of the protection of personal data under human rights law. It is necessary to ensure an adequate level of substantive data protection law for the handling of the transferred data in the recipient state. The BND must carry out this assurance of the rule of law as an independent prerequisite before transferring data abroad.
- An appeal to the 'third-party rule' may not limit the control of data processing of the BND with reference to foreign intelligence services. The legislator must create independent, continuous legal control for strategic foreign telecommunications reconnaissance, which controls the lawful use of the strategic foreign telecommunications reconnaissance as a quasi-judicial control and the practice of data processing as an administrative control.

complete control of all data processing procedures in the BND is hampered by the fact that an unrestricted exchange between other control bodies, such as the G 10 Commission, and myself is not possible under the current legal situation. In addition, the BND invokes the ‘third-party rule’ against me and refuses to control data it has received from foreign partner services which it is not allowed to pass on to third parties without their consent according to informal transmission agreements with these services. Fortunately, however, the BVerfG has made it unmistakably clear that the legislator must organise the future control of the BND in such a way that it is not hindered by the ‘third-party rule’.

The BVerfG has ordered that the impugned provisions shall continue to apply for the time being, but at the latest until 31 December 2021, despite them being unconstitutional. The legislator is therefore called upon to rewrite the provisions in the BNDG relating to strategic foreign telecommunications reconnaissance. On 16 December 2020, the Federal Cabinet approved a corresponding draft of the Federal Chancellery for an amendment to the BNDG (see 5.4). Even though I generally welcome the fact that the Federal Government is attempting to implement the requirements of the Federal Constitutional Court for strategic foreign telecommunications reconnaissance in conformity with the constitution through the amendment, I have considerable doubts in some areas of the bill as to whether it has succeeded in doing so.

Cross-reference: 5.4 Amendment of the Federal Intelligence Service Act

6.4 The Haber procedure

The Federal Ministry of the Interior, for Construction and Home Affairs (Bundesministerium des Inneren, für Bau und Heimat, BMI) still refuses to acknowledge that a separate legal basis is required for the data processing that takes place in the ‘Haber procedure’.

As already discussed in the Activity Report 2019 (see no. 6.5 of the 28th AR), there is no legal basis for the involvement of the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) in the award of state services to prevent abusive use by anti-constitutional organisations (‘Haber procedure’). Subsequently, I formally objected to the lack of legal authorisation for the data processing carried out by the BfV in this context during the reporting period in question pursuant to Section 16 (2) of the Federal Data Protection Act, Section 27 No. 1 of the Federal Protection of the Constitution Act.

The BMI’s refusal to take steps to address the legislative deficit is unacceptable. A ministry as an executive body cannot arbitrarily and on its own initiative create new data processing powers for one of its departmental authorities by means of decree regulations to the detriment of holders of fundamental rights, as the BMI has done in the present case with the Haber-Diwell Decree. This is exclusively the task of the legislator, who is legitimised to do so.

The case law of the Federal Constitutional Court from last year also leaves no doubt about this and forces the legislator to carry out extensive reforms, especially in the area of intelligence services. In its ruling on strategic foreign telecommunications reconnaissance (see also 6.3), the Federal Constitutional Court made it clear that the need for secrecy in intelligence activities does not justify a reduction in the number, scope and quality of legal authorisations.

Cross-reference: 6.3 The ruling of the Federal Constitutional Court on strategic foreign telecommunications reconnaissance

6.5 Security screening of applicants to intelligence services

Applicants to intelligence services are not informed of the outcome of their security clearance, nor do they have a right to be heard in advance if the security investigation reveals a potential security risk. In future, however, they will be informed of this legal situation in advance.

In the area of security clearance law, I am receiving an increasing number of submissions from applicants to federal intelligence services. In particular, data subjects claim that they are not informed, in the context of employment being refused, as to whether this is related to the security clearance carried out and ask for my assistance in this respect. I am pursuing this matter in the context of my data protection law review authority in Security Screening Act (Sicherheitsüberprüfungsgesetz, SÜG).

Even though these are not primarily data protection regulations, I would like to clarify that according to clause 4 of Section 6 (1) of the SÜG, the right to be heard does not apply to applicants to federal intelligence services within the framework of the security clearance process, and according to clause 2 of Section 14 (4) of the SÜG, they also do not have to be informed of the results of the security clearance. The SÜG explicitly provides for these special provisions for intelligence services.

The background to this is that foreign intelligence services should be prevented from conducting research into the state of knowledge and recruitment practices of German intelligence services. It is sometimes the case that foreign intelligence services smuggle potential applicants into recruitment processes.

The submissions have nevertheless prompted me to find out from the relevant intelligence services whether applicants are made aware of the applicable restrictions, either in writing or verbally, in advance of the security clearance being carried out. Feedback has indicated that this is not always the case.

In order to create more transparency for applicants, I have recommended that intelligence services provide written information on the exemptions in the SÜG in advance of the security clearance process. Fortunately, all intelligence services have followed up on my recommendation and have implemented it.

6.6 Passenger name records—how much data collection is justified to fight terrorism?

While the ECJ is examining the compatibility using passenger data to combat terrorism and other serious crimes with European fundamental rights in several cases, the Commission took positive stock of the situation this summer. However, the scope of the authorised data processing raises further doubts as to its proportionality.

For many years, I have criticised the extent of the processing of PNR data by police authorities in my activity reports (see no. 13.5.4 in the 22nd AR, no. 2.3.2 in the 26th AR, no. 1.3 of the 27th AR and no. 6.4 of the 28th AR). Directive (EU) 2016/681 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) requires Member States to collect, match and store PNR data from air carriers on an ad-hoc basis for a period of five years to allow for retrospective analysis. This applies to all passengers, even if there is no reason for them being stored in a police database for several years.

This year, the EU Commission carried out an evaluation of the implementation of the PNR Directive (see Evaluation Report of 24 July 2020, COM [2020] 305 final). From their point of view, the overall result is positive. The Directive serves its purpose and no changes are to be made at present. We should first of all wait for the ECJ's decision on the compatibility of the PNR Directive with

European fundamental rights. References for preliminary rulings are pending there from courts in various Member States. In Germany, too, lawsuits are pending against airlines and the BKA's Passenger Information Unit, which are directed in particular at the long-term storage of passenger data.

According to the statistical data collected by the Commission from the Member States, the automated instantaneous comparison of the transmitted passenger data with databases of wanted persons or samples achieves technical hits for 0.59% of the passengers. After a manual check, 0.11% of confirmed hits remain and are sent to the competent authorities for further verification. In the Commission's view, the small percentage shows that the system generates targeted hits and that innocent travellers have nothing to fear here. However, when translated into absolute figures, this conclusion is open to doubt.

In 2018, for example, some 924 million passengers crossed the EU's external or internal borders, according to Eurostat data. With a technical hit rate of 0.59%, more than 5.4 million people would have been subject to manual follow-up. At a rate of 0.11% of confirmed hits, more than one million people would have to be reported to the competent authorities for follow-up action. Even if the figures are currently probably lower in practice, as the full development of passenger databases has not yet been achieved in all states, these millions of checks would be legally justified in the future.

By contrast, the Commission only presents a small number of case studies to demonstrate the effectiveness and efficiency of the use of PNR data (see accompanying document to the Evaluation Report of 24 July 2020, SWD [2020] 128 final). Even if these cases are only a selection, the question arises as to whether the chosen form of bulk data processing and retention is still proportionate to achieve the undisputed legitimate objectives of combating terrorist offences and other serious crimes. This is all the more true in light of the recent ECJ case law in the 'La Quadrature de Net' case, according to which laws authorising data retention must always set out objective criteria that establish a link between the data retained and the purpose of the retention.

Data protection authorities call for improvements

Within this context, together with the other European data protection supervisory authorities in the EDPB, I have once again called on the EU Commission to make improvements to the legal situation.

The discrepancy between technical hits and manually confirmed hits also highlights a fundamental data quality problem. The data collected by airlines for their own

purposes is often not suitable for police data comparison because important data such as date and place of birth are missing and the search thus results in nothing.

In this context, the positive effect of the interaction with API data is referred to again and again. This is another form of passenger data transmission. The legal basis is Directive 2004/82/EC of 29 April 2004 on the obligation of transport companies to communicate passenger data (API Directive). Member States may require the transmission of specific passenger data to their border control authorities in respect of certain flights from third countries. Unlike PNR data, airlines must collect API data separately from official identification documents for this purpose. Therefore, such data is of higher quality and the data set is better adapted to police purposes. If it is collected, the PNR Directive also requires it to be transferred to the passenger information units, where it indirectly results in better data quality. However, this positive effect should not hide the fact that the interaction of the API Directive and the PNR Directive constitutes double supervision for data subjects and raises additional questions of proportionality. This aspect should be taken into account urgently in the forthcoming evaluation of the API Directive.

6.7 PCJA Directive still not fully implemented

The implementation of European law requirements in the Federal Police Act (Bundespolizeigesetz) and the Customs Investigation Service Act (Zollfahndungsdienstgesetz) is continuing to fail due to political wrangling over additional powers of intervention. I have already developed the first application aids for practical use.

Uniform minimum standards must be implemented in all EU Member States for the processing of personal data in the police and judiciary since 6 May 2018. I already provided information on this in the activity report before last (see no. 1.2 of the 27th AR). If certain requirements have not yet been implemented in the specialised police laws, the regulations in the first and third parts of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) additionally apply. However, some provisions of the BDSG must be compulsorily supplemented by specific and normatively clear specialist law.

This applies, for example, to Section 48 of the BDSG, according to which the processing of special categories of personal data is only permissible if it is absolutely necessary for the performance of the task and if, in addition, suitable safeguards are provided for the legal interests of the data subjects. This concerns, for example, genetic or biometric data.

The wording of the law raises the question of whether this provision should be regarded as an independent legal basis alongside the specialist law. However, this is out of the question because it is not formulated in a sufficiently specific and clear manner. The legislator should clarify that Section 48 of the BDSG is only intended to impose additional requirements in addition to the specific requirements of sectoral law, which are still to be regulated in detail.

In practice, it also becomes difficult where old regulations still exist in sectoral law which do not or not completely fit the requirements of the Directive. An example of this are the requirements of the PCJA Directive and the BDSG for data transfers to third countries. According to this provision, data controllers must satisfy themselves that an adequate level of data protection exists in the recipient state.

According to the Federal Police Act (Bundespolizeigesetz, BPolG) (which has not yet been amended), the level of data protection in the recipient state is only to be taken into account in the context of a balancing of interests between the public interest in the transfer and the legitimate interest of the data subject. At first glance, this may seem irrelevant in practice. However, the requirements of the Directive generally give more weight to the existence of an adequate level of data protection, when a derogation should only be allowed in exceptional cases. This may well lead to a different result in individual cases.

Within this context, I am therefore critical of the fact that the transposition of the Directive into both the BPolG and the Customs Investigation Service Act (Zollfahndungsdienstgesetz, ZFdG) has still not been completed.

There was already a draft bill for the amendment of the BPolG at the start of 2020, but it has not yet been possible to reach agreement on it due to differences of opinion between the coalition partners on the need for new powers of intervention. This draft was then not pursued further. At the time of going to press, it was known that the parliamentary groups of the governing coalition were working on a draft for the BPolG, which would then be introduced into parliament by the parliamentary groups.

The German Bundestag had even already passed a bill to amend the ZFdG (see no. 5.3.1 of the 28th AR), but the bill was not signed and promulgated. The background to this is apparently the decision of the Federal Constitutional Court on how to provide information about inventory data (see no. 7.4). According to this, the police laws must clearly regulate which authority may retrieve which data on which occasions and how the data may

then be used. However, the new ZFdG, which had already been passed by the German Bundestag prior to the BVerfG decision, contained a provision that did not meet these requirements, which I had already advocated in the legislative process (see no. 9.1.4 of the 27th AR).

BOX: While the legislator remains committed to the implementation of the PCJA Directive, I have evaluated initial experiences with the practical application of the new provisions of the BDSG in order to develop application aids for individual provisions of the BDSG. I would hereby like to support judicial, police and regulatory authorities in their practical work with data protection requirements.

You can find materials on the following regulations on my website:

- SECTION 53 OF THE BDSG: Data secrecy (sample)
- SECTION 67 OF THE BDSG: Data protection impact assessment (template with guidance, suggested methodology)
- SECTION 70 OF THE BDSG: List of processing activities (model with instructions)
- (coming soon:) Section 76 of the BDSG: Logging (notes).

Cross-reference: 7.4 Judgement on providing information about inventory data

6.8 Redesign of the FIU 2.0 information network

The Central Office for Financial Transaction Investigations, also known as the Financial Intelligence Unit (FIU), is planning to redesign its IT landscape. In future, methods and algorithms from the field of artificial intelligence (AI) will be used to deal with the steadily growing number of incoming SARs. I have demanded my participation due to the significant associated risks to the rights and freedoms of natural persons. In doing so, I was able to act in an advisory capacity at an early stage and point out deficiencies in data protection law.

The FIU is an independent organisational unit under the umbrella of the Central Customs Authority (Generalzoll-direktion) at the Customs Investigation Bureau (Zollkriminalamt). It is responsible for receiving, collecting and analysing reports on suspicious financial transactions that may be related to money laundering or terrorist financing. If, during its analysis, it determines that an asset is related to money laundering, terrorist financing or any other criminal offence, it shall transmit its analysis

findings and all relevant information to the competent law enforcement authorities.

By the end of 2023, the FIU plans to redesign its IT landscape in the form of the 'FIU 2.0 information network'. With respect to the data protection evaluation and monitoring of the project, I requested my participation and had the specifications prepared by the FIU submitted to me. In this way, I was able to get a first impression at a very early stage of the development of the IT project and check the technical and functional requirements of the system with regard to compliance with data protection regulations.

Unfortunately, I identified numerous deficiencies in terms of data protection law, which I pointed out to the FIU.

Lack of legal bases

Some of the FIU's planned data processing activities, such as the systematic collection and analysis of personal data from public sources, may already lack a legal basis. In some cases, I was also able to point out that the plans were no longer likely to be covered by the FIU's statutory mandate.

Erase concepts and technical process safeguards for compliance with selection test periods independent of event were not originally planned at all.

Use of artificial intelligence (AI) methods

From a data protection perspective, the planned use of AI methods to process the steadily increasing number of incoming suspicion of money laundering reports is particularly noteworthy.

In the future, automated applications and self-learning systems will be used to filter out cases of value from the large number of existing reports. They should first prioritise processing proposals and network representations.

In the future, it is planned to replace the manual analysis of all reported issues with an automated assessment. The systems are to decide in advance which reports require individual case examination by FIU human analysts.

The remaining notifications are to be automatically sent to the 'information pool'. This means that the reports are transferred to the FIU's central database, where they are continuously re-evaluated in an automated process. Manual processing should only take place if, for example, a new data situation results in a different valuation at a later date. I have already expressed reservations about this approach.

Data protection requirements

Section 54 (1) of the BDSG stipulates the requirement of a specific legal basis for a decision based exclusively on automatic processing which entails an adverse legal consequence for the data subject. Such a sufficiently specific and clear legal basis is not yet apparent in the Money Laundering Act (Geldwäschegesetz), which is relevant for the FIU.

The use of automated systems may entail high risks for the further rights and freedoms of individuals, in addition to intensive data interference. This is especially true if the applications are to make or at least prepare automated decisions. This is because complex systems are difficult to understand, even for experts.

In the case of the FIU, the situation is aggravated by the fact that data processing is particularly intrusive. On the one hand, the FIU is not a law enforcement agency. Its activity is of a purely preliminary character. Therefore, the level of suspicion for a money laundering SAR is still below the initial suspicion in terms of criminal proceedings. On the other hand, it carries out the described encroachments on fundamental rights secretly, so data subjects usually have no knowledge of the processing of their personal data.

Due to this particular intensity of interference with fundamental rights, AI applications should therefore be used restrictively at best. At the very least, however, AI applications here must be subject to special prior checking and ongoing monitoring in accordance with the recommendations of the Data Ethics Commission (Datenethik-Kommission).

6.9 Data protection breach in the area of customs investigation

In the customs investigation, improvements in the handling of seized data storage devices were achieved through the reporting of a data protection breach.

Customs investigators reported a loss of evidence to me as a data breach. The data storage devices in question were seized in criminal proceedings. My involvement was warranted because such data storage devices can often contain a large amount of sensitive personal data. For example, photos, chat histories, passwords and much more information can quickly accumulate in the memory of a smartphone. In the course of my review, I found that the evidence devices concerned were not adequately secured against unauthorised access to their contents.

Working through the facts of the case, it was possible to achieve a considerable improvement in the future handling of seized data storage devices. In particular, the organisational guidelines of the customs investigation department for handling this type of evidence were revised. The new measures particularly include a secure transport route, encryption in accordance with the specifications of the Federal Office for Information Security and the sending of data storage devices and access data via separate routes. In future, they are to be evaluated at regular intervals and adapted to technical developments.

6.10 Employee data protection in the Customs Administration

In the course of processing numerous submissions in the area of employee data protection, the Customs Administration often lacked willingness to cooperate and was missing awareness of the problem. This made it considerably more difficult for me to carry out my duties during the reporting period.

In 2020, I again received a large number of submissions from employees of the Customs Administration. In the course of processing, my staff repeatedly encountered resistance from the Customs Administration. The Central Customs Authority has already pointed out in writing in the past that queries made by my staff on statements were not welcome. Documents relating to the investigation of the relevant facts were not made available to me as requested, contrary to Article 58 (1) (a) of the GDPR. In administrative court proceedings, which are still ongoing, the Customs Administration doubts my claim to be provided with information to carry out my duties under Article 58 (1) (a) of the GDPR in conjunction with Section 16 (4) of the BDSG.

Initiation of disciplinary proceedings in response to my involvement

In one case, disciplinary proceedings were initiated against an employee from the Customs Administration because he contacted me. The employee made clear indications to me regarding an inadmissible exchange of official information via the messenger service WhatsApp. The Customs Administration then demanded that I hand over the file for use in disciplinary investigations, but I refused, citing my right to refuse to testify under Section 13 (3) of the BDSG. In the disciplinary proceedings, the employee was accused of circumventing official channels and causing damage to the reputation of the Customs Administration vis-à-vis me. The data protection breach possibly committed with the official use of the messenger service WhatsApp, on the other hand, was denied by the Customs Administration and has not been prosecuted in the same way so far. In my view, the reacti-

on of the competent body within the Customs Administration indicates insufficient sensitivity to data protection and the fundamental right to informational self-determination. The way whistleblowers are dealt with within the Customs Administration is not compatible with my ideas of a transparent, problem-conscious, data protection-sensitive and fair federal administration. In particular, the reference to a potential data breach must not lead to disadvantages for the notifying person, even if they are not directly affected by the breach. Otherwise, there is a risk that the willingness to flag potentially unlawful data processing, which is in the public interest, will decrease overall for fear of possible repression.

Loss of disciplinary cases

Also during the reporting period, the Customs Administration notified me of the loss of two disciplinary files as a data breach. In the course of my investigation, I announced my intention to instruct the Customs Administration to only distribute personnel files in the future only in person (hand to hand) or via restricted mailrooms or lockable mailboxes. The Central Customs Authority responded to this by claiming that a corresponding instruction was null and void due to the impossibility of implementation. The Central Customs Authority has since been instructed by the Federal Ministry of Finance to pass on disciplinary documents in person (hand to hand), via courier service or via restricted mailrooms and/or mailboxes. I expressly welcome this instruction and thank the Federal Ministry of Finance for supporting my work and strengthening data protection within the Central Customs Authority.

