

Activity Report 2021

30th Activity Report on Data Protection
and Freedom of Information



BfDI

Federal Commissioner
for Data Protection and
Freedom of Information



This report was presented to the President of the German Bundestag, Ms Bärbel Bas.

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

Table of contents

Introduction

2. Recommendations

- 2.1 Summary of the recommendations of the 30th Activity Report
- 2.2 Recommendations of the 29th Activity Report

3. Committees

- 3.1 Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK)
 - 3.1.1 Working Group DSK 2.0
 - 3.1.2 Positive data held by credit agencies
 - 3.1.3 Microsoft Working Group
 - 3.1.4 Important resolutions and decisions
 - 3.1.4.1 Coronavirus: There is a need to introduce legislation covering evidence of vaccinations, test results and recoveries
 - 3.1.4.2 Processing of “vaccination status” data of employees by the employer
 - 3.1.4.3 Measures for the protection of personal data during transmission by email
- 3.2 European Data Protection Board
 - 3.2.1 General report
 - 3.2.2 Third country transfers / Schrems II decision
 - 3.2.2.1 Supplementary Measures Taskforce / Implementation of Schrems II
 - 3.2.2.2 Focus on third country transfers
 - 3.2.3 Completion of consistency mechanism CoC EU Cloud and CISPE
 - 3.2.4 Guidelines on accountability and new standard contractual clauses
 - 3.2.5 Guidelines on right of access to data under Art. 15 GDPR
 - 3.2.5.1 Right of access to data held by social benefit institutions
 - 3.2.5.2 Provision of information by health insurance funds under Art. 15 GDPR
 - 3.2.6 Guidelines for dispute resolution procedures before the EDPB
- 3.3 Global Privacy Assembly
 - 3.3.1 General Report
 - 3.3.2 Reference Panel
- 3.4 Other international bodies
 - 3.4.1 G7
 - 3.4.2 Berlin Group
 - 3.4.3 Data protection principles for government access to personal data in the international sphere

4. Main topics

- 4.1 Coronavirus
 - 4.1.1 Coronavirus warning app
 - 4.1.2 SORMAS
 - 4.1.3 EU digital COVID certificate
 - 4.1.4 Coronavirus Notification Regulation
 - 4.1.5 The Federal Emergency Brake and the Exemption Regulation
 - 4.1.6 Coronavirus Testing Ordinance
 - 4.1.7 The “Epidemic Situation Continuation Act”
 - 4.1.8 Second IfSG Amendment Act: retrospective digital recording of vaccinations and 3G in the workplace
 - 4.1.9 Digital vaccination rate monitoring
- 4.2 Artificial intelligence - Regulation as a task for society as a whole
 - 4.2.1 AI draft regulation
 - 4.2.2 AI consultation process
- 4.3 Interdisciplinary Advisory Council on Employee Data Protection

5. Legislation

- 5.1 Telecommunications legislation TKG/TTDSG
- 5.2 Lobby Register Act
- 5.3 Open Data Act
 - 5.3.1 Open Data Strategy of the federal government
- 5.4 Amendments to the Central Register of Foreigners Act
- 5.5 Federal Police Act
- 5.6 Amendments to the BND Act come into force
- 5.7 Evaluation of the BDSG
- 5.8 IT Security Act
- 5.9 EU digital legislation
- 5.10 Developments in health registers
- 5.11 Data collection powers of the health insurance providers in sickness benefit case management

6. Individual topics

- 6.1 Electronic patient file
- 6.2 Data strategy of the federal government
- 6.3 Cooperation between cartel and data protection supervisory authorities
- 6.4 Restart of the Research Data Centre at the Federal Institute for Drugs and Medical Devices
- 6.5 Use of the health insurance number in the telematics infrastructure
- 6.6 Genome sequencing model project
- 6.7 Prenatal testing in Hong Kong
- 6.8 Implementation of the right to correct a diagnosis under Section 305 SGB V
- 6.9 Reimbursable digital health applications
- 6.10 Digitalisation of public administration
- 6.11 Brexit - Data transfer with the United Kingdom
- 6.12 Outing of asylum seekers
- 6.13 Analysis of mobile phone data by the Federal Office for Migration and Refugees unlawful?
- 6.14 P 20 - Police 20/20: The path to a common “data house”
- 6.15 GETZ: Inadequate evaluation
- 6.16 Data processing at the BND
- 6.17 Transfer of the Stasi files to the Federal Archives
- 6.18 Applications on the electronic health card
- 6.19 Digital identities
- 6.20 The Security Clearance Act - A law with many question marks
- 6.21 Pilot project for “intelligent” video surveillance at Berlin Südkreuz station, 2nd part
- 6.22 Eurojust, European Public Prosecutor’s Office: New responsibilities
- 6.23 Cooperation with other supervisory bodies in the area of federal intelligence services
- 6.24 Passenger name records (PNR) - Central questions remain unresolved
- 6.25 Agile project development
- 6.26 Personnel management system PVSplus: Data protection challenges that have not yet been solved

7. Freedom of information

- 7.1 Committees
 - 7.1.1 Conference of Freedom of Information Commissioners in Germany
 - 7.1.2 International Conference of Freedom of Information Commissioners
- 7.2 “Glyphosate” judgement - The publication of an opinion prepared by the authorities after access to information
- 7.3 Open Government Partnership
- 7.4 Format choice: Yes or No?
- 7.5 Transparency in the legislative process
- 7.6 Complaint against the BMVI for refusing access to information without reason
- 7.7 IFG - “Competition” for the book trade?
- 7.8 Building Academy Foundation Board
- 7.9 Environmental Information Act