Unauthorised operation of an access control and alarm system

In a Customs Investigation Office, an electronic access control and alarm system had been operated for years without the necessary data protection requirements being met. It was not until 2019 that the envisaged role and erasure concept was implemented and a commissioned processing agreement concluded with the company commissioned to operate and maintain the system. The erasure of collected access log data also occurred for the first time in 2019, several years too late. As a result, I made use of my remedial powers under the GDPR and issued a warning to the Customs Investigation Office, at the same time instructing it to finally comply with the duty to provide information when collecting personal data pursuant to Article 5 (1) (a) and Article 13 of the GDPR. My order was complied with by the Customs Investigation Office.

Advisory and monitoring visit to the Central Customs Authority

In the course of an advisory and inspection visit carried out by my staff at the Central Customs Authority, I checked the privacy-compliant management of personnel files and identified various violations of data protection law. I refrained from taking any action. Firstly, the Central Customs Authority only took on responsibility for a portion of personnel files for the first time in 2016 as a result of the reorganisation and establishment as a higher federal agency. Secondly, I could not see any direct adverse effect of the infringements on employees' rights. I will check on the promised processing of personnel files in due course.

Cooperation on the part of the Customs Administration was often characterised by a lack of sensitivity to data protection concerns, persistent denial of allegations, dismissal of evidence and failure to prosecute infringements. For the future, I hope for mutually respectful and constructive cooperation with the Customs Administration.

6.11 Data protection breaches at the Federal Police

I became aware of data protection grievances at the Federal Police (Bundespolizei, BPol) through enquiries and complaints, and was able to make improvements here. This also concerned the release of images on Twitter.

In the context of citizens' submissions, my attention was drawn to abuses of data protection law at the BPol. One case, for example, concerned the border clearance of coaches. Border crossing papers were often not returned to passengers by the Federal Police officers, but by coach drivers. My enquiries into this practice resulted in a review by the BPol and a procedural change was promised. In the future, papers are only to be returned by police officers authorised to do so.

A case examining the lawfulness of video surveillance in a railway station in the context of travel to and from a demonstration should also result in data protection improvements in the future. For example, in similar cases, video data will now be erased as soon as possible rather than after a maximum of 30 days. In addition, I have drawn attention to the fact that the review of whether video surveillance is permissible at all must be carried out more comprehensively, especially in the case of demonstrations, which regularly lie in the area of conflict between the prevention of danger on one hand and the fundamental right to freedom of assembly on the other. In December 2020, a complaint was also filed

with the Berlin Administrative Court regarding this video surveillance.

There was also room for improvement in the use of Twitter. In three cases, the BPol used a illustrative photo on which the passport of a real person was recognisable. It was possible to identify the data given in the passport, such as name, personal characteristics and the passport photo. Here, I could achieve a quick erasure.

The BMI would have the opportunity to put an end to this unlawful state of affairs. Political uncertainties should not lead to a further prolongation of this significant deficiency.

6.12 Protected border-crossing records

The Federal Police's 'Protected Border-Crossing Records' (PBCR) continues to be managed without a sufficient legal basis.

The regular PBCR inspection that I carry out also took place in 2019. It was terminated in 2020 following the final opinion of the BMI. With regard to the extent and nature of the use of the file by the Federal Police, the inspection did not lead to any formal complaints. In particular, the distinction between PBCR alerts and Schengen Information System alerts was easy to understand. I only found errors in individual alerts. Here I was able to achieve an immediate correction from the Federal Police (Bundespolizei, BPol). I asserted that there was room for improvement with respect to logging design.

Once again, I had to object to the fact that there is still no sufficient legal basis for the PBCR. The BPol maintains the PBCR file on the basis of Sections 30 and 31 of the BPolG. According to this, the BMI is legally obliged to define in greater detail, by means of a statutory order, the mere framework conditions which the BPolG stipulates for the PBCR. It cannot and must not leave this task to the executive agency, i.e. the BPol. Managing the PBCR without this legal regulation is unlawful.

I already pointed this out to the BMI in April 2015. After the BMI had still not issued a legal ordinance in 2018, I objected to the lack of a legal basis in the same year (see no. 9.3.9 of the 27th AR). Also, at the time of the 2019 inspection and as of the November 2020 editorial deadline, the BMI has not issued the constituent legal regulation. While the BMI initially expressed willingness to issue the legal ordinance, since 2018 it has been focusing on the upcoming amendment to the BPolG. However, this amendment has not even been introduced in the German Bundestag yet.

Alerts are sent out for several thousand people in the PBCR. For them, alerts can have significant consequences, such as detention, ban on leaving the country or border police surveillance. The Office for the Protection of the Constitution can also issue alerts.

7

Other individual topics

7.1 Data protection supervision in the parliamentary area

The supervision of data processing by the German Bundestag, its parliamentary groups and members raises difficult legal questions. The parliamentary groups in the Bundestag have now followed up on my recommendation to adopt their own data protection regulations. To this end, they have set up a working group in whose deliberations I am involved.

With the applicability of the General Data Protection Regulation (GDPR) as of 25 May 2018, the question arose as to what extent these regulations apply to the German Bundestag, the parliamentary groups and committees, as well as individual members of parliament, and whether they are subject to my supervision under data protection law. In the parliamentary area, personal data is processed for a wide range of purposes. For example, data from citizens is processed in the context of petitions or enquiries (e.g. from constituencies). The same applies to public relations work, for example via their own website or the many activities of members of parliament in social networks. Last but not least, members of parliament are employers and also process the personal data of their employees in this way. In my 27th AR, I initially assumed a corresponding GDPR application to data processing by parliaments and their subdivisions. Accordingly, for constitutional law reasons, I limited myself to only carrying out my advisory duties. At that time, I recommended that the German Bundestag should adopt its own data protection regulations in compliance with GDPR provisions (see no. 14.1.1 of my 27th AR).

Several data protection-related submissions on data processing by members of parliament and parliamentary groups of the German Bundestag prompted me to examine my responsibility for data protection-related control over the members and parliamentary groups of the German Bundestag, taking into account the BVerfG's case law on parliamentary autonomy. In November 2019, I informed the German Bundestag that I intend to exercise my supervisory powers under data protection

law in future in cases where I do not consider parliamentary autonomy to be affected. Since then, I have been in discussions with the German Bundestag as to how far parliamentary autonomy extends in connection with the processing of personal data by members of parliament, or where there are areas beyond this in which supervisory measures under data protection law are permissible by me, so as not to create any spaces that are free from supervision.

In the summer of 2020, the ECJ ruled (Judgment of 9 July 2020, Case C-272/19) on the basis of a submission by the Wiesbaden Administrative Court that the Petitions Committee of the Hessian State Parliament is a controller within the meaning of the GDPR. It can also be inferred from the reasoning of the Judgment that the ECJ also considers the GDPR to be directly applicable to data processing by the parliament and its members in the core area of parliamentary activities. This means that the parliamentary groups and members of parliament, like other federal public bodies, are in principle subject to my supervision under data protection law. However, I am aware that in exercising this oversight I must take into account the special position of the members of the German Bundestag as part of the legislature. Here, in accordance with the case law of the BVerfG, the principle of the separation of powers from clause 2 of Article 20 (2) of the GG and the freedom to exercise a mandate by a member of the German Bundestag (clause 2 of Article 38 [1] of the GG) must be preserved. According to constitutional law, the individual members of parliament are not deprived of all executive control from the outset. However, this is primarily a matter for the German Bundestag, which must act within the framework of its parliamentary autonomy.

The parliamentary groups of the German Bundestag are currently discussing, with my involvement, what German Bundestag data protection rules could look like, and what a data protection supervision regulation could look like, taking special parliamentary features and GDPR provisions into account. As such, for the time being I

will continue to confine myself to my advisory role vis-à-vis members of the German Bundestag.

7.2 Interdisciplinary Advisory Board for Employee Data Protection

Data scandals repeatedly illustrate that there is often little transparency or legal certainty in the processing of employee data. For many years, federal and state data protection supervisory authorities have therefore been calling for an employee data protection act. In the summer of 2020, the Federal Minister of Labour and Social Affairs appointed an interdisciplinary, academic advisory board headed by the former Federal Minister of Justice, Prof. Dr. Herta Däubler-Gmelin, of which the BfDI is also a member.

In the increasingly digitalised world of work, more and more personal data of employees is being processed through the use of artificial intelligence and big data applications. This increases the risk of employees losing privacy, which goes as far as total surveillance. Artificial intelligence in application procedures, employee screening, GPS tracking and video surveillance are just some of the challenges where regulatory gaps are becoming apparent. They make the protection of employees through clear legal regulations more important than ever. That is why federal and state data protection supervisory authorities have been calling for an employee data protection act that regulates specific processing operations and the use of new technologies in the context of employees for many years. In particular, this concerns key points such as a ban on total surveillance, limits to the monitoring of conduct and performance, and bans on the use of evidence. In response to the review mandate on employee data protection anchored in the coalition agreement of the 19th legislative period, the Federal Ministry of Labour and Social Affairs appointed an interdisciplinary and independent advisory board in the summer of 2020 to develop joint recommendations for action on an independent employee data protection act. The advisory board, chaired by Prof. Dr. Herta Däubler-Gmelin, is made up of renowned representatives from science, business and administration who consider the issues of employee data protection from a legal, ethical, philosophical and technical perspective. The Advisory Board's deliberations were still ongoing when this Activity Report went to press.

7.3 Registers in the healthcare sector

The use of data for research purposes remains a hot topic in the healthcare sector. The trend towards mandatory collection of medical data on a statutory basis continued unabated in 2020. The advantages for research and treatment must not be at the expense of the protection of the patients concerned, for example from misuse and identification. It is therefore necessary to provide for secure procedures. Potential 'side effects' must be kept in mind if data collection is to be seen as a 'cure-all'.

Implant register

I have already reported in detail on the newly established nationwide implant register in no. 4.2.2 of my last activity report (p. 28/29). It proved to be problematic here that the Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) wanted to dissolve the German Institute for Medical Documentation and Information (Deutsches Institut für medizinische Dokumentation und Information, DIMDI) and transfer its tasks to the Federal Institute for Drugs and Medical Devices (Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM). Here, I was able to ensure that this transfer did not take place through a BMG decree.

Instead, there was a formal legislative procedure to amend the relevant provisions by the German Bundestag itself. This transfer of tasks was of key importance because it resulted in the merging of various functions at the BfArM which had previously been deliberately assigned to different authorities. This problem was solved for the implant register by temporarily assigning the management of the register to the BMG. Unfortunately, this is not in line with my recommendation to create an independent registry authority. The register has not yet become directly operational. There is still a lack of a legislative decree that provides more detailed specifications. Since it is envisaged that various authorised parties, including the BfArM, will be able to use the register data for their tasks as well as universities for scientific research, it is essential to regulate access to the data by means of an appropriate procedure. A request for use must be properly reviewed. This is only ensured if the deciding body—in this case, the registry—is independent and, in particular, does not have any user interests of its own. The implant register will contain a huge number of data records on a mandatory legal basis. Therefore, special precautions must be taken here to safeguard storage and access to use.

Organ donor register

Following lively political debate, the Act to Strengthen Decision-Making in Organ Donation (Gesetz zur Stär-

kung der Entscheidungsbereitschaft) was passed on 16 March 2020 and will enter into force on 1 March 2022. This will establish a nationwide online register for documenting the declaration of organ donation. I first advised DIMDI, then the BfArM on technical implementation. A key issue here was secure authentication to ensure that the documented declaration actually comes from the designated person. The easiest way to ensure this is to use the new ID card's online feature. Unfortunately, many citizens do not use this feature yet. Therefore, alternative options had to be developed. It is also important that, if a transplant is possible, the right declaration is guaranteed. To avoid confusion, I agreed that the health insurance number could be used as a distinguishing criterion to protect data subjects. Since the health insurance number may actually only be used for health insurance purposes, this is an exception. This regulation must not lead to the use of the health insurance number as a personal identification number for allocation or identification purposes. The BfArM will not maintain the organ donor register itself, but has commissioned Bundesdruckerei to maintain the register. Unfortunately, the BfArM failed to inform me about this at an early stage.

Other registers in the healthcare sector

During the reporting period, I also dealt with the expansion of the scope of data stored in the Research Data Centre at the BfArM due to data transparency regulations. This is the account data that the health insurance providers have with respect to the persons they insure. From 2023, this will be joined by data insured persons voluntarily release for research from their 'electronic health record' (EHR).

A further collection of medical data is to be created at the Robert Koch Institute (RKI) through a central consolidation of data from state clinical cancer registers. The bill for this reached me at the end of the year. Cancer registers already exist in the federal states and contain epidemiological and clinical data on cancer. The clinical cancer registers document oncological care in inpatient and outpatient treatment throughout the course of the disease. The uniform nationwide data records contain a lot of information about the person and the treatment, including surgery, type of therapy, medication and dose. The epidemiological cancer registers are used for population-based analysis. They provide information on how frequently cancers occur in a region and at a certain age. Some of this largely statistical information has already been compiled by the RKI's Centre for Cancer Register Data (Zentrum für Krebsregisterdaten, ZfKD). It is now intended to also merge extensive data from clinical cancer registers at the ZfKD. I take a critical view of this, as merging largely duplicates the data. This contradicts the principle of data economy. It should be possible to

make the data available to various authorised persons for research purposes. The use of health data for research purposes is of importance to society as a whole. It is therefore important that the procedure for deciding on the application is designed in line with data protection law and offers the best possible protection for sensitive data concerning health.

Cross-references: 4.2 Patient Data Protection Act, 5.7 Data Transparency Regulation

7.4 Improve, but please do it right—the second decision of the Federal Constitutional Court on providing information about inventory data

In May 2020, the Federal Constitutional Court declared that the transmission provision of Section 113 of the German Telecommunications Act (Telekommunikationsgesetz, TKG) and a number of corresponding specialist retrieval provisions were unconstitutional. In doing so, it set out in detail its case law from the first ruling on providing information about inventory data from 2012. Lawmakers now have until 31 December 2021 to make improvements.

In its decision of 27 May 2020 (1 BvR 1873/13, 1 BvR 2618/13), the Federal Constitutional Court (Bundesverfassungsgericht, BVerfG) imposed new requirements on the disclosure by telecommunications service providers to security authorities of their customers' inventory data. I have already provided a detailed report on the BVerfG's first ruling on providing information about inventory data in my 24th Activity Report (see no. 6.2 of the 24th AR).

At that time, the court declared clause 1 of Section 113 (1) of the TKG to be in conformity with the Basic Law (Grundgesetz) if interpreted in a constitutional way. It has now declared Section 113 (1) of the TKG, amended as a result of the first ruling on providing information about inventory data, to be unconstitutional. In particular, due to the lack of legal clarity, the judges in Karlsruhe declared that a number of other provisions in the Federal Police Act (Bundespolizeigesetz), the Federal Criminal Police Office Act (Bundeskriminalamtgesetz), the Customs Investigation Service Act (Zollfahndungsdienstgesetz), the Federal Protection of the Constitution Act (Bundesverfassungsschutzgesetz), the Federal Intelligence Service Act (BND-Gesetz) and the Military Countersintelligence Agency (MAD-Gesetz) which correspond to Section 113 (1) of the TKG were unconstitutional. These individual powers of data retrieval are not sufficiently

limited and disregard the necessary requirements of transparency, legal protection and control.

The court requires that retrieval rules must sufficiently limit the purposes for which the data may be used. In this context, the reason, purpose and scope of the operation must also be defined for the data retrieval in a sector-specific, precise and legally clear manner. Thus, retrieval for multiple and unlimited uses throughout an agency's scope of duties is impermissible.

The court also declared clause 1 of Section 113 (2) of the TKG to be unconstitutional, since the provision is not limited to the prevention of threats to legal interests of particular importance. Moreover, information about inventory data can also be provided after administrative offences have been committed.

With the supreme court decision, information concerning stored inventory data of telecommunications customers continues to be permissible in principle. However, the BVerfG has made it clear that the legislator must create proportionate and sufficiently specific legal bases for the telecommunications providers and the security authorities carrying out the searches.

Double door model confirmed

In its decision, the court confirmed the 'double-door model' from its first ruling on providing information about inventory data. According to this provision, both the request by the security authority and the transfer of the inventory data by service providers may only take place on the basis of a separate legal basis in each case. Thus, two 'doors' need to be opened to effectively provide information about inventory data. The BVerfG has also clarified that in order for a request for inventory data to be admissible, there must be specific danger or an initial suspicion of a criminal offence in the individual case. Otherwise, higher-ranking legal interests must be affected.

If the provision of information about inventory data involves the allocation of a dynamic IP address, this intervention is of higher significance. Therefore, in addition to the specific danger in the individual case or the initial suspicion of a criminal offence, sufficiently significant legal interests must be affected. To a large extent, the challenged regulations do not meet these requirements. The legislator must therefore improve the transmission powers and the retrieval regulations for security authorities. It has until 31 December 2021 to do so. However, I recommend that the legislator should act earlier to clarify the legal situation and make it more data protection-friendly. I have also advocated for swift action by the legislator in the context of a resolution on the manual information procedure of the Conference of

Independent Federal and State Data Protection Supervisory Authorities (Data Protection Conference [Datenschutzkonferenz, DSK]) of 25 November 2020.

I had already advocated critically questioning the fundamental necessity and the very broad scope of providing inventory data information during the legislative changes in the TKG as a result of the first ruling on providing information about inventory data (see no. 6.3 of the 24th AR). In particular, my concerns regarding the proportionality of the newly formulated Section 113 (1) of the TKG were unfortunately not taken into account in the legislative process at that time and in further legislative processes.

Right to informational self-determination strengthened

With its second ruling on providing information about inventory data, the BVerfG has confirmed my long-standing criticism, strengthened the right to informational self-determination and set clear limits to inventory data information. I also criticised the vague scope and unclear purpose of many of the regulations in my comments during the court proceedings. The BVerfG also took up the argument made by me in the proceedings that so far, no documentation obligations have been imposed on public authorities with regard to the allocation of IP addresses. However, the documentation makes it possible to control the retrieval of inventory data on the basis of IP addresses under data protection law and facilitates control by administrative courts. According to the BVerfG, the legal and factual basis of corresponding requests for information in connection with the allocation of dynamic IP addresses must be put on record.

With regard to information on the basis of IP addresses, I had already pointed out during the legislative procedure that the provision of clause 3 of Section 113 (1) of the TKG is much too broad and contradicts the first ruling on providing information about inventory data. The legislator ignored the fact that this was unconstitutional. To avoid a repetition of such an error in the context of the upcoming TKG amendment, a constitutional adjustment of the

Section 113 TKG is required. I have explicitly pointed this out to the legislator during the current legislative procedure. The Federal Ministry of the Interior presented a draft bill for 'reparation legislation' in November 2020 with the aim of

designing Section 113 of the TKG and the corresponding retrieval regulations under the relevant laws in a constitutional way in the context of the second ruling on providing information about inventory data. I am of the opinion that the provisions of the BVerfG's decision have not yet been fully implemented in the 'reparation legis-

lation' and I have criticised this in the legislative process. My criticisms, however, have so far gone unheard.

Cross-reference: 5.10 Current legislation and other regulations in the telecommunications sector

7.5 Anonymisation—positioning between the GDPR and the TKG

In my position paper on anonymisation—with a special focus on the telecommunications sector—I successfully carried out the first public consultation procedure for my agency. Despite various differences of opinion among the parties involved, clear positioning was reached in the end.

On 29 June 2020, I published my 'Position Paper on Anonymisation under the GDPR with Particular Emphasis on the Telecommunications Sector'. It came about after my agency carried out its first public consultation process. Despite the high practical importance of anonymisation, the General Data Protection Regulation (GDPR) only makes very rudimentary statements on anonymisation. I took this unclear legal position as an opportunity to launch a public consultation on anonymisation—with particular reference to the telecommunications sector—from 10 February to 23 March 2020. In the course of the procedure, I received a total of 41 comments from state data protection authorities, associations, companies, research institutions and private individuals. Following the evaluation of all comments, the position paper was published on my website, together with comments for which I received consent from the parties involved. The paper is intended to show the current legal framework for anonymisation and to provide guidance to data controllers in the data protection assessment of their anonymisation practices. Ultimately, the paper should thus contribute to legal certainty.

After considering the comments, the main points of the paper are as follows: any anonymisation constitutes—for various reasons—the processing of personal data and therefore requires a legal basis. In principle, any of the permissible circumstances mentioned in Article 6 (1) of the GDPR can be considered to be a legal basis. In practice, consent and further processing under Article 6 (4) of the GDPR in conjunction with the original legal basis are likely to be of particular relevance, provided that the new purpose is compatible with the original processing purpose. The fact that the original legal basis applies in the case of further processing under Article 6 (4) of the GDPR is also made clear by clause 2 of Recital 50 of the GDPR. The processing purpose for the respective anonymisation is the actual interest of the controller behind the anonymisation—and not the removal of the personal reference.

For telecommunication service providers in particular, anonymisation is also possible for traffic and location data. For example, according to clause 2 of Section 96 (1), alternative 2, of the Telecommunications Act (Telekommunikationsgesetz, TKG), traffic data may only be used to the extent that this is necessary for the purposes justified by other legal provisions. In this respect, clause 3 of Section 96 (1) of the TKG obliges the service provider to erase other traffic data immediately after the connection is terminated. Since personal data can also be erased by making it anonymous, telecommunications service providers are in compliance with the erasure obligation of clause 2 of Section 96 (1), alternative 2, of the TKG by making traffic data anonymous. According to Section 98 (1) of the TKG, location data may be processed anonymously if this is necessary for the provision of services that add value. A typical example of this is location services.

Furthermore, any anonymisation is a continuous process and is not something that happens all at once. In this respect, the controller has the ongoing task of checking that its anonymisation procedures are valid. However, absolute anonymisation is neither technically feasible nor required by data protection law. Rather, it is sufficient that re-identification of data subjects is no longer possible from a practical perspective.

As part of the transparency obligations, the controller must inform data subjects of the purposes and legal basis of anonymisation in accordance with Article 13 (1) (c) of the GDPR or Article 14 (1) (c) of the GDPR. If anonymisation represents further processing for another purpose, the transparency obligation of Article 13 (3) of the GDPR also applies. Prior to anonymisation, a data protection impact assessment in accordance with Article 35 (1) of the GDPR must be carried out. This is because, in the case of anonymisation, the controller must regularly assume this is likely to involve a high level of risk. This is because 'large-scale processing' is usually carried out and the anonymisation technique in question falls within the notion of new technologies. Another argument in favour of carrying out a data protection impact assessment is that the generation of an anonymous dataset is a complex task for the controller and involves many sources of error.

My consultation goes hand in hand with efforts of the European Data Protection Board (EDPB) to further set out in detail the requirements for possible anonymisation techniques. The EDPB's Technology subgroup is currently planning to revise Opinion 5/2014 on anonymisation techniques in order to make it even more innovation-friendly and user-friendly.

7.6 Unencrypted tax data

Communication with the tax authorities by e-mail is typically unencrypted, meaning it could be read or altered by third parties. Some tax authorities send out a form in advance through which citizens can consent to unencrypted e-mail communication by the tax authorities. Through this consent, tax authorities are trying to comply with data protection law and maintain tax secrecy. As described in my 28th Activity Report (no. 8.3), however, effective consent to unencrypted e-mail communication with a public authority is not possible under data protection law.

Citizens have a growing need to communicate with tax authorities digitally. Only limited technical options are currently available for this purpose. The responsibility to provide a secure transmission channel lies with the tax authorities. If tax authorities want to send a document digitally, it must ensure, in accordance with Article 32 (1) (a) of the General Data Protection Regulation (GDPR), that the technical and organisational measures applied guarantee a level of protection appropriate to the risk of the data transmission. In practice, this means that non-critical data may be sent unencrypted by e-mail, while more extensive information must be transmitted encrypted.

According to the second half of clause 3 of Section 87a (1) of the German Fiscal Code (Abgabenordnung, AO), which has been newly inserted into the law since 12 December 2019, unencrypted e-mail communication by the tax authorities is permissible with the consent of all parties involved. However, I consider this regulation to be incompatible with the GDPR and therefore contrary to EU law. Consent cannot relate to the legal obligation to comply with the necessary technical and organisational measures. This is due to the fact that the technical and organisational measures to be taken by the controller are freely chosen according to Article 32 of the GDPR and thus not subject to consent. I had already expressed my doubts in the legislative procedure and had explicitly recommended that they refrain from the planned new version of clause 3 of Section 87a (1) of the AO. My statement of 11 October 2019 can be found on my website under the heading 'BfDI Transparency/Opinions'.

I have informed the tax authorities of my position. I reserve the right to exercise my remedial powers in the event of unencrypted data transmission by e-mail by the tax authorities.

The interests of citizens in the protection of their personal data and at the same time in straightforward communication with the tax authorities can be safeguarded by the tax administration providing secure communication channels, as other public authorities and private companies regularly do today. At present, citizens can typically

only choose between unencrypted digital transmission and transmission by letter by the tax authorities. The state should not be released from the obligation to take the necessary technical and organisational measures within the meaning of Article 32 GDPR. The consent solution provided for in Section 87a of the AO is unsuitable in practice to solve the problem of unencrypted e-mail communication. Consent is subject to considerable uncertainties, ranging from the question of whether it is voluntary, through to the rights of third parties that may be affected. The tax authorities bear the risk in the transmission that consent has been effectively given and is relevant at all.

When I receive enquiries from citizens, I regularly advise against giving consent to the tax authorities for unencrypted e-mail communication.

I assume that planned IT procedures for secure transmission by the tax authorities will be implemented in a timely manner and in compliance with data protection requirements.

7.7 Federal IT consolidation

The 'Federal IT Consolidation' project is intended to ensure the Federal Government's ability to work for the next few years and to guarantee efficient IT operations. Compliance with data protection is a fundamental requirement in this context, and the BfDI has a major responsibility in its implementation.

On 6 November 2019, the Federal Cabinet approved the reorganisation of federal IT consolidation, thus eliminating the previous bundling of operational consolidation and service consolidation at the Federal Ministry of the Interior, for Construction and Home Affairs (Bundesministerium des Inneren, für Bau und Heimat, BMI). Since then, the Federal Ministry of Finance (Bundesministerium der Finanzen, BMF) has been responsible for operational consolidation, while the BMI is responsible for service consolidation. In addition, BWI GmbH has left the service provider network, meaning ITZ Bund is the sole service provider for the federal administration. However, BWI can be used as a subcontractor.

The reorganisation of the operational consolidation initially blocked the progress of the overall project and caused many IT consolidation subprojects to be delayed. The lack of basic protection certification and clearance for classified information at the 'official use only' level of ITZ Bund's central data centres resulted in delays in agency projects and IT measures. Uncertainties about the future of BWI led to the almost complete cessation of tasks originally assumed by BWI.

Over the course of last year, service consolidation was able to make up for the shortfall and operational consolidation is playing catch-up accordingly. The most important service consolidation projects, i.e. the federal e-file and the federal cloud, can already be used by the authorities.

As before, my advisory role in the project mainly relates to subproject 6 'Service Consolidation'. This subproject includes several measures such as the 'federal client', the 'federal cloud', 'identity and access management' and the 'multifunctional electronic service card'.

The 'federal cloud' is defined as a standardised, scalable platform for the basic, cross-sectional and specialised procedures of federal IT. It is operated as a private cloud in the Federal Government's data centres. The federal cloud already provides services for some pilot agencies.

The 'federal client' measure involves the provision of a uniform nationwide PC workstation by the end of 2025 with a standardised operating system as well as basic and cross-sectional services, such as e-mail and document processing applications. The federal client is further developed according to plan and continuously tested by ITZBund.

To support project management for federal IT consolidation in the long term with strategic decisions, my participation in the corresponding committees was necessary, for example on the architecture guidelines. In addition, I am in regular contact with the project leaders of operational consolidation and service consolidation.

7.8 Microsoft, data protection and digital sovereignty

How do Windows 10, Microsoft 365, privacy and digital sovereignty fit together? This question has been controversially discussed by data protection experts in recent months. On 14 January 2020, product support for Windows 7 ended, increasing the pressure to upgrade to a current operating system. More and more federal agencies are moving their systems to Windows 10. The central provision of infrastructures and services is becoming increasingly critical to success, which puts cloud-based offerings in the spotlight.

Telemetry data versus data protection

Back on 7 November 2019, the Data Protection Conference (Datenschutzkonferenz, DSK) published advice on Windows 10 privacy (available at www.bfdi.bund.de/beschluesse-positionspapiere). When using the operating system, data controllers are confronted in particular with the question of how the transmission of telemetry

data to Microsoft can be justified under data protection law.

Telemetry data is technical data that is collected from the system, transmitted to Microsoft, and analysed. The company wants to use this to check the stability of the system, identify sources of errors more easily and thus improve system functionality. Telemetry data contains identifiers that allow Microsoft to recognise an individual user on an individual device and their usage patterns. It is therefore considered to be personal data protected under data protection law.

The simplest data protection solution to the problem outlined would be to simply stop the processing and transmission of telemetry data in the operating system. Microsoft had told supervisory authorities that no telemetry data would be transmitted, at least when using the 'Security' telemetry level. However, this telemetry level can only be set on certain versions of Windows 10, specifically the Enterprise and Education editions.

However, current investigations by the DSK and the SiSyPHuS study by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) came to the conclusion that even an appropriate configuration of the system does not reliably lead to the complete and, above all, permanent exclusion of data transmission.

The supervisory authorities therefore currently see no other option than to order controllers responsible for the use of Windows 10 to take measures to securely prevent telemetry data transmission. To this end, the DSK adopted a corresponding resolution on 26 November 2020 (also available at www.bfdi.bund.de/beschluesse-positionspapiere). In concrete terms, this means that in addition to the security telemetry level, controllers must also ensure by means of contractual, technical or organisational measures (e.g. by filtering Internet access from Windows 10 systems via an appropriate infrastructure) that there is demonstrably no transmission of telemetry data to Microsoft.

In my area of responsibility, I recommend that, for the use of Windows 10, the operating system is separated from the Internet, as is planned in the federal administration with the federal client as a standard workstation until 2025.

Intensive dialogue on Windows 10 and MS 365 required, including in perspective

The decisions outlined are based on an intensive dialogue with Microsoft and a joint assessment within the DSK. This exchange will also be important in the future in order to be able to derive generally valid and viable recommendations for action under data protection law.

As an example, this also applies to the current discussion about the legal improvement potential of Microsoft's commissioned processing documents in the context of MS 365. As a result, the DSK identified some deficits here, for example in the definition of what data is to be processed for what purposes, in the possibility for data controllers to check technical-organisational measures for the protection of personal data or in the information on subcontractors. A DSK working group will now contact Microsoft in order to promptly achieve improvements in line with data protection law. The discussions should also serve to achieve adjustments to the standards for the transfer of personal data to the USA or other states outside the European Union as indicated by the ECJ's Schrems II Judgement (see no. 4.3).

Digital sovereignty still a long way off

'Digital sovereignty' has now established itself as a political objective, even if no uniform, clear-cut definition is used. In essence, the aim is always to reduce dependencies on individual hardware and software providers and to counteract a growing dependence on technology. Sovereignty aims at being able to have a role in the digital that is independent, self-determined and secure. A sovereign controller under data protection law can thus freely decide on the courses of action to take in order to securely implement data protection requirements.

At the end of 2019, the consulting firm PWC presented a strategic market analysis for the federal administration to reduce dependencies on individual software providers. It was shown that the federal administration is dependent on individual providers to a critical degree. This is especially true for Microsoft, whose products are widely used and closely linked to business applications. So things don't look great for the digital sovereignty of the German administration.¹

To develop sustainable models for IT in public administration, I believe we would be well advised to take a broader view and focus on diversity and open source. The perspective use of new cloud infrastructures in particular can become an important turning point and reduce the dependency on manufacturers.

7.9 Artificial intelligence—progress

Artificial intelligence (AI) applications and algorithmically controlled decision-making processes dominate current developments in science, research, business and politics. Many areas of life are increasingly and fundamentally shaped by the enormous possibilities that AI opens up for us. In the

meantime, the weaknesses and risks of these systems are becoming apparent and need to be addressed as much as their potential.

Artificial intelligence (AI) is significant for many areas of society today. The potentially large impact of AI systems on all areas of life therefore requires clear guidelines and regulations. I firmly believe that AI applications add a lot of value to a modern, digital society. Moreover, I am sure that progress in this area can be shaped in such a way that AI can be privacy-compliant and oriented towards the common good at the same time. I am actively involved in national and international committees dealing with AI development in order to contribute to this design process.

Transparency and traceability

Algorithmic decision making, as the foundation of an AI, can add tremendous value in objectifying decisions, for example. The greater the damage potential of AI and algorithms, the more requirements must be placed on its use and the more control options must be provided. For the field of AI, transparency of decisions plays a very key role.

AI applications must therefore be repeatedly checked for legality by the relevant supervisory authorities so that violations can be punished. To this end, the supervisory authorities must be strengthened in terms of personnel. They also need improved technical equipment and ongoing staff training in order to be able to evaluate the sometimes highly complex AI systems and the algorithms behind them. Only strong data protection authorities can ensure strong independent supervision.

AI in national and international bodies

In the context of positive technology design, I want to actively accompany the developments towards AI. That is why I participated in drafting a resolution on how to deal with the use of AI at an international level, which was successfully adopted by the Global Privacy Assembly in October 2020. The paper sets out the basic requirements for the development and use of AI that it needs in order to meet accountability requirements. The aspects of risk assessment, transparency, verifiability and intervenability are very important here. The paper is available at <https://globalprivacyassembly.org/wp-content/uploads/2020/11/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf>

In its final report, the Data Ethics Commission (Dateethikkommission, DEK) also emphasises the prominent role of data protection in the field of AI. The DEK provides specific recommendations for action to shape the digital future in this area. As a member of the Commis-

¹ This was also stated by the DSK in its resolution of 22 September 2020 (www.bfdi.bund.de/entschl%C3%BCssungen)

sion, I am very pleased that data protection is of central importance here.

In addition to the DEK, numerous other bodies have dealt with the issue. As an example, the Bundestag's Enquete Commission has addressed issues relating to AI, social responsibility and its economic, social and ecological potential. I very much welcome the fact that the developments surrounding AI are being intensively discussed and dealt with in the context of political and social processes. It is now time to draw the right conclusions from this and implement appropriate measures. It must not stop at recommendations.

Human focus

The Federal Government's strategy is for Germany to expand its market share in the field of AI in the future. When implementing this strategy and the accompanying projects, AI applications must put people at the centre, while complying with data protection requirements. For example, each data subject has the right, guaranteed by data protection law, not to be subject exclusively to decisions based on automated processing. It must also be possible to actually implement this data subject right.

Precisely because technological developments in this area are dynamic and rapid, there is a need for an ongoing social debate on the application of certain AI technologies. The guiding principle of the debate must be human-centred AI.

Data protection is an essential success factor for AI applications. I am committed to ensuring that data protection in this context is perceived not only as a necessary but also as a valuable feature.

7.10 Certification and accreditation—initial procedures start

The General Data Protection Regulation (GDPR) introduces data protection-specific certification at a European level in Articles 42 and 43. This is intended to promote compliance with the Regulation and to facilitate the demonstration of conformity. The initial applications for accreditation have already been submitted. Certifications are expected in 2021.

Articles 42 and 43 of the GDPR provide the basis and framework for the establishment of a certification procedure in the field of data protection. The Member States formulate concrete specifications so that national features are taken into account. In this way, binding rules for data protection certification, directly applicable in the EU Member States, will be established.

No certification without accreditation

Data protection certifications in accordance with Articles 42 and 43 of the GDPR may only be issued by bodies that have previously been accredited as a certification body. This multi-level system serves the purpose of quality assurance and is intended to prevent a 'proliferation' of seals and test marks. This gives rise to a whole range of new tasks for the supervisory authorities.

According to Section 39 of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), the competent data protection supervisory authorities decide on whether a body may act as a certification body. They do this on the basis of an accreditation by the German Accreditation Body (Deutsche Akkreditierungsstelle, DAkkS) and in agreement with the body (see Section 4 [3] of the Accreditation Act [Akkreditierungsstellengesetz, AkkStelleG]).

Accreditation is a very complex process¹. It requires compliance with set criteria. These were developed by the independent supervisory authorities of the federal and state governments in the 'Certification' working group, a subgroup of the Data Protection Conference (Datenschutzkonferenz, DSK). The criteria have been developed in accordance with ISO/IEC 17065/2012 with a specific focus on the area of data protection. In accordance with Article 64 of the GDPR, the specifications were then submitted to the European Data Protection Board (EDPB) for an opinion. The aim is to achieve as much uniformity as possible in the specifications throughout Europe without neglecting national circumstances.

Another essential requirement for the accreditation of a certification body is the existence of a certification scheme containing appropriate certification criteria. According to Article 42 of the GDPR, these criteria must be approved. A guideline has been drawn up at a European level in this respect.² The 'Certification' working group closely followed these guidelines when formulating guidelines for national processes.

The certification procedure

If the 'granting of authority' by the competent supervisory authority has taken place within the framework of a successful accreditation, the certification body can operate on the basis of its certification scheme. In this context, it is important that quality assurance is ensured on an ongoing basis. If necessary, a certification body can be instructed by the competent supervisory authority in accordance with Article 58 of the GDPR at any time to no longer issue certifications if the prerequisites for this are not or no longer met.

² Guideline 1/2018 as amended on 4 June 2019 can be found at <https://www.bfdi.bund.de/edsa-guidelines>

The supervisory authorities are in principle free to issue certifications themselves. They do not require accreditation in this case. My agency will not offer its own certifications, as is the case for do the majority of state supervisory authorities, as things stand. I am sure that a vibrant landscape of certified accreditation bodies will emerge.

In addition to certification at national level, there is also the possibility of obtaining a European Privacy Seal. The criteria for this must be approved by the EDPB. The certification procedures approved throughout Europe are then to be included on a central list. The main steps of the process have now been adopted by the EDPB, and further details will gradually be fleshed out.³

Certification as a quality feature

Reliable and transparent procedures for accreditation and certification are a mandatory prerequisite for credible evidence of compliance with the GDPR in processing operations by controllers or processors. For this very reason, particular importance was attached to a well-founded design of the processes at both a national and European level. My goal is to create trust seals on this basis in the future. Certified data protection thus becomes an objective quality feature.

7.11 Video identification procedure—current fundamental decision of the BfDI with a spill over effect for many areas

Video identification procedures are risky. Where a very high level of trust must be achieved, they are even inadmissible under data protection law.

I have pointed out the risks regarding identification via video chat several times in the past, most recently in my 27th AR. Due to the coronavirus pandemic, I have been asked about the admissibility of video identification procedures under data protection law, since they allow identification without personal contact.

Video identification is used in many different areas of life, especially when opening online bank accounts or signing mobile phone contracts. Increasingly, consideration is being given to introducing video identification in areas where identification must meet a very high level of trust. For example, when protecting categories of personal data requiring special protection under Article 9 of the GDPR, such as in the healthcare sector.

Video identification cannot guarantee this very high level of protection. Increasingly, deceptively real-looking

audio and video manipulations—what is known as ‘deep-fakes’—can be observed. In a response of the Federal Government to a minor enquiry (BT printed matter 19/15657), the following was stated on this subject: “The work units in the departments ‘Digital Society; Administrative Modernisation and Information Technology’ and ‘Public Security’ deal with the topic in the context of remote identification. By using deepfakes, it is possible to manipulate video-based procedures. For example, a person to be identified may impersonate another person using a stolen identification document.”

In principle, several questions have to be considered when assessing the admissibility of video identification procedures under data protection law: for what purpose should they be carried out, what are the risk situations and what is the need for protection? In addition, the possible consequences for data subjects must be taken into account when assessing admissibility and the question of how data subjects are protected against the risks that arise (e.g. identity theft) must be clarified. Orientation is provided by the standard data protection model (available at www.bfdi.bund.de/sdm) with the protection requirement levels ‘normal’, ‘high’ and ‘very high’. With respect to identifications for which the protection requirement level ‘very high’ must be achieved, I reject video identification procedures without exception.

In the remaining cases, the admissibility of video identification under data protection law must be examined on the basis of data protection impact assessments, in particular with regard to the potential risks for data subjects. Provided that it is possible to reduce the risks of the processing activity to an appropriate and thus responsible level by means of accompanying technical and organisational measures, video identification procedures could be permissible under data protection law.

7.12 Impact of Brexit

The transitional period provided for in the Withdrawal Agreement between the European Union and the United Kingdom ended on 31 December 2020. The Trade and Cooperation Agreement, which has now been in force since 1 January 2021, provides for a further, maximum six-month, transitional arrangement for data transfers.

On 31 December 2020, the transitional period ended during which the UK was no longer a member of the European Union (EU) but EU law and the General Data Protection Regulation (GDPR) still applied. The Trade and Cooperation Agreement¹ negotiated shortly before the end of the transitional period now provides for a

³ EDPB's 28 January 2020 document can be found at www.bfdi.bund.de/edsa-dokumente

transitional regime for data transfers to controllers and processors in the UK.

According to this, transfers of personal data from the EU to the UK are not to be considered as transfers to a third country (Article 44 of the GDPR) in the transitional period. This period ends when the EU Commission makes adequacy decisions concerning the United Kingdom, but shall be after a period of four months at the latest. This end date may be extended by two months if none of the parties involved objects.



An adequacy decision is a determination by the European Commission, following a set procedure, that a third country provides an adequate level of data protection in line with Union law. If such a decision is made, data transfers to third countries do not require specific authorisations.

7.13 New developments in research with health data

Research using health data is of considerable importance to society. The 'new trend' towards mandatory data collection on a legal basis leads to understandable reservations. I advocate—also at an EU level—for research with data subject consent.

Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak were adopted at an EU level. In parallel, guidelines on the processing of personal data for research purposes are currently being developed by the EDPB, which will include statements on research with health data and address the issue of legal basis and data subjects' rights. In the EU, there are several Member States that directly regulate the admissibility of research with health data by law. The scope of the provision in the second half of the sentence of Article 5 (1) (b) of the GDPR has not yet been conclusively clarified: under what conditions can the purpose of research be compatible with the purpose for which the data was originally collected?

If, for example, the German legislator wants to provide a legal basis for the use of health data for research purposes, I am of the opinion that the protection of sensitive health data requiring special protection is best served if this law includes data subject consent as a condition of admissibility. If, as has been standard in Germany up to now, data subject consent constitutes the legal basis for

data processing for research purposes, then—insofar as the research project and thus the purpose of processing cannot (yet) be conclusively described—'broad consent' is possible in principle. This requires certain protective measures on the part of the responsible research bodies, which the Conference of Independent Federal and State Data Protection Supervisory Authorities specified in a resolution from 2019. These additional measures are also currently being discussed at a European level.

Nationally, the Research Data Centre for Data Transparency has been substantially expanded on a statutory basis, regrettably without providing for consent or at least a general, unconditional possibility for the data subjects to object.

In Germany, more and more registers are being established that make medical personal data available for research. Even if data processing is carried out on a legal basis, I consider it necessary that data subjects must additionally—as part of the legal basis—consent to the use of their health data for research purposes. Then they can decide for themselves whether their personal health data should be made available for research. This is because the standard pseudonymisation and encryption of data cannot usually provide absolute protection from re-identification. The more data there is on a 'case' in the register, the greater this risk is. This makes additional procedures such as aggregation, research on encrypted data or 'differential privacy' all the more important. In addition, the possibility of carrying out research on anonymised data should be examined as a matter of priority. For example, to the extent that artificial intelligence is included, the possibility of carrying out research on synthetic datasets unrelated to individuals should also be considered.

A consent-based concept is the basis for the future possible release of data from the electronic health record for the Research Data Centre in accordance with Section 363 (1) to (7) of SGB V. In many cases, data subject consent is the legal basis for even comprehensive research projects, such as the National Cohort (Nationale Kohorte) or the Medical Informatics Initiative (Medizininformatikinitiative). It is not just a tradition in Germany for human research to be voluntary. Ultimately, this right is also part of the recognised ethical standards in the research field, to which the GDPR also refers. This fundamental voluntary nature of research can be thwarted by the fact that research is carried out with sensitive personal health data without data subjects being able to object.

For this reason, care must be taken to ensure that the data subject's voluntary and informed consent is at least stipulated as a constituent element of the registers to be created in future on a statutory basis. At the very least, a

comprehensive right to object against the processing of one's own personal health data for research purposes is indispensable, which goes far beyond the possibilities of Article 21 of the GDPR.

Cross-references: 4.2 Patient Data Protection Act, 5.7 Data Transparency Regulation, 7.3 Registers in the healthcare sector

7.14 Rectification of diagnostic data

In the case of inaccurate diagnostic data, an addition to national law will help insured persons to enforce their right against health insurance providers to have inaccurate data rectified, as guaranteed by the GDPR.

During the reporting period, I received numerous complaints from insured persons who had indications that their health insurance provider had stored incorrect diagnostic data about them. Section 303 (4) of SGB V prevents a remedy for this situation, which is contrary to data protection law. According to this, in the event that data transmissions on diagnoses in accordance with Sections 295 and 295a of SGB V are incorrect or incomplete, a renewed transmission in rectified or supplemented form is only permissible in the event of technical transmission or formal data errors.

Section 303 (4) of SGB V, created through the Act to Improve the Supply of Therapeutic Appliances and Remedies (Heil- und Hilfsmittelversorgungsgesetz) of 4 April 2017, aims to prevent the inadmissible practice of various health insurance providers. Otherwise, they could subsequently influence diagnoses in order to increase the financial allocations from risk structure compensation ('upcoding', see no. 10.2.3 in the 22nd AR). This welcome objective meant that not only were inadmissible diagnostic rectifications by health insurance providers prevented, but insured persons no longer had any possibility of enforcing a rectification of their inaccurate diagnostic data stored. This curtailment of insured persons' rights is contrary to Article 16 of the General Data Protection Regulation (GDPR). The standard gives the data subject the right to obtain from the controller rectification of inaccurate personal data concerning them without undue delay.

I have drawn the attention of the legislator to the incompatibility of the national legal situation with higher-ranking European law and to the need for the law to be adjusted. With an addition to Section 305 of SGB V, inserted by the PDSG (see 4.2), the national legislator has taken on this urgent reference. According to the clause 6 of paragraph 1 of this standard, health insurance pro-

viders must, at the request of the insured person and by derogation from Section 303 (4) of SGB V, use diagnosis data that was transmitted to them in accordance with Sections 295 and 295a of SGB V and whose inaccuracy is proven by a medical certificate, in corrected form for the information in accordance with clause 1 ('insured person information') and for the transmission in accordance with clauses 2 and 3 (consent-based transmission of insured person information to third parties). The health insurance providers must decide on this application within four weeks of receiving it.

I assume that the scheme will enable insured persons to enforce their right of rectification under Section 16 of the GDPR. I will therefore closely monitor the practical implementation of Section 305 (1) of SGB V in the next reporting period.

Cross-reference: 4.2 Patient Data Protection Act

7.15 Sickness benefit case management—no consensus on the scope of the health insurance providers' data collection powers

It was not (yet) possible to complete discussions with the National Association of Statutory Health Insurance Funds (GKV-Spitzenverband) and the Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) on the privacy-compliant design of the 'Assessment Guidelines on the Incapacity for Work'.

The 'Assessment Guidelines on the Incapacity for Work' allow health insurance providers and the Medical Services of Health Insurance Providers (Medizinische Dienst der Krankenversicherung, MD) to assess cases of incapacity for work for the people they insure in a structured manner. This promotes the preservation of the ability to work or earn a living. Numerous complaints from insured persons, but also my health insurance provider inspections, repeatedly show that the understanding of individual health insurance providers regarding their powers derived from the guidelines goes far beyond the legal regulations.

Thus, if there are doubts about the incapacity for work (IW), the health insurance providers are obligated to obtain an opinion from the MD according to Section 275 (1), No. 3 b) of SGB V. However, this does not authorise them to collect additional data to substantiate or remove doubts. Insofar as this is necessary in individual cases, on the basis of the

Section 284 (1), No. 4 of SGB V, enquiries with insured persons would be permissible at best. These must be directly related to the review of formal performance

requirements. The only questions that can be taken into consideration are those about an expected follow-up IW or about planned diagnostic/therapeutic measures that stand in the way of starting work again.

I consider (remote) verbal enquiries of insured persons to be generally inadmissible. Complaints from insured persons addressed to me show that the telephone enquiries of insured persons in particular are repeatedly used by some health insurance providers for uncontrolled data collections that partly increase pressure. I have been informed of inadmissible questions about health and family situations, social problems, or details from rehab or hospital discharge reports, as well as attempts to persuade people to change health insurance provider.

Discussions with the GKV-Spitzenverband and the BMG did not result in a common understanding of the scope of the health insurance providers' data collection powers prior to commissioning the MD. Therefore, I will resume the deferred complaint procedures under Article 77 of the General Data Protection Regulation and enforce compliance with the legal requirements by supervisory means.

7.16 Division of responsibilities in the telecommunications sector

Data protection supervision and control also belong in one place in the area of telecommunications services. The previous division of responsibilities between the Federal Network Agency and myself has proven to be less than expedient in practice. Both competences should be transferred to the BfDI.

The current division of responsibilities between the Federal Network Agency (Bundesnetzagentur, BNetzA) and myself is still in need of reform. Based on the

current legal situation, I have no powers to enforce the data protection provisions of the Telecommunications Act (Telekommunikationsgesetz, TKG). Instead, I am required to submit my complaints to the BNetzA. This regulation is not in line with European primary law. In accordance with Article 8 (3) of the Charter of Fundamental Rights, compliance with data protection provisions must ultimately be monitored by independent authorities in Germany as well (see also no. 5.2 of the 28th AR). Therefore, I urgently recommend to the legislator, within the framework of the new Act on Data Protection and Privacy in Electronic Communications and Telemedia and on the Amendment of the TKG, the Telemedia Act and Other Acts (Telekommunikation-Telemedien-Datenschutzgesetz, TTDSG), to create a clear and uniform regulation of the responsibility for monitoring compliance with the protection of personal data (see also no. 5.10). Jurisdiction must be uniform, regardless of whether this protection stems from the General Data Protection Regulation, the Federal Data Protection Act or the secrecy of telecommunications (previously regulated in Section 88 et seq. of the TKG). Previous administrative practice has often taken a disproportionate amount of time to produce results, and sometimes did not produce any at all. And it is mainly due to the fact that I cannot prosecute the actual companies for violations of the TKG, but can only lodge a complaint with the BNetzA.

This is more than unsatisfactory for all data subjects. Only by clearly and exclusively assigning data protection supervision to my authority can data subjects expect consistent reviews of companies and, if necessary, sanctions in line with data protection rules.

Cross-reference: 5.10 Current legislation and other regulations in the telecommunications sector

7.17 Cyber attacks on the Institute for Federal Real Estate (Bundesanstalt für Immobilienaufgaben)

The publication of information concerning an attack of the malicious software Emotet on the website of a data subject authority does not replace the notification of data subjects when personal data has been leaked



Where a personal data breach is likely to result in a high risk to the personal rights and freedoms of natural persons, the controller must notify the data subject of the breach without undue delay (Article 34 [1] of the GDPR).

In December 2019, the Institute for Federal Real Estate (Bundesanstalt für Immobilienaufgaben, BImA) was attacked by the Emotet malware. The software managed to infect several computers of BImA employees. On 19 December 2019, the BImA published a press release on its website stating that it could not be ruled out that personal data had also been leaked.

This general notice does not replace the notification of data subjects required under Article 34 (1) of the General Data Protection Regulation (GDPR).

In this cyber attack, the first and last names and, in some cases, private e-mail addresses and bank details were disclosed in nine cases. In another case, a person's first name and surname was also disclosed in a context that could indicate a long-term illness that person had. This is health data within the meaning of Article 9 (1) of the GDPR.

I have ensured that the BImA notifies the data subjects in accordance with Article 34 (1) of the GDPR.

8

Freedom of Information Act (Informationsfreiheitsgesetz)

8.1 Individual topics

Although this is just a selection, the individual topics selected for this report from my advisory and mediation activities on the Freedom of Information Act (Informationsfreiheitsgesetz, IFG) show how broad the spectrum of content of the requests and thus of the interests of the requesting persons is.

8.1.1 Freedom of information in the pandemic

The coronavirus pandemic was the subject of conciliation proceedings and of requests addressed to me under the Freedom of Information Act (Informationsfreiheitsgesetz, IFG).

The development of the pandemic could also be traced by the emergence and content of the appeals sent to me. A large proportion of these complaints related to Freedom of Information Act (Informationsfreiheitsgesetz, IFG) applications to the Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) and the Robert Koch Institute (RKI).

At the start of the pandemic, the modalities of the Foreign Office's retrieval operation were also the subject of requests and appeals. As the pandemic progressed, the focus increasingly turned to information on case numbers, the design of testing facilities, administrative assistance by other authorities, and situation reports by the Federal Government and the Federal Ministry of the Interior, for Building and the Home Affairs (Bundesministerium des Inneren, für Bau und Heimat, BMI). IFG submissions on the Corona-Warn-App were sent to me in the middle of the year.

With more than 1000 similar IFG requests from one applicant, the request for information with the highest volume probably concerned 'savings in the business operations of the federal agencies due to the pandemic' and read:

"What were the savings in current business operations due to the COVID-19 crisis from March to May 2020 for

- ongoing business operations, e.g. electricity, water, paper, etc. through
- people working from home;
- the cancellation of events and business trips;
- the savings resulting from reductions in guard and protection services; and
- other savings?

Approximate numbers are sufficient to give me an idea here."

Since the information sought was often not available from the bodies contacted, the result for the applicant here was unproductive.

Applicants often turned to me because the one-month time limit of clause 2 of Section 7 (5) of the IFG for a decision on access to information had been exceeded. Insofar as this could be conclusively justified, as was the case in particular with the RKI, which was extremely burdened because of the pandemic, but also with the BMG, with the exceptionally high workload, I asked applicants for their understanding in this extreme, exceptional situation. I hope, however, that timely processing will be increasingly possible.

IFG requests on the subject of 'coronavirus' were also made to my department. The petitioners were particularly interested in my support of legislative procedures and in my assessments of measures such as the Corona-Warn-App, the BMG's digital offerings or the 'disembarkation card'.

8.1.2 What is actually a trade secret?

Impact of the new Trade Secrets Act (Geschäftsgeheimnisgesetz) on freedom of information

A petitioner had requested the Federal Ministry for Economic Affairs and Energy (Bundesministerium für Wirtschaft und Energie, BMWi) send them all documents relating to the EU's planned Digital Services Act. In par-

ticular, it included correspondence with stakeholders. One company, which had submitted comments on the legislative project, objected to disclosure in the context of third-party participation on the grounds that the letter contained ‘business or trade secrets’ within the meaning of clause 2 of Section 6 of the Freedom of Information Act (Informationsfreiheitsgesetz, IFG). The BMWi then granted the petitioner’s application only in part.

After they had unsuccessfully lodged an objection, the petitioner turned to me through the IFG ombudsman procedure. It considered that the interpretation should be based on Directive (EU) 2016/943 of 8 June 2016 on the protection of trade secrets, which was implemented in Germany through the Trade Secrets Act (Geschäftsgeheimnisgesetz, GeschGehG) of 18 April 2020. According to Article 2 (1) (c) of the Directive and Section 2, No. 1 b, of the GeschGehG, respectively, a trade secret must be ‘the subject of non-disclosure measures taken by its lawful owner that are appropriate in the given circumstances’. The petitioner argued that the company had waived appropriate confidentiality measures. It had sent the statement to the BMWi itself, voluntarily and on its own initiative, and had not obliged the BMWi to remain silent. There were therefore no ‘trade or business secrets’ within the meaning of Section 6 of the IFG.

Based on the previous understanding, appropriate confidentiality measures are not a feature of trade and business secrets. Since the IFG lacks a definition, the term was developed with a view to the constitutional protection of entrepreneurial activities. Accordingly, trade and business secrets are understood to be ‘all facts, circumstances and processes relating to an undertaking which are not in the public domain but are only accessible to a limited group of persons and in the non-disclosure of which the legal entity has a justified interest’ (see BVerfG 14/03/2006 - 1 BvR 2087/03, 1 BvR 2111/03, Recital 87).

The petitioner had now raised the legal question as to whether the new GeschGehG had changed the interpretation of ‘business or trade secrets’ in Section 6 of the IFG. The provisions on the scope of application (see Section 1 [2], [3], No. 2 of the GeschGehG and Article 1 [2] [a] and [b] of Directive (EU) 2016/943) go against this. In addition, according to the explanatory memorandum to the Act, the Act is not to be applicable ‘to information claims against state agencies, public law provisions on the non-disclosure of trade secrets or confidentiality obligations for members of public services’ (BT printed matter 19/4724, on Section 1 [2]—p. 23). Nevertheless, the question is controversial in the legal debate.

The question could ultimately be left open in the conciliation proceedings in question. The Ministry plausibly argued that the information allowed conclusions to be

drawn about the company’s market strategy and was therefore relevant for competition. It pointed to the confidentiality obligations of its employees, which apply even in the absence of specific confidentiality agreements (e.g. Section 67 [1] of the Federal Civil Service Act [Bundesbeamtengesetz]). The information had therefore not become public knowledge by being forwarded to the BMWi. This view is supported by Recital 18 of Directive (EU) 2016/943. According to this provision, the transmission of trade secrets to public authorities ‘shall not relieve them of their obligation of secrecy (...), irrespective of whether such obligations are laid down in Union or national law’. This suggests that sensitive commercial information does not—also—lose its status as a trade secret under the Directive merely because it is transmitted to public authorities without further confidentiality agreements. Nor does it appear that the company would have waived appropriate confidentiality measures by providing the information to an entity known to be bound to non-disclosure.

Shortly after negotiations concluded, the Federal Administrative Court (Bundesverwaltungsgericht, BVerwG) dealt with the relationship between the IFG and the GeschGehG (see BVerwG 17/06/2020 - 10 C 22.19, Recital 16), which, however, only partially contributed to the clarification: the BVerwG regards trade secrets according to Section 2, No. 1 of the GeschGehG (Article 2 [1] of Directive [EU] 2016/943) to be the minimum of what is protected by clause 2 of Section 6 of the IFG. The court assumes that the term ‘trade or business secret’ in clause 2 of Section 6 of the IFG is to be interpreted independently, but that it must be based on the evolved understanding of the term in competition law. This is open to further developments and is also shaped by the new GeschGehG. The BVerwG sees it as a guideline that protection according to clause 2 of Section 6 of the IFG must at least include trade secrets that are defined as such under the Trade Secrets Act (Geschäftsgeheimnisgesetz) or the Know-How Protection Directive, so that protection is not undermined by an authority obligation to provide information. However, the court did not define whether clause 2 of Section 6 of the IFG grants a more far-reaching protection, but considered this to be a possibility.

The boundaries of the scope of protection have therefore not yet been conclusively outlined. The further development of case law remains to be seen, in particular whether a ‘convergence’ will develop here or whether the concepts will ‘drift apart’ in their interpretation by the courts.

8.1.3 Access to records detailing processing activities

The processing records of federal agencies can in principle also be the subject of a request for access to information under the Freedom of Information Act.

An applicant requested that the Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge, BAMF), on the basis of the Freedom of Information Act (Informationsfreiheitsgesetz, IFG), send them an extract from records detailing processing activities to be drawn up pursuant to Article 30 of the General Data Protection Regulation (GDPR). The BAMF rejected this application with reference to the provision of Article 30 (4) of the GDPR, which constitutes a special provision within the meaning of Section 1 (3) of the IFG, which takes precedence over the IFG. Accordingly, the records would only be made available to the supervisory authority on request. However, a general right of inspection, as provided for in the former Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), no longer existed. The applicant then made a submission to me. The BAMF also upheld its legal opinion vis-à-vis me.

I cannot agree with the BAMF's legal opinion. Article 30 (4) of the GDPR does not constitute a special provision that takes precedence over the IFG. According to the case law of the Federal Administrative Court, the IFG is only superseded by regulations that have substantive legislative content identical to Section 1 (1) of the IFG and are understood to be conclusive (see BVerwG, Judgment of 22 March 2018 - 7 C 30/15). However, this does not apply to Article 30 (4) of the GDPR. The provision of Article 30 of the GDPR is intended to enable the supervisory authorities to carry out ex-post controls under data protection law. The performance of this control task is also served by the provision of paragraph 4, which standardises the obligation to transmit the records to the supervisory authority on request. While Article 30 (4) of the GDPR thus aims to ensure the effective performance of tasks by supervisory authorities, Section 1 (1) of the IFG grants everyone the right to access information on official documents. Article 30 (4) of the GDPR is therefore not to be seen as a special provision superseding the IFG within the meaning of Section 1 (3) IFG due to the lack of identical legislative content.

In addition, however, it is not to be assumed that the regulation is conclusive. Although the provision of Section 4g (2) of the old BDSG—which in turn is based on the requirements of Directive 95/46/EC (Data Protection Directive)—has not been adopted in the GDPR and the current version of the BDSG, there are no indications that the provision of Article 30 (4) of the GDPR should be understood to be conclusive. Rather, the regulations in Article 12 et seq. of the GDPR have created specific

obligations which are primarily intended to provide information to data subjects and which have thus replaced the provision in the Data Protection Directive on sending processing records, which were originally created for this purpose. Following the idea of GDPR transparency, the intention to exclude absolutely mandatory information of interested persons by providing the directory of processing activities also seems far-fetched.

Thus, it can be concluded that, based on the criteria developed by the Federal Administrative Court, the provision of Article 30 (4) of the GDPR is not a special provision that supersedes the IFG.

8.1.4 Federal Freedom of Information Act does not apply to the Association of German Cities (Deutscher Städtetag)

The German Association of German Cities (Deutscher Städtetag) is not a federal agency. Therefore, the federal Freedom of Information Act (Informationsfreiheitsgesetz, IFG) does not apply here. Members of the Association of German Cities are obliged to provide information in accordance with the respective state law.

A petitioner asked me to mediate because they considered their right of access to information to have been violated by the Association of German Cities.

The Association of German Cities had informed them that 'as an association, it the relevant laws which provide for a citizen's right to information against state institutions did not apply to them' and had not sent them the requested internal information.

Rightly so: in fact, the federal IFG does not grant a claim to access to information vis-à-vis the Association of German Cities.

This is because only federal agencies are obliged to provide information according to clause 1 of Section 1 (1) of the IFG. The IFG does not grant any right of access to information to private or legal persons under private law. One such body is the Association of German Cities as an association of municipalities under civil law. Private persons are exceptionally and only obliged to grant access to information if they perform sovereign tasks for the Federal Government as 'authorised persons' and thus functionally act as authorities. The Association of German Cities is a voluntary association of German cities. As the leading municipal association, it represents the interests of the cities. Federal tasks have not been transferred to the Association of German Cities. The Association of German Cities is therefore also not another federal body and also not another federal institution which, according to the wording of clause 2 of Section

1 (1) of the IFG, would in principle be obliged to grant access to information.

I ultimately recommended that the petitioner direct the request for access to information to a city that is a member of the Association of German Cities and is subject to a state freedom of information law.

8.2 Case law

In the reporting year 2020, the courts again made a significant contribution to the specification and further development of freedom of information law. It is not just the over 45,000 IFG applicants that had a great interest in the decision of the Cologne Regional Court on the glyphosate opinion of the Federal Institute for Risk Assessment (Bundesamt für Risikobewertung).

The Berlin Administrative Court clarified that direct messages from the Twitter account of the Federal Ministry of the Interior and Home Affairs are official information within the meaning of the IFG.

8.2.1 Dispute over the publication of an opinion on glyphosate: justified protection of intellectual property or censorship?

To what extent can a public authority rely on copyright law to prohibit the dissemination of official information?

The scope and significance of copyright protection for freedom of information have not yet been comprehensively clarified. In particular, the extent to which public authorities can rely on it is disputed. In the dispute, which was sometimes carried out in public, catchwords such as ‘censorship’ and ‘censorship copyright law’ were even used.

The subject of the dispute is a paper on the herbicide glyphosate. The Federal Institute for Risk Assessment (Bundesinstitut für Risikobewertung, BfR) and its own staff had written a statement on a 95-page English-language monograph on glyphosate by the International Agency for Research on Cancer (IARC). The six-page statement is a summary and contains translations of passages of the monograph selected by the BfR.

The BfR has received more than 45,000 IFG requests for access to the opinion since March 2019. Thereupon, the BfR decided by general order to make the document available to each applicant via a BfR website. Access was granted via an individual read-only access limited to seven days; it was not possible to save, forward or print the document. The BfR explicitly contradicted a publication. The BfR chose this type of access to information in order to comply with the IFG on the one hand and to protect its copyright as a scientific institute on the other.

Some petitioners contacted me because they felt that their right to access information under the IFG had been violated by the way in which the document was made available, subject to time limits and the exclusion of publication. Thus, it was not the access to information as such that was in dispute, but the restrictions on use, in particular on publication, based on copyright law.

An association—the Open Knowledge Foundation (OKF)—received the statement from the BfR via an IFG application, although the BfR had made further publication subject to approval. The association posted the document—without the BfR’s consent—in an editorial article on its website ‘Frag den Staat’ (Ask the State) for public access. The BfR warned the association and demanded injunctive relief. The action was unsuccessful before the Cologne Regional Court.

The Cologne Regional Court ruled on 12 November 2020 (Case 14 O 163/19) that the publication of the statement does not constitute a copyright infringement. The court justified its decision by stating that the BfR had published its opinion itself by granting the IFG request. The information was thus made available not only to a limited and specific number of persons, but to the general public. It follows from this that the applicant consents to further publication. Publication by the association in an article was a permissible ‘quotation’ under Section 51 of the Copyright Act (Urheberrechtsgesetz, UrhG). In addition, the expert opinion was to be qualified as an official work within the meaning of Section 5 (2) of the UrhG at the latest upon publication of the general ruling in the Federal Gazette. The general ruling demonstrates that the BfR was not interested in limiting the group of recipients.

The Cologne Regional Court continues the discussion on the relationship between copyright protection and the IFG in an interesting way. The decision is also of particular interest because the question has not yet been decided by the highest court. According to the reasoning of the regional court, even simply granting access under the IFG may constitute publication within the meaning of copyright law. If this were to apply to any grant of access to information, it would be a significant strengthening of the right to freedom of information vis-à-vis public authorities who wish to restrict the further use of information by invoking their copyright. At the time of the editorial deadline for my activity report, the judgment had not yet become legally binding.

8.2.2 What applies? The Political Parties Act or the Freedom of Information Act?

Is the Political Parties Act a special legal regulation within the meaning of the Freedom of Information Act (Informati-

onsfreiheitsgesetz, IFG)? The Federal Administrative Court has now issued a ruling.

A petitioner asked me to mediate because the German Bundestag had rejected their request for the transmission of correspondence, notes, memos and instructions relating to accountability reports and party donations for 2013 and 2014.

The German Bundestag based its refusal of access to information on the Political Parties Act (Parteiengesetz, PartG) which, as a special legal regulation of access to information according to Section 1 (3) of the IFG, excluded the application of the IFG and thus access to information according to the IFG.

I have already taken a different legal view on this in the 4th Activity Report on Freedom of Information:

it is true that according to Section 1 (3) of the IFG, special statutory access regulations take precedence, irrespective of whether they grant a narrower or a broader right of access. However, this only applies insofar as the scope of the special standard extends and it is to be regarded as a final regulation. In all other respects, the IFG remains applicable.

I see the regulations of Sections 23 et seq. of the Political Parties Act (Parteiengesetz, PartG) referred to by the German Bundestag as objective transparency regulations and therefore not as area-specific, special access regulations which exclude access to information according to the IFG (see IFG, no. 5.1.3 of the 4th AR).

The petitioner had filed a complaint against the negative decision of the German Bundestag and was successful in the first two instances. Both the Berlin Administrative Court and the Berlin-Brandenburg Higher Administrative Court ruled that 'the provisions on the accountability of political parties in the PartG are not overriding special provisions within the meaning of Section 1 (3) of the IFG which take precedence over the Freedom of Information Act and have a blocking effect' (see Berlin Administrative Court, 2 K 69.16 of 26/01/2017, Berlin-Brandenburg Higher Administrative Court, 12 B 6.17 of 26/04/2018).

In contrast to the lower courts, the BVerwG assesses the transparency regulations of the PartG as 'a self-contained regulatory concept for the publication of information relating to the accountability of parties and the development of party finances' and therefore considers access to information under the IFG to be excluded (BVerwG, judgement of 17/06/2020, Case 10 C 16.19).

8.2.3 Social media and freedom of information

Federal agency messages exchanged via social media may also be subject to a Freedom of Information Act request.

An applicant requested access from the Federal Ministry of the Interior, Building and Community (Bundesministerium des Innern, für Bau und Heimat, BMI) to the direct messages exchanged via its Twitter account. After the BMI refused access, the applicant brought an action before the Berlin Administrative Court, where they were proven right (Berlin Administrative Court, Judgment of 26 August 2020, VG 2 K 163.18). According to the court, direct messages exchanged via Twitter are also official information, as they do not exclusively and clearly serve private (personal) purposes. In that regard, it is also irrelevant that they have not become part of an administrative procedure. The court also answered the question of whether the information was available at all at the BMI in the affirmative, since the BMI could still access it via its Twitter account. It is irrelevant in this context that the messages are not stored on the BMI's own servers. Moreover, the court also rejected the grounds for exclusion put forward by the BMI.

If this case law holds, other areas of federal agency communications could be affected. Particular importance is attached to the fact that access to information does not require a record in an administrative process, but that information stored elsewhere can also be the subject of an access to information request. This applies in particular to the use of communication channels beyond the classic e-mail, such as messenger services or SMS. Provided that corresponding messages are still retrievable and thus available, a claim for surrender would be possible in principle.

The BMI has appealed the decision to the Federal Administrative Court. Further developments therefore remain to be seen.

8.3 Statistics on freedom of information

In 2020, the steady increase in my mediation work over previous years continued.

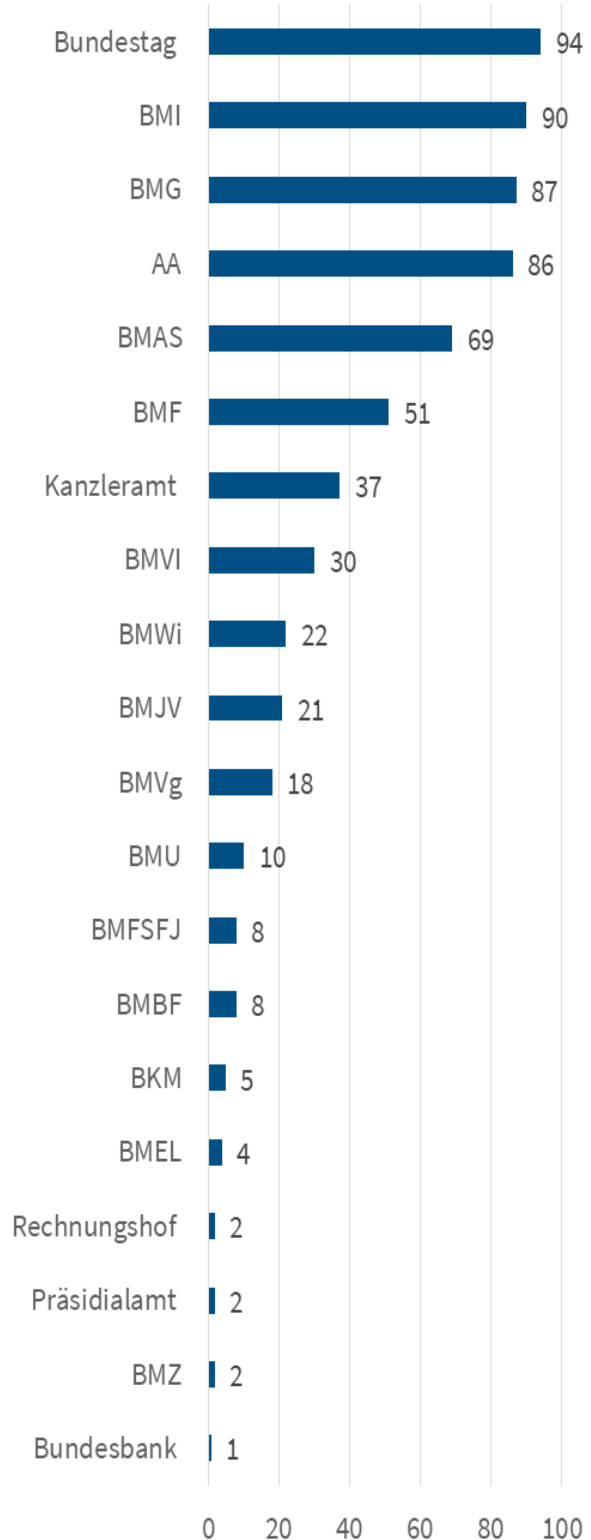
I received a total of 900 submissions during the reporting period. This corresponds to an increase of around 12 percent.

In 679 cases, petitioners called on me as ombudsperson pursuant to Section 12 (1) of the IFG. They considered that their right to access information under the IFG had been violated because information had not been made available, had not been made available in a timely manner and/or had been made available by charging excessive fees. This means that I was asked to mediate significantly more often in the reporting year than in 2019, when 461 appeals were received. This corresponds to an increase of 47 percent.

In terms of departments, the distribution of submissions was also different from that in previous periods (see chart below). This time, the focus was on the processing of the Freedom of Information Act by the Bundestag administration, the Federal Ministry of the Interior and the Federal Foreign Office. Another focus was on IFG requests to the Federal Ministry of Health, which is due to the strong interest of applicants for information in connection with the coronavirus pandemic. The content of the application included risk management of coronavirus diseases, quarantine regulations and contact tracing.

In addition to the appeals concerning violations of the right of access to information, I also had to deal with numerous general enquiries during the reporting period, mostly requesting legal information on the IFG or other regulations of the Freedom of Information Act or mediation that falls outside my responsibility.

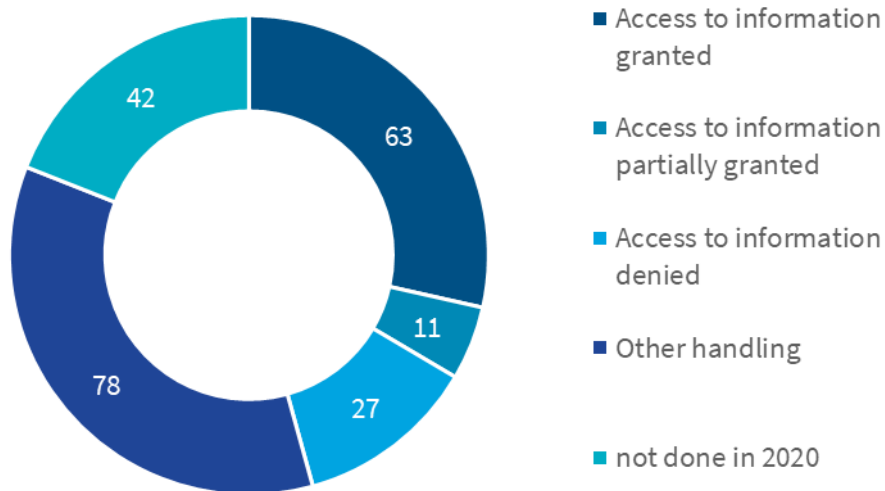
Calls according to section 12 IFG



IFG requests to my agency

During the reporting period, a total of 221 requests for access to official information were received by my agency. Compared to previous years, the volume remains stable at a high level. Among other things, the requests were directed at the provision of reports on advisory and inspection visits and my opinions on often privacy-sensitive legislative projects, but also at my files on individual conciliation procedures. The chart shows the distribution of access granted, access refused, and other settlements during the reporting period.

IFG requests to my agency



9

Controls and effects

Due to the rules on the control of the coronavirus, it was only possible to carry a few of the spot checks actually planned for 2020. For this reason, new types of controls, such as questionnaire checks, have been increasingly used.

9.1 Questionnaire checks for authentication at call centres

You can't show ID for a telephone hotline. How can and must a telecommunications company determine whether it is actually the customer calling?

A stalking case, in which an ex-partner had obtained the new mobile phone number of her former partner on the a telecommunications provider's hotline by authenticating themselves—without pretending to be the actual contracting—using their date of birth, shows that authentication is not always adequately carried out for telephone services. I imposed a fine on the company concerned, against which the company took legal action. Various fundamental legal issues were clarified in these proceedings (see no. 10.2). Among other things, the court confirmed my view that there had been a breach of the requirements for security of processing under Article 32 of the General Data Protection Regulation (GDPR).

A person's date of birth is known to many people in their private and professional environment and is therefore unsuitable for legitimising the provision of data or a change of personal data during a call. The GDPR requirements to take technical and organisational measures for data security are thus not met. In the specific case, the company had argued that it would carry out 'two-factor authentication' using the 'factors' of name and date of birth. In the field of information security, however, the term 'factor' is used differently. In addition to the data required to identify a person, e.g. name with address, customer number or user name, the factors

- knowledge (a secret, e.g. password or PIN);

- possession (e.g. a chip card or a TAN generator); and
- biometrics (e.g. a fingerprint)

are required.

The easiest way to implement this is usually a secret, e.g. a password. The user must be aware that this is a secret. This can currently be considered as a sufficient measure in many areas. However, attempts are made to spy on access data, e.g. through fraudulent e-mails and fake websites. In this respect, two-factor authentication should be the standard we aspire to, especially if a higher level of security has to be achieved (also see the Federal Network Agency's Catalogue of Safety Requirements, which was revised during the reporting period¹). Customer numbers etc. cannot be regarded as secret knowledge during authentication—at most, it is special knowledge.

Based on this incident, I conducted a written questionnaire check with the major telecommunications companies on their procedures for authenticating callers. Although all of these checks have not yet been completed, the following can already be said: the majority of the companies checked use passwords or comparably secure procedures such as a PIN. However, an alternative for a forgotten password was often offered, where only the customer number or similar data, which is not to be considered as secret knowledge, is used for authentication. Such procedures are clearly better than just asking for name and date of birth, but I still can't consider this to be sufficient either. The relevant companies—but of course, also all telecommunications companies not reviewed with respect to this issue—are called upon to implement secure and state-of-the-art procedures in a timely manner.

I found two companies to have similar insecure authentication procedures like those used in the original case, so I am looking into appropriate corrective measures.

All companies are obliged to offer sufficiently secure procedures. In this context, procedures must be reviewed on a regular basis and adapted if the technical

and organisational measures to ensure the security of processing are not (or are no longer) sufficient.

Cross-reference: 10.2 Judgement of Bonn Regional Court confirms BfDI's legal opinion

9.2 Hand scanner questionnaire check

In the second half of the year, I carried out a questionnaire check at 30 parcel service providers to examine the use of hand-held scanners in line with data protection requirements.

The delivery staff of the parcel service providers use mobile data capture devices to document the delivery of parcels to recipients and to transmit this information directly to the merchandise management system. I have received repeated submissions from citizens who are concerned that these devices are being used to capture fingerprints, make unauthorised video and audio recordings or collect unauthorised identification data. Often, the delivery staff, who were always in a hurry, were unable to answer well-founded questions from recipients.

The Postal Act allows service providers to collect certain personal information to document proper delivery or age verification. This includes the ID number, the expiry date for the ID document, the recipient's signature and, if applicable, the name of a substitute recipient. Postal service providers each use different equipment and procedures for this purpose. In addition, deliveries made during the coronavirus pandemic are documented differently to allow for low-contact delivery. This has contributed to further uncertainty among recipients.

I have sent the companies a comprehensive structured questionnaire on the device used in each case, its link to the tracking system and the verification of the processing of personal data in compliance with data protection requirements.

The result of the questionnaire check is positive. The devices, the software and the underlying processes operate in compliance with data protection regulations—for example, biometric data such as fingerprints are never collected. In most cases, this is technically not feasible at all due to the devices used—due to the lack of a fingerprint scanner. Individual data protection breaches of which I am aware in advance are usually due to operating errors, e.g. incorrect data being displayed to a recipient in the shipment tracking system. Structural deficiencies in terms of data protection, such as the possibility of unintentional data transfer to third parties or the collection of too much personal data, could not be identified. The hand-held scanners used by the delivery

staff of parcel service providers are used in compliance with data protection regulations.

9.3 Change of official Data Protection Officer in the Federal Ministry of Defence

Deficiencies with respect to the independence of the official data protection officer in the Federal Ministry of Defence were eliminated through my intervention.

The Bundeswehr Data Protection Officer (Beauftragte für den Datenschutz der Bundeswehr, BfDBw) in the Federal Ministry of Defence (Bundesministerium der Verteidigung, BMVg) was assessed in the course of an advisory and inspection visit. My staff found that the current organisational position and integration of the BfDBw within the BMVg unduly restricts their independence and freedom to issue instructions. In particular, the lack of a direct right of presentation to departmental management and the integration into ministerial line organisation met with data protection concerns. The procedures for the approval of business trips and further training of the BfDBw and their staff, their respective official assessment and the organisational integration of outposts were also incompatible with the BfDBw's statutory independence. As a result of the data protection check, the direct right of the BfDBw to present to management was laid down in the BMVg's internal regulations. The BfDBw was detached from the line organisation of the BMVg and was directly subordinate to the Office of the State Secretary. To independently carry out its tasks, the BfDBw was granted a permanent duty travel permit for Germany as well as more extensive possibilities with regard to foreign business trips and training measures. To ensure the independence of its employees, the BfDBw has been entrusted with their official evaluation. In future, the official assessment of the BfDBw itself will be carried out by the State Secretary. To maintain the independent performance of tasks in the field offices of the BfDBw, the posts located there were subordinate to the BfDBw. These measures have sustainably strengthened the independence of the BfDBw and thus data protection within the Bundeswehr.

9.4 Advisory and inspection visits on the application of the Freedom of Information Act

My advisory and inspection visits to the Federal Agency for Civic Education and the Federal Agency for Technical Relief produced pleasing results.

Federal Agency for Civic Education

My inspection visit to the Federal Agency for Civic Education (Bundeszentrale für politische Bildung, bpb) showed that the application of the Freedom of Information Act (Informationsfreiheitsgesetz, IFG) is carried out in a citizen-oriented and service-oriented manner and that the procedural regulations as well as the substantive legal requirements of the IFG are observed. The inspection was carried out on the basis of the evaluation of a large part of the IFG procedure files from 2016 to 2020. The processing of IFG applications and the involvement of the specialist departments is concentrated at the central 'Communications' unit, which also acts as a press office and is also responsible for citizens' enquiries. This ensures the fast and reliable allocation, and expert and service-oriented processing of the different requests for information. The processing of applications is consistently rapid and decisions and access to information are regularly made within the one-month time limit without any difficulties.

Federal Agency for Technical Relief

The Federal Agency for Technical Relief (Technisches Hilfswerk, THW) also demonstrates a citizen-oriented and service-oriented approach to IFG requests and observes the material as well as the formal requirements of the IFG. I was able to view all IFG case files from 2016 to August 2020. IFG applications are processed centrally by THW management in Bonn. If IFG applications are received by the non-independent eight regional or 668 local THW associations, they are forwarded to the responsible central department. Processing after forwarding is consistently speedy. The inspection of record keeping did not reveal any anomalies. I gave advisory advice and suggestions in individual practical points, such as fees. Using the example of IFG applications from the group of helpers, I had the THW explain the implementation of data protection in IFG procedures to me; I did not see any indications of irregularities, such as standardised comparisons with data for other purposes. The THW provides basic information on access to information online.

9.5 Controls in the security sector

In addition to mandatory inspections required by law—this time at the Federal Office for the Military Countersintelligence Service (Bundesamt für den Militärischen Abschirmdienst, BAMAD)—I was able to conduct a number of important advisory and inspection visits in the security sector despite pandemic-related restrictions. Among other things, the focus was on the transfer of data to security authorities in third countries as well as the implementation of the requirements of the Security Clearance Act.

9.5.1 Checks and complaints in the area of the Federal Office for the Protection of the Constitution

At the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV), I checked data processing in connection with alerts in the second-generation Schengen Information System (SIS II), with searches in the Visa Information System (VIS) and with data transmissions of the Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge, BAMF) during the reporting period.

Discreet tender checks in the SIS II

In the first quarter, I checked discrete tenders in the SIS II at the BfV. The BfV may initiate tenders in the SIS II if the information to be obtained in this way is necessary to avert a serious threat posed by the data subject or other serious threats to national security. In addition to documentation deficiencies, the main finding in the operations checked was that the volume of data exchanged between the authorities involved was not covered by the European rules on SIS II. The storage and erasure processes also need to be revised in line with legal requirements.

At the time of going to press, no response to my inspection report had been received from the responsible Federal Ministry of the Interior, Building and Community (Bundesministerium des Innern, für Bau und Heimat, BMI). In 2021, I expect further constructive discussions on my findings and the resulting necessary changes in data processing at the BfV.

VIS search checks

I also checked BfV searches in the VIS at the start of 2020. Such searches may be carried out by the BfV if they make a considerable contribution to the prevention or detection of serious criminal offences and are necessary. During the inspection, it became apparent, among other things, that the documentation and verification of the existence of the search prerequisites did not comply with the legal requirements and that the storage period

of the data searched for had to be structured in a more differentiated manner.

I received the BfV and BMI statement shortly before the editorial deadline for this report. I will now evaluate these and assume that this will also be followed by a further exchange on any adjustments to data processing that may still be necessary.

Data transfer checks between the BAMF and the BfV

In the third and fourth quarters, I also examined aspects of the BAMF's data transfers to the BfV pursuant to clause 1 of Section 18 (1a) of the BVerfSchG. The BAMF may transmit to the BfV information on persons which it collects in the performance of its duties if it finds factual indications that such information is required for the collection and evaluation of anti-constitutional endeavours or activities within the meaning of Section 3 (1) of the BVerfSchG. The inspection revealed, among other things, that the criteria established in practice by the BfV, which the BAMF uses to make transfers, need to be revised. The criteria do not guarantee in every case that there are actual indications that the BfV is relevant to the task. This issue will also be discussed with the BfV and the BMI as next steps.

9.5.2 Anti-terror file checks

At the Federal Office for the Military Counterintelligence Service, I carried out a compulsory check on the use of the anti-terrorist file. Based on the findings of the 2018 inspection, I also tracked the possibility and impact of additive encroachment on fundamental rights. This resulted in a considerable amount of control work.

No data protection breaches were found during this year's inspection of the anti-terrorism file (Anti-Terror-Datei, ATD) at the Federal Office for the Military Counterintelligence Service (Bundesamt für den Militärischen Abschirmdienst, BAMAD). The same applies to the inspection carried out in 2018. However, as a follow-up to this review, I conducted a review for 'additive encroachment on fundamental rights' in 2019 and now conclusively in 2020.

In the course of the participation of several authorities in the ATD, data records on one person may be used and stored by several authorities. According to Section 1 (1) of the Act on the Anti-Terror File (Antiterrordateigesetz, ATDG), in addition to federal agencies, the authorities involved are the state criminal investigation offices and the constitutional protection authorities of the states. This can result in an 'additive encroachment on fundamental rights', especially if, in addition to being stored in the ATD, one and the same person is simultaneously observed by various authorities using measures used

by intelligence services or the police. Measures that are proportionate in isolation may therefore become disproportionate.

To be able to assess this, an overall view and interaction between different supervisory authorities is necessary. Therefore, during the reporting period, in connection with the 2018 inspection, I asked the Federal Criminal Police Office to provide log data showing which agencies made or obtained searches with hits on records stored by the BAMAD. As a result, several federal and state agencies could be identified. Thereupon, I wrote to the state data protection commissioners (Landesdatenschutzbeauftragte, LfD) responsible for these authorities and asked them to check, because checking search requests by state authorities for data files of federal agencies is the responsibility of the respective LfD. My colleagues in the responsible state authorities also supported me accordingly in this review.

In terms of content, neither violations of data protection law nor additive unlawful encroachments on fundamental rights were identified. However, the examination of whether there were additive encroachments of fundamental rights produced different results. In some cases, no further action was taken by the requesting authority as a result of search queries with hits. In some cases, the underlying data had been—lawfully—erased in the meantime, as the time of the query had already been some time ago. There were also technical and organisational challenges that made it difficult for the LfD to carry out a review. Other queries did not yield a positive result, i.e. apparently the person searched for did not match the person stored by the BAMAD.

Overall, it was found that this type of review involved a considerable amount of additional work. It took me about eight months to complete the entire process. With a data protection check of the ATD to be carried out every two years for the federal agencies involved, this time aspect represents a major hurdle for the evaluation of a possible additive encroachment on fundamental rights.

In the 2017-2018 Activity Report, I had already noted that the effort expended by the authorities in storing, maintaining and erasing the data from the ATD and the RED is very high and apparently disproportionate to the benefit involved for them (see numbers 9.3.5 and 9.3.11 of the 27th AR). Despite the emerging routine in the checks for these files on the part of the BfDI, the effort also remains high in my agency. Since the cost-benefit analysis for the agencies that store the data is so negative, I continue to recommend that both files be abolished.

9.5.3 The case processing system at the Federal Criminal Police Office

The case processing system (CPS) is a central tool for day-to-day work at the Federal Criminal Police Office (Bundeskriminalamt, BKA) with respect to electronic information. Its current design still shows considerable deficiencies in terms of data protection law.

The CPS is used to create and process operations. It also offers various functionalities relevant to police case processing, such as case management and documentation, as well as search options in the data collected there, etc.

During an earlier advisory and inspection visit, I identified and objected to considerable data protection deficiencies in CPS data processing at the BKA. I provided detailed information on this in my last activity report (see 6.7.3 of the 28th AR).

I particularly objected to the following:

- the lack of delimitation of the data stored in the CPS for different purposes;
- the assignment of access rights in the CPS;
- the ‘file circular run’ function,
- the lack of specification of deadlines for selection tests;
- the storage of files on group drives as a ‘file substitute’; and
- no option to flag data collected in covert actions.

In the meantime, the Federal Ministry of the Interior, Building and Community (Bundesministerium des Inneren, für Bau und Heimat, [BMI]) informed me that the CPS had already been functionally adapted at the end of 2019 in such a way that data from particularly intervention-intensive measures could be marked so that their origin could be identified. Apart from that, it was intended to standardise the use of the CPS as far as possible with regard to the deadlines for segregation checks and case management, taking into account the range of BKA tasks. To guarantee complete, audit-proof and uniform file management in the BKA, the introduction of a demand-adapted electronic file is planned.

With regard to the deficiencies in documentation and file management that I have identified, the BMI does share my view that these require comprehensive restructuring. The design phase should be completed by mid-2021. However, it is both regrettable and astonishing that the conceptual design of such urgently needed changes should only be completed almost two years after my inspection report was sent and that actual implementation should take place even later.

Other—especially central—points of the objections have not yet been picked up by the BMI.

What is very fundamental for me is the need for a separation between the different purposes for which the BKA processes personal data in the CPS. In this respect, the BMI takes the legal view, e.g. with regard to the processing of personal data for case management and for the documentation of police actions, that Section 22 (2) of the BKAG permits storage in particular in cases in which the necessity of further processing for the performance of tasks cannot yet be assessed and it cannot be ruled out that the data in question could be of use to the police at a later point in time. ‘The data can’—according to the BMI—‘be kept and, if necessary, supplemented with further findings until a decision can be made on the necessity of storage for the fulfilment of the task or until the data is separated out or has to be erased due to the expiry of maximum storage periods’.

Such a view has no basis in law and contradicts the basic understanding of constitutional law, according to which data may only be stored for specific, precise and clearly defined purposes from the outset. As early as the time of storage, it must be sufficiently ensured that the data is only used for purposes that justify the weight of the data storage. This is settled Federal Constitutional Court case law. It is not permitted to store data in a stockpile in case it might be ‘useful’ for the performance of police tasks at some point in the future.

I will press for a prompt privacy-compliant design of the CPS at the BKA and, if necessary, take appropriate measures to remedy the identified deficiencies in accordance with Section 69 (2) of the BKAG.

9.5.4 International BKA data transfers

In 2016, the Federal Constitutional Court made statements on the requirements for the transmission of data by the Federal Criminal Police Office (Bundeskriminalamt, BKA) to public agencies abroad (Judgment of 20 April 2016, Case BvR 966/09) for the first time. Therefore, the legislator had to establish regular inspection intervals every two years. This year, I attended an obligatory advisory and inspection appointment at the BKA and examined selected data transfers to the Russia, Qatar, Japan and Israel. The BKA has put some effort into mapping out the legal issues and training the departments. In individual cases, however, I nevertheless identified data protection deficiencies and objected to them.

Data transfers to third countries (states outside the EU) represent daily ‘bulk business’ for the BKA. It is therefore worth mentioning on a positive note in my inspection that the BKA endeavours to provide regular training to all the relevant departments and to raise awareness of the issue.

The legal regulations provide for an examination of the level of data protection law in each country in accordance with the provisions of the Federal Data Protection Act. A distinction must be made here between whether the EU has adopted an adequacy decision for the country in question and whether appropriate safeguards are laid down in a legally binding instrument. In order to assess the respective level of protection, the BKA—also in cooperation with the Federal Office of Justice—makes use of a wide range of information, e.g. annual reports on human rights, reports by the Federal Foreign Office, bilateral agreements and other agreements. However, the requirements to be met by suitable guarantees in a legally binding instrument have not yet been conclusively clarified at either national or European level.

As a result, however, this assessment is more of a dogmatic nature for the BKA than of practical relevance. The national legislator has provided for data transfers to third countries to be examined in each individual case to ensure that the recipient of the transfer handles the data in a manner that is appropriate in terms of data protection law and safeguards fundamental human rights. In my inspection, I was able to establish that the BKA also predominantly carries out this case-by-case examination.

Only in two cases did I issue a complaint: these were cases where data transfer had been requested by a third country to the national police authorities. In such cases, the respective country's authority may ask the BKA to take over the exchange of data with the requesting country. The BKA then acts in a 'correspondence role' provided for by law.

In such constellations, the BKA assumes that a substantive review of the legality of the data transfer is carried out by the respective country's authority. In the instance of a case examined on site, I urgently advised the BKA to carry out at least a summary legality check, since the BKA is responsible under data protection law for the data transfer, including in this correspondence role. The BKA does not act here as a mere 'messenger', but conducts the correspondence independently. This is a statutory task of the BKA, not mere commissioned processing.

In another case, the Japanese authorities investigated (predatory) theft and approached the BKA. The BKA asked the competent state police authority for information on the data stored about the data subject. The BKA transmitted to Japan almost all of the data provided by the state police authorities without, however, first checking on what suspicion the data subject was even stored. In addition, the Japanese authority was informed that the data subject was classified here as being 'politically-motivated-left'. I consider the data quality and data validity to be insufficient. Moreover, the transmission went

beyond the scope of the data requested by the requesting authority. I therefore objected to the BKA's approach as a violation of the principle of necessity.

9.5.5 General contribution on Security Clearance Act checks carried out

The data protection checks of the requirements of the Security Clearance Act (Sicherheitsüberprüfungsgesetz, SÜG) at two public agencies and one commercial enterprise revealed room for improvement in the maintenance of security files and data files as well as in communication between the agencies involved.

During the reporting period, I inspected two federal agencies and one commercial enterprise to determine whether they were complying with the data protection requirements of the SÜG.

The first job was the assessment centre for Bundeswehr leadership. The subject of review was a recruitment test for male and female soldiers as Bundeswehr leaders. Since 2017, all servicemen and women have been required to undergo at least a simple security check when they are first appointed to a post, in accordance with Section 37 (3) of the Military Act (Soldatengesetz).

I also checked the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV). Here, the check related to security checks for the BfV's own employees.

The commercial enterprise inspected was a company from Bonn. The subject of review in this case was the security clearances for classified information.

In all three cases, I found isolated violations of the requirements on how security files should be maintained. These range from incomplete files to inadmissible documents in security files to files that were overdue for destruction.

There were also errors in individual cases in the files examined, which may be kept in order to facilitate procedures. These concerned the unauthorised storage of data or the failure to erase such data.

In addition, in the case of the company inspected in particular, there were serious shortcomings in the communication between the staff administration and the body responsible for security clearance. For example, the body responsible for security clearance actively received no or very late notification from the staff administration regarding security-cleared persons leaving employment.

At the time of going to press, the checks at the assessment centre for Bundeswehr leaders had already been completed. In the remaining two cases, the inspected bodies still have the opportunity to comment. However,

the inspected bodies have shown a willingness to cooperate and have already corrected some of the deficiencies found. I can also report constructive cooperation with the inspected bodies in the follow-up for the inspections.

10 Internal developments within the BfDI

10.1 Courses for action by the BfDI if legislation is contrary to European law

National regulations must be in line with the General Data Protection Regulation (GDPR). If this is not the case, the implementation of these regulations may violate the GDPR. I try to counteract these cases in the legislative process by issuing corresponding opinions and, if necessary, announcing to the bodies under my supervision that supervisory measures will be taken if they apply the national regulations despite this being in violation of the GDPR.

If a draft law shows that regulations do not adequately meet GDPR requirements, I bring this up at an early stage in the legislative process as part of my comments. Examples of this are some regulations in the Patient Data Protection Act (see 4.2). As an example, Section 342 (2) (2) (b) of SGB V only provides for users of suitable end devices such as mobile phones or tablets to have sufficient access to their own electronic health record in accordance with data protection law, and only from 2022. Irrespective of the associated unequal treatment in the exercise of the right to informational self-determination from 2022, the regulation in the first implementation phase violates the principle of necessity. This is because, at this stage, all service providers to whom insured persons grant access to their data are given access to all of the information contained therein. And this is regardless of whether it is required for the specific treatment. Another example is the second half of the sentence in clause 3 of Section 87a (1) of the German Fiscal Code (Abgabenordnung), according to which unencrypted e-mail communication by the tax authorities is permissible if all parties involved have consented to this (see 7.6). This is contrary to the fact that the provisions of the GDPR, which oblige the controller to comply with technical and organisational measures, are non-negotiable.

I have the legal mandate to raise awareness and advise the bodies under my supervision about the obligations arising for them from the GDPR, the Federal Data Protec-

tion Act and the other regulations on data protection. Therefore, I am also communicating my position on this matter to the bodies affected by the respective new regulation. In addition to the formal warning that intended processing operations are likely to violate the GDPR due to its primacy, I reserve the right to exercise the other remedial powers available to me in the event that the new provisions are not implemented in compliance with the GDPR. These are regulated in Article 58 (2) of the GDPR. Among other things, the instruction to bring the processing operations in breach of European law in line with the GDPR may be considered. In addition, a ban of the processing operations concerned is also possible.

Cross-references: 4.2 Patient Data Protection Act, 7.6 Unencrypted tax data

10.2 Ruling of Bonn Regional Court confirms the BfDI's legal opinion

In its ruling of 11 November 2020, the Regional Court of Bonn clarified essential questions of principle with nationwide and European-wide significance regarding the liability of companies for fines under the General Data Protection Regulation (GDPR) and, in doing so, largely followed my legal opinions. Liability is not limited to violations by executive bodies or management staff. In addition, the fine must be based on the turnover of the 'economic entity'. In the specific case, the regional court only considered a minor infringement and therefore reduced the fine amount.

In my last activity report, I reported on a fine imposed on 1&1 Telecom GmbH (see Annex 2 to the 28th AR). In my decision about the fine, I had alleged that the company had at times failed to adequately protect its customer data when providing customer service by telephone. Thus, there was a risk that unauthorised third parties could obtain further customer data simply by knowing the customer's name and date of birth. To prevent this, in my view, callers' entitlement needed to be appropria-

tely checked (authentication). In my view, knowledge of the customer's name and date of birth was not sufficient in the case of the data concerned. During my administrative offence proceedings, 1&1 Telecom GmbH had promptly adjusted its internal measures to ensure a higher level of protection. As part of its telephone customer service, the company now uses a PIN solution to authenticate its customers. Because of this case, I have also inspected other telecommunications providers with regard to telephone authentication measures, have worked towards any necessary changes and am examining whether supervisory measures are required (see 9.1).

After the company lodged an appeal against my decision to impose a fine, the matter of the fine was passed on to the Bonn Regional Court via the public prosecutor. In its ruling of 11 November 2020, the regional court upheld my decision about the fine on the merits, but imposed a reduced fine. Beyond the specific case of fines, the ruling is ground-breaking for the entire nationwide and Europe-wide enforcement practice under the GDPR and brings more legal clarity and security for companies and supervisory authorities. In particular, the regional court confirmed many of my legal opinions which had previously been challenged by trade associations. At the same time, the court gave important guidance to data protection supervisory authorities on how to set fines that are effective, proportionate and act as a deterrent.

For example, the regional court confirmed that under the GDPR, the liability of legal persons is not limited to infringements committed by bodies or managers. The direct association liability of the GDPR is in this respect paramount and leaves no room for deviating regulations of the German legislator, for such regulations would distort fair competition within the EU and contradict the GDPR's objective of uniform sanctioning. The provision of Section 30 (1) of the Administrative Offences Act (Gesetz über Ordnungswidrigkeiten, OWiG) is thus incompatible and inapplicable on the basis of the 'primacy of application' of Union law.

In addition, company structures are often complex. They may consist of parent companies and several subsidiaries, which either some of or all of are controlled by the parent company and between which economic values are shifted. From an economic point of view, they can then form an overall unit together. In its decision, the Bonn Regional Court confirmed that the question of the upper limit of a fine must be based on the total turnover of the economic entity and not just on the turnover of the subsidiary. It therefore follows the stated wishes of the European legislator.

Fine recalculation by the court

When assessing the specific fine, both the offence-related aspects of Article 83 (2) of the GDPR and the overarching sanctioning principles of Article 83 (1) of the GDPR must be taken into account. The principles of effectiveness, proportionality and deterrence also allow for the consideration of individual sensitivity to punishment, as the court clarified. This can vary depending on the size of the company. Thus, GDPR fines also concern fundamental questions regarding the equality of liability. This is because the identical amount of the fine can have a disproportionately greater economic impact on a micro-entrepreneur than on a large company. The court confirmed that turnover and other economic factors can provide initial guidance for determining the amount of the fine. This is a clear rejection of trade association demands that turnover should not play a role in the assessment. This initial guidance shall then be adjusted as an increase or decrease by taking due consideration of the seriousness of the offence.

The fact that both the seriousness of the offence and the size of the undertaking must be taken into account was already in line with the established practice of data protection authorities. However, new evidence emerges from the court's subsequent observations: The lighter or more serious the infringement, the greater the weight of the seriousness of the offence compared to the size of the undertaking. In practice, I believe that even in the case of very minor and very serious infringements, particular attention will have to be paid to ensuring that the size of the undertaking does not become so insignificant that fines could be ineffective in relation to large undertakings or disproportionate in relation to micro-undertakings. This would be contrary to the overarching sanctioning principles of Article 83 (1) of the GDPR.

In the specific case of 1&1 Telecom GmbH, the regional court only considered the infringement to be a minor one when applying the assessment criteria outlined above and therefore reduced the amount to just under one tenth of the fine originally imposed. Applying the above-mentioned method of assessment, the fine imposed by the court is comprehensible and should be sufficiently effective, at least from a special prevention perspective, due to the general data protection sensitivity of 1&1 Telecom GmbH.

The judgment is now final

The considerations of the regional court on the assessment of the amount of a fine under the GDPR are of particular interest both for the further development of the German concept of fines and for the development of European guidelines on fines. I have therefore introduced and discussed them with my sister authorities at both a German level and a European level. In this context, it

is important to me that, following the consultations, we will arrive at an approach that is as uniform as possible throughout Germany and Europe. However, this requires not only the publication of joint papers, but also and above all law enforcement and sanctioning practice that is lived accordingly.

10.3 Staffing developments in 2020

From 2016 to 2020, the German Bundestag almost tripled the positions available to the BfDI to 324.9 positions. Despite the pervasive coronavirus pandemic, we managed to fill about 80 percent of those positions in 2020. Thanks to the early recruitment of junior staff and a new planned staff development and promotion concept, I believe I am well equipped for the future.

Since 1 January 2016, the BfDI has been the youngest, independent supreme federal agency. Previously, it was part of the Federal Ministry of the Interior, Building and Community and did not require its own organisational or staffing substructure. Sufficient organisational and personnel resources are required to ensure my ability to work. While my department had 110.5 positions in 2016, the year it became independent, I have since seen a further increase in positions to a total of 324.9 positions. For 2020 alone, I was granted a total of 67 positions by the budget legislator to supervise security agencies and carry out new tasks.

To fill vacant positions in 2020, despite the coronavirus pandemic, I conducted a total of 14 selection processes, including collective advertisements for several positions. I also resorted to the use of modern in-house video conferencing technology to find qualified staff. In 2020, of 361 applications received, a total of 185 people were presented to my department, from which I was able to recruit over 50 new colleagues. This has allowed me to fill more than 250 positions out of a total of 324.9 positions. I am confident that I will be able to fill most of the remaining vacancies in my department over the next year, especially in view of the additional 23.5 positions that the budget legislator granted me. I have already set the course for this in 2020 and, following the move to Graurheindorfer Straße, have again invited more students and trainee lawyers to complete their practical training periods with me in order to attract and retain junior staff. I am also currently working on an updated staffing development and promotion concept adapted to the modern working world.

To ensure regular and efficient data protection supervision, my office, as the supervisory body for security authorities and intelligence services, has been staffed in

such a way that the compensatory function required by the Federal Constitutional Court can be fulfilled efficiently. The increase in staff not only made it necessary to restructure the police and intelligence services, turning the original four units into six, but the groups were also renamed as departments in order to bring them into line with the terminology used by federal ministries and other authorities. I am grateful to the legislator for supporting me in continuing to strengthen my data protection oversight.

Should further tasks be added to my current activities or should increased measures be necessary due to legal as well as technical developments, a further increase in staff would be necessary.

10.4 New premises

Modern workplaces, improved accessibility and security – the BfDI moved into new premises at the Bonn site in May 2020.

On 25 May 2020, BfDI management symbolically accepted the key for a new office building on Graurheindorfer Straße in Bonn. After several months of intensive renovation and relocation, an important goal was achieved on schedule: the consolidation of all workplaces at the Bonn location in a modern equipped property. The two previous buildings were no longer sufficient for the space requirements of the growing authority. When equipping the building, the focus was on compliance with safety standards on the one hand: the fast-growing area of police and intelligence services monitoring requires particularly secure networks, bug-proof rooms and strict access controls. On the other hand, special attention was paid to accessibility during the renovation work. This provides both employees and visitors with the best possible conditions for working and staying in the office. Another focal point for equipping the building was modern information and communication technology. Meeting rooms with up-to-date video conferencing technology meet the need for modern means of communication. The move has now created very good and sustainable working conditions for BfDI employees.

10.5 Press and public relations

The public's need for information on data protection and freedom of information issues remained strong in 2020. To comply with the legal mandate to raise awareness and educate society on my issues, I therefore further expanded my press and public relations work. Among other things, I have also been active in the decentralised and particularly privacy-friendly microblogging service Mastodon this year.

Public relations

Media interest in my work continued to grow during the reporting period. This is also shown by the thematic diversity of the requests:

the main interest was on data protection issues relating to the coronavirus pandemic. Even during the development phase of the Corona-Warn-App (see no. 4.1.1) in spring, I was very often asked for my assessment. The second wave of the pandemic was also noticeable in the press enquiries from November onwards, when there were high-profile calls for the further development of the app.

The topic of data protection in the healthcare sector is generally met with a high level of journalistic interest. This was due not least to the large number of legislative projects in this area. The introduction of the electronic health record in particular (see point 4.2) and the behaviour of the various stakeholders in this context raised new questions. The medical press asked for information that was sometimes very detailed here.

Legislative projects outside the healthcare sector were also the subject of press enquiries, for example the planned register modernisation (see no. 5.1).

In addition, individual events often led to enquiries. Here, the reporting on the US platform Clearview, the European Court of Justice's Schrems II Judgment (see also 4.3) and the ruling of the Federal Constitutional Court on the Federal Intelligence Service (see also 6.3) should be mentioned in particular.

In the case of several enquiries, I referred to my responsible colleagues in the federal states, since I repeatedly receive enquiries, for example, about Deutsche Bahn (competent supervisory authorities in Berlin and Hesse), Facebook and Google (competent supervisory authorities in Hamburg and Ireland, respectively) and SCHUFA (competent supervisory authority in Hesse), for which I have no legal responsibility. The same applies to enquiries regarding companies that don't have their headquarters or head office in Germany, such as PimEyes (competent supervisory authority in Poland), ByteDance or TikTok.

In addition, I issued 30 press releases during the reporting period and was a guest at the Bundespressekonzferenz (Federal Press Conference) on two occasions. I also wrote twelve guest articles or essays for various media.

Social media

In October 2020, I set up my own instance of the decentralised microblogging service Mastodon. I run an official authority account there (<https://social.bund.de/@bfdi>). By doing so, I want to give interested citizens the oppor-

tunity to exchange ideas using a more privacy-friendly alternative to other established social media offerings. They can communicate on Mastodon and do not have to disclose any or very little personal data. It is possible to simply read my posts without having to register for Mastodon.

Events

Due to the restrictions imposed by the coronavirus pandemic, it was not possible to hold any face-to-face events with a larger number of participants during the reporting period. Among other things, the IGF symposium planned for September in Berlin unfortunately had to be cancelled, as well as a continuation of the joint event series with the European Data Protection Supervisor in Brussels.

Visitor groups

Visitor group support was also very limited due to the coronavirus pandemic. My staff supervised a total of four groups with up to 50 participants.

Information material

One focal area of my public relations work continues to be the publication of information on fundamental and current issues in the areas of data protection and freedom of information.

The six brochures currently on offer are mainly aimed at the specialist public. The 14 available flyers, with their diverse range of practical topics, are aimed at citizens in particular. As well as regularly updating these existing materials, my colleagues and I also regularly develop new concepts for corresponding information offerings.

In this context, I have commissioned the translation of selected flyers into different languages this year. Work has also started on a new flyer on 'Data protection for refugees and asylum seekers'.

Furthermore, I would like to expand my counselling and educational work, especially for children and parents. For this purpose, I am currently developing a Pixi book and Pixi learning with the CARLSEN publishing house, which are intended to provide an introduction to the topic of data protection and freedom of information for children and their parents. The first books will be published next year and are to be the start of a new Pixi series.

Although all current publications, under www.bfdi.bund.de/informationmaterial, can be downloaded as accessible PDF documents, I note that there is still an unbroken interest in print publications. Therefore, I still offer people the opportunity to order paper copies in addition to the downloads, where available. I have also been working for several years now with an institution

that supports the integration of people with intellectual disabilities into working life.

10.6 The BfDI's work in figures

I have gone over my main activities from 2020 in the previous chapters. In addition, my work is also generally shaped by the numerous enquiries and complaints received from citizens, the supervision of data processing bodies and the provision of advice to a wide range of institutions. At this point, I would like to give a brief overview of the most important figures.

Committee work

Data protection covers more and more areas of life and thus involves interactions that often go beyond the scope of competence of a single supervisory authority. In addition, the General Data Protection Regulation (GDPR) requires a coordinated approach across Europe, which can sometimes become a complex matter. This is also evidenced by the existence of a total of 66 national and international working committees in which the BfDI is represented. In a good third of these bodies, I have assumed (sometimes temporarily) special responsibility in the roles of chairman or rapporteur.

In this context, my office has participated in almost 350 meetings and has tabled seven resolutions, five of them at a national level and one each at a European and international level.

Complaints and general enquiries

In 2020, citizens sent me a total of 7,878 complaints and enquiries. So compared to the previous year, when I received 7,489, there was a little more interest in data protection.

An enquiry is a complaint if the data subject believes that their rights have been violated in the collection, processing or use of their personal data. The right of appeal is regulated in the GDPR as well as in special laws.

Advice and inspections

An important part of my work is advising responsible bodies and data subjects. In addition to 4,897 general enquiries, I was able to provide telephone advice in 7,212 cases.

The opportunity to hold on-site appointments was severely limited in the reporting year due to the impact of the coronavirus pandemic. This has also had an impact on my inspection practice. Nevertheless, 88 consultations and inspections were still carried out during the reporting period. To fulfil my legal duty under the special conditions of a pandemic, I have increasingly resorted to alternative methods such as written inspections.

Reports of data protection breaches

All public and non-public bodies must report data protection breaches to the competent supervisory authority. I received 10,024 such reports during the reporting period. A particularly large number of reports were received from tax offices, job centres and telecommunications companies in 2020.

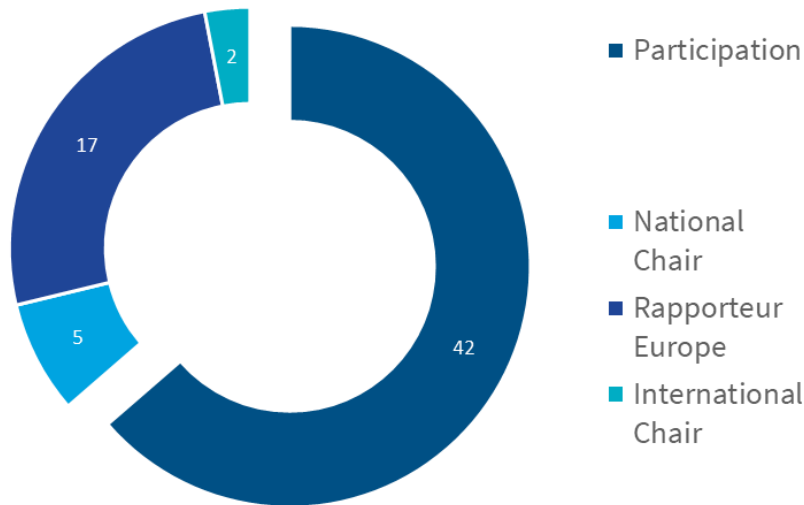
Reports of data protection breaches	2019	2020
Article 33 of the GDPR	14.649	9.985
Section 65 of the BDSG	0	2
Section 109 a (1) of the TKG	40	37

Formal monitoring of legislative projects

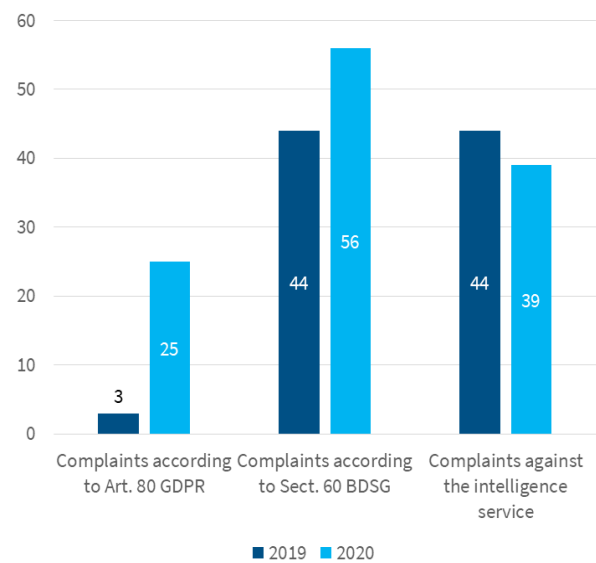
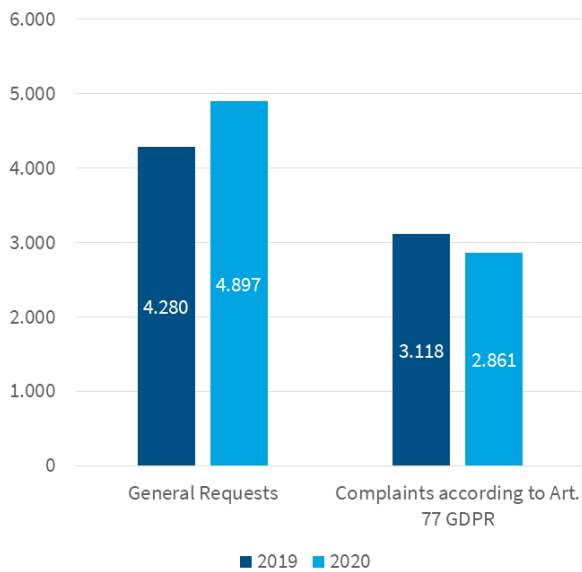
Pursuant to Section 45 of the Joint Rules of Procedure of the Federal Ministries (Gemeinsame Geschäftsordnung der Bundesministerien, GGO), the lead Federal Ministry must involve me in the preparation of draft legislation at an early stage insofar as this affects my duties. In the reporting period, I was involved in 423 cases under Section 21 of the GGO. The significant increase from the previous reporting period (273 instances of participation in 2019) is also related to increased legislative activity due to the coronavirus pandemic.

In addition, I commented on 31 file orders, four proceedings of the Federal Constitutional Court and seven EU legal acts. I also contributed my expertise to five public hearings in the German Bundestag and three Federal Government hearings.

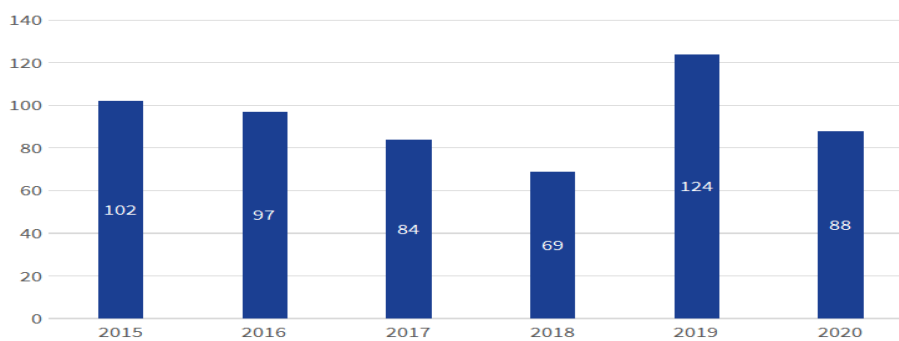
Participation in national and international committees



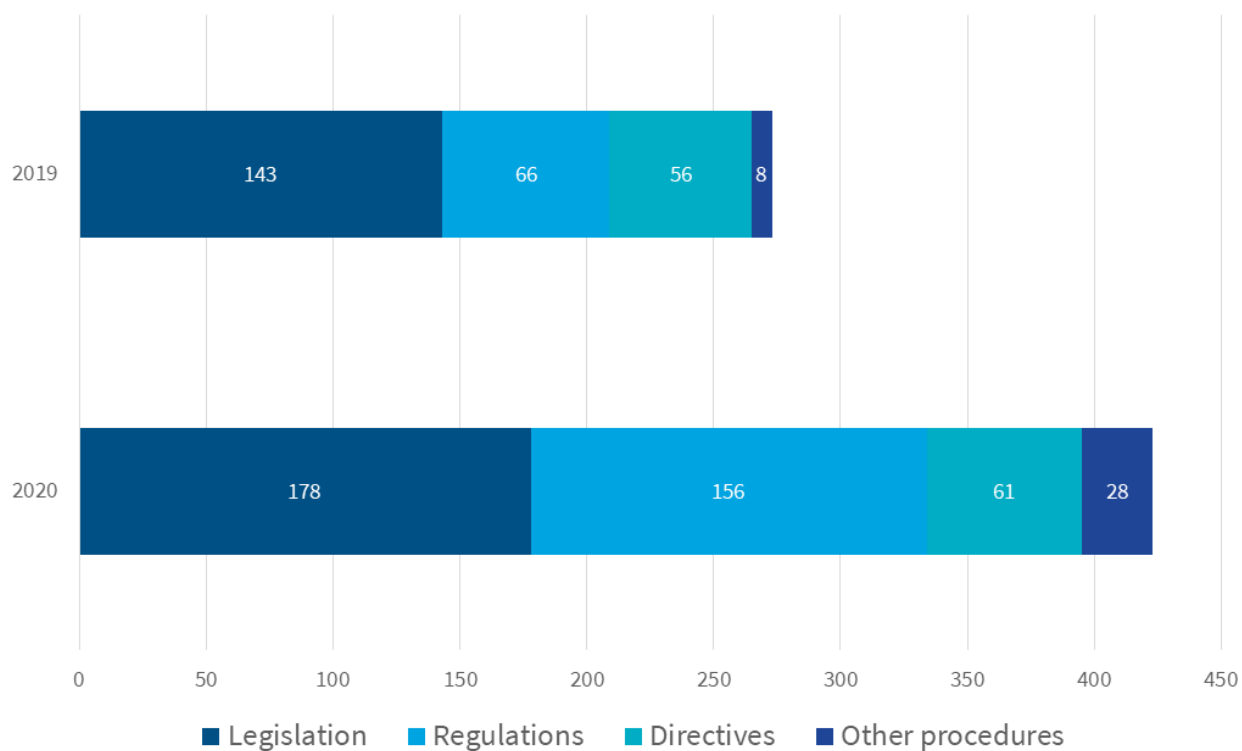
Complaints and Requests



Advice and inspections on supervised authorities



Participations according to § 21 GGO



11 BfDI as the single point of contact (SPOC)

11.1 Strengthening the One-Stop-Shop

State and federal supervisory authorities confirm the chosen path of cooperation with the single point of contact (SPOC) established at the BfDI for EU matters and entrust it with further important coordination tasks.

The BfDI and the state supervisory authorities cooperate on EU matters with the aim of ensuring the uniform application of the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (PCJA Directive). The SPOC acts as an interface and ensures the effective involvement of national supervisory authorities and rapid and smooth cooperation at a European level. This cooperation between the federal and state supervisory authorities and the SPOC is governed by Recital 119 to Article 51 of the GDPR and Sections 17 et seq. of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) and has been set out in further detail in the ‘SPOC concept’. This set of rules, adopted by the Data Protection Conference (Datenschutzkonferenz, DSK) on 23 April 2018, was subject to an initial evaluation after just over two years.

The Evaluation Report concluded that the SPOC concept, with its rules on cooperation between the SPOC and the federal and state supervisory authorities, has essentially proved its worth. The need for adaptation in certain areas is largely due to the fact that there have since been developments at an EU level which impact national cooperation. In addition, various procedural and competence issues have since been decided on by the DSK and its working groups. To continue to fulfil its role as a central set of rules for cooperation, the SPOC concept was supplemented by the relevant decisions and agreements and adapted to the processes which are now largely in place.

The most important needs for adaptation concern the role of the SPOC in voluntary administrative assistance

procedures (see no. 11.2 below), the written procedures of the European Data Protection Board (EDPB) (see no. 11.2 below) as well as in the cooperation with my representation in the EDPB to be elected by the Federal Council.

The representation of Germany in the EDPB is incumbent on me as joint representative as well as a deputy to be elected by the Federal Council from among the heads of the state supervisory authorities (Section 17 [1] of the BDSG). In this important and responsible role, it is the task of the deputy to propose, together with me—by a consensus, if possible—common positions for EDPB negotiations. In addition, voting rights in the EDPB are conferred on the deputy in certain country matters. Unfortunately, the Federal Council has not yet selected a person for the position of deputy. Therefore, although practical experience of cooperation is still lacking, the SPOC has been assigned an important role by the DSK in the coordination between joint representatives and future deputies, particularly to the extent necessary to establish common positions.

In view of the continued dynamic development of European cooperation processes and the fact that sufficient experience has not yet been gained with some types of procedures under the GDPR, it was agreed to re-evaluate them after three more years at the latest.

On the basis of the Evaluation Report, the DSK unanimously adopted the new SPOC concept in November 2020, paving the way for continued successful and trusting cooperation.

Cross-reference: 11.2 Statistical overview of cooperation and coherence procedures at a European level from the perspective of the SPOC

11.2 Statistical insight into the work of the SPOC as part of the cooperation and coherence procedures at a European level

Cross-border case processing is picking up speed. First successes, but also challenges in the cooperation in the EDPB are emerging.

Assumption of responsibility in the GDPR's One-Stop-Shop procedure

The handling of cross-border cases goes through different stages in the cooperation between European data protection supervisory authorities. Since the start of application of the GDPR in May 2018, the focus of processing has increasingly shifted from formal questions to content-related issues.

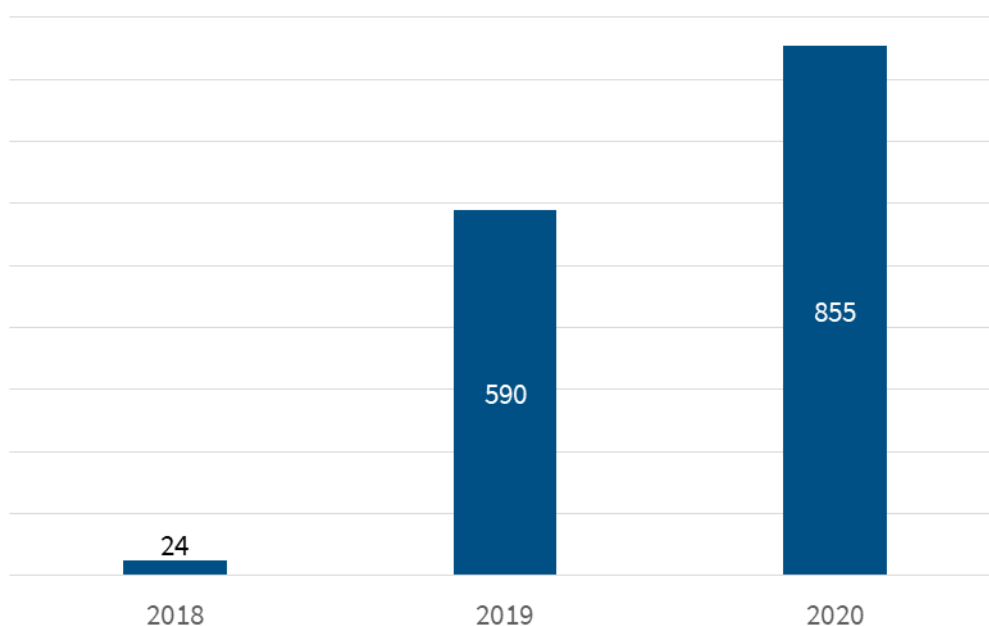
The first formal step in cross-border case processing is the procedure for identifying the lead supervisory authority as well as the supervisory authorities concerned in accordance with Article 56 of the GDPR (56ID). After 543 of these procedures were initiated in 2018 (25 May to 31 December) and 798 procedures in 2019, this was down to 742 procedures in 2020.

In total, there are currently 2,083 procedures under Article 56 of the GDPR to determine the lead supervisory authorities and the supervisory authorities concerned. In this context, the lead supervisory authority bears the main responsibility and is constructively and critically accompanied and supported by the respective supervisory authorities concerned with the aim of harmonising the application of the law throughout the EU.

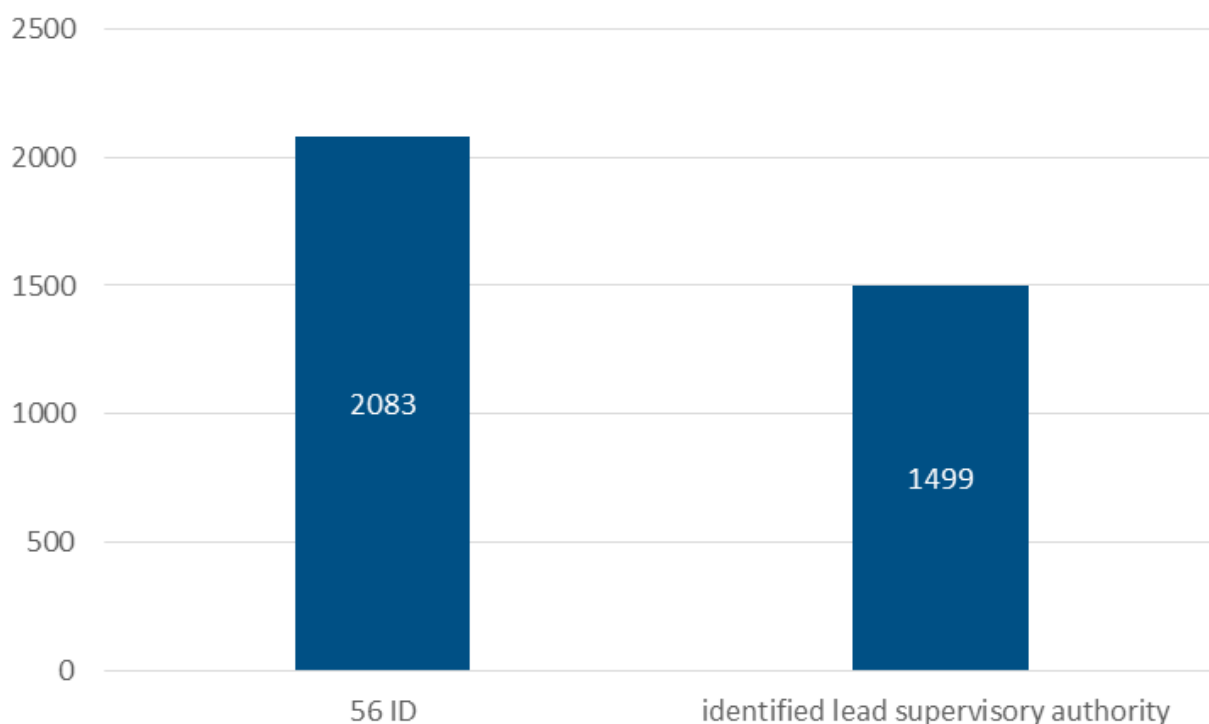
In 1,499 of these cases, the lead supervisory authority has since been identified by officially declaring its competence in the Internal Market Information System (IMI), the IT tool for European administrative cooperation. With respect to the total number of cases created, the lead supervisory authority has already been identified to a large extent, so that content-related processing can be carried out.

The transition to content-related processing is also evidenced by the sharp increase in the number of voluntary administrative assistance procedures under Article 61 of the GDPR. These methods are mainly used for two use cases: in about 10 percent of the cases, general legal questions are asked about the application practice or legal expertise of the supervisory authorities. However, the vast majority of procedures are used for case-related enquiries. This could be, for example, a request from a

Number 56ID and identified lead supervisory authorities since the GDPR



Development of voluntary administrative assistance procedures with German participation



concerned supervisory authority to the lead supervisory authority regarding the status of the complaint or a request from a lead supervisory authority to the supervisory authority concerned to transmit the documents submitted in the context of the complaint.

2020 came with new challenges and tasks for the SPOC

In the context of the voluntary assistance procedures previously considered, the SPOC was also assigned a new role by the DSK.

At the start of December 2019, there was a technical change in the IMI to allow voluntary assistance procedures to be sent in parallel to several recipients from different Member States of the European Economic Area. However, this had the side effect that voluntary requests for administrative assistance could only be addressed to Member States as a whole and no longer to individual federal and state supervisory authorities. As a result, requests sent to Germany were initially received by all 18 German supervisory authorities, although they were often only meant for one of them. This not only created additional work, as each individual supervisory authority had to clarify for itself whether it was responsible, but it also meant that all German supervisory authorities, regardless of their competence, had equal access to the contents of the procedures and the communication contained therein, which has been criticised at a European level for data protection reasons.

Following coordination in the DSK, since 24 April 2020, the SPOC alone has been receiving procedures for voluntary administrative assistance and sending them on to the recipient authorities in Germany in a targeted manner. The SPOC does not carry out a binding competence check, and instead only carries out provisional allocation, which is then checked by the respective supervisory authority and, if necessary, adjusted in consultation with the SPOC. This not only results in a considerable administrative relief for the individual supervisory authorities, but also an increased level of data protection, since only the supervisory authorities actually involved have the necessary access to personal data related to the case.

Since the changeover, the SPOC has already carried out this new task in 329 cases. As a rule, incoming general legal questions are forwarded by the SPOC to one of the working groups of the DSK for a concerted and coordinated German response.

Moreover, as in all other areas of life, the COVID-19 pandemic posed new challenges for the cooperation of European data protection supervisory authorities. Due to the fact that the EDPB was no longer able to meet in person from March 2020, the possibility of taking decisions by written procedure, as provided for in its internal regulations, was used noticeably more often.

To prepare for EDPB procedures, it is the task of the SPOC, in the case of written procedures, to coordinate the establishment of a common position between the

federal and state supervisory authorities in accordance with Section 18 of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). While this task had to be carried out six times in 2018 and only four times in 2019, the impact of the COVID-19 pandemic resulted in a significant increase to 47 EDPB written procedures in 2020.

To optimise this internal coordination process, which is unique in Europe, a new IMI module tailored to the needs of the German supervisory authorities was designed in 2020 at the suggestion of the SPOC. The SPOC works closely here with the German supervisory authorities, the EDPB Secretariat and the European Commission, which is responsible for the IMI system as a whole. The new module will enable the internal German voting procedure to be carried out even more efficiently and securely in the future in an environment free from media discontinuity.

Increased completion of One-Stop-Shop procedures

2020 marks a caesura in that the number of data protection procedures terminated through a final decision made by the lead supervisory authority with the involvement of the supervisory authorities concerned under Article 60 of the GDPR (60FD) is continuously increasing, but the number of 56 procedures is (slightly) decreasing for the first time in 2020 (see figure 'Development of 56ID and 60FD procedures'). In addition to the formal closure of the procedure under Article 60 of the GDPR, a number of cross-border cases were also closed by means of 'amicable settlements' between the responsible bodies and the complainants. Something that is not unproblematic about this way in which procedures are terminated is

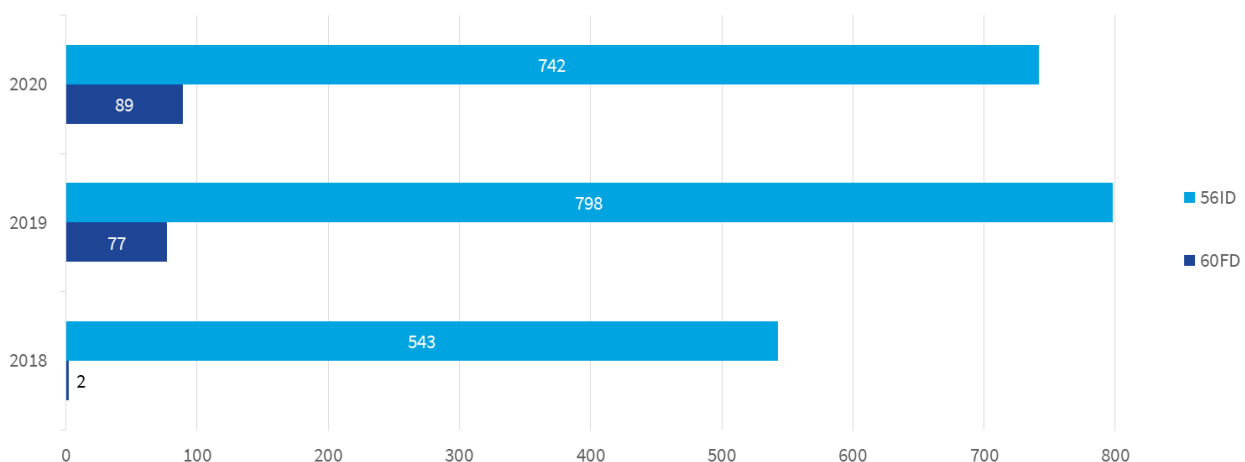
that the lead supervisory authority often does not involve the supervisory authorities concerned.

Heavy demands are placed on the German supervisory authorities in the European voting process: as the last graph in this chapter shows, Germany is the third most frequent lead supervisory authority and has already submitted a decision that terminates procedures in 52 of these 176 cases. Following the final withdrawal of the UK from cross-border case processing under the GDPR at the end of 2020, only Ireland will still process more cases in a lead role compared to Germany. However, of 196 cases identified as being led by Ireland, only four cases have so far been closed through a decision terminating the procedure in a formal procedure under Article 60 of the GDPR. In addition, there have been a number of settlements brought about by the Irish supervisory authority by way of amicable settlement.

It is expected that the number of 56 procedures will continue to decrease in 2021 and that the number of final decisions under Article 60 of the GDPR will continue to increase. It is eagerly awaited how case processing for data processing concerning large, global Internet companies, which often have their European headquarters in Ireland and Luxembourg, will progress.

It is expected that the number of 56 procedures will continue to decrease in 2021 and that the number of final decisions under Article 60 of the GDPR will continue to increase. It is eagerly awaited how case processing for data processing concerning large, global Internet companies, which often have their European headquarters in Ireland and Luxembourg, will progress.

Development of 56ID and 60FD procedures



Identified lead supervisory authority and number of its 60FDs since GDPR implementation