- 7.9.1 Ombudsperson function in environmental information law
- 7.9.2 UIG or IFG? A sometimes tricky question of demarcation

8. Inspections and advice

- 8.1 Mandatory inspections
 - 8.1.1 Inspections and complaints in relation to the Anti-Terror Filing System (ATD) and the Right-Wing Extremism Filing System (RED)
 - 8.1.2 Eurodac
 - 8.1.3 VIS
 - 8.1.4 Inspection of the data retrievals in the INZOLL customs investigation information system
 - 8.1.5 Schengen Information System
- 8.2 Other inspections
 - 8.2.1 Questionnaire survey of data protection officers in job centres
 - 8.2.2 Case processing system of the Federal Criminal Police Office
 - 8.2.3 First order issued to the BKA
 - 8.2.4 Radio cell database of the Federal Criminal Police Office
 - 8.2.5 Processing of identification data by the Federal Criminal Police Office in INPOL-Z
 - 8.2.6 Data protection supervision and advice in respect of the Federal Office for the Military Counter-Intelligence Service (BAMAD)
 - 8.2.7 Data protection supervision and advice in respect of the Federal Office for the Protection of the Constitution (BfV)
 - 8.2.8 Inspections relating to the Security Clearance Act - A lot of bad practice and a bit of best practice
 - 8.2.9 Inspection and advice in respect of the Financial Intelligence Unit (FIU)
 - 8.2.10 Inspection of unlicensed postal service providers
 - 8.2.11 Questionnaire on rights of data subjects

9. BfDI internally

- 9.1 Organisational review
- 9.2 Personnel development in 2021
- 9.3 Press and public relations
- 9.4 At the scene of the action: The Capital Team of the BfDI
- 9.5 BfDI facts and figures

10. Single Contact Point

- 10.1 Review

11. Where is the positive?

- 11.1 Successful cooperation with the BMU
- 11.2 Privacy-friendly disaster warning
- 11.3 Deactivation of access on secondment
- 11.4 Raise awareness, create transparency, promote data protection!

1 Introduction

2021 - another year that was repeatedly and entirely shaped by the coronavirus pandemic and the fight against it. As in 2020, the federal government submitted draft laws and ordinances on pandemic control as necessary, and as in the previous year, there was rarely time to examine these drafts properly and advise the federal government. With all due understanding for the sometimes necessary haste, a little more care and involvement from the beginning - as is actually prescribed by law - would certainly have helped.

In fact, not all the measures to be taken came as a surprise: I pointed out to the federal government back in the summer, for example, that a legal basis would be needed to regulate 3G or 2G monitoring in the workplace (monitoring of vaccination, recovery or testing in relation to coronavirus, from the German words “geimpft, genesen, getestet”). However, a corresponding legislative procedure was only initiated at the end of November and again with an extremely short review and comment period.

I would gladly spare myself my constant references to the need for a legal basis for such measures, if action were taken accordingly. Instead, proposed solutions - even those that would be acceptable under data protection law if properly designed - are often not even submitted to me or discussed. On the contrary, there are public complaints that “data protection” would only get in the way. Contrary to this repeatedly voiced criticism, however, data protection, and hence my organisation, has not restricted or even stopped a single appropriate pandemic control measure by the federal government. However time-consuming it has now become, I will not tire of setting the record straight in the future and opposing blame games that only obstruct an understanding of the necessary measures.

The discussion about monitoring of compliance with 3G or even 2G regulations in the workplace have also shown in an exemplary way how necessary, sensible and overdue regulations on employee data protection are. The advisory board set up by the Federal Ministry of Labour,

of which I was also a member, has drawn up proposals to this end.

The digitalisation of our living and working environments is accelerating because of the pandemic. The use of artificial intelligence (AI) and machine learning is increasing significantly, but it is not always clear whether programming, commissioning, training and outcomes really correspond to the goals set. The results are almost impossible to monitor in complex tasks. After the Data Ethics Commission made far-reaching proposals for dealing with “algorithmic systems” in its 2020 report, the EU Commission has now presented a draft regulation that needs to be fleshed out.

In relation to the use of AI in law enforcement and security, I have launched an extensive consultation process to start a public debate.

We had to wait more than ten years for legislation to implement the Privacy Directive when the Telecommunications Act was revised in 2021 by the Telecommunications Modernisation Act. At the same time, the Telecommunications Telemedia Data Protection Act was created, which includes provisions to regulate or even prevent cookie banners, which are so annoying to many.

Increasingly important is the work in EU and international bodies. After lengthy preparatory work by the competent data protection supervisory authorities of the EU countries and their working groups, the European Data Protection Board (EDPB) makes decisions and introduces guidelines that are binding for all EU states. While there are still important decisions outstanding on certain aspects of data collection and processing especially by the big internet corporations, there are initial signs of tougher action against obvious data protection violations. For the first time, the EDPB has also significantly tightened up decisions by lead national supervisory authorities and, for example, significantly increased fines.

Just as the GDPR is now setting the standards for data protection worldwide, international cooperation is becoming increasingly important. I serve on the Executive

Committee of the Global Privacy Assembly (worldwide association of national data protection authorities) and participated in the G7 meeting of data protection authorities. In parallel to the G7 presidency of the Federal Republic of Germany, I will chair this new grouping in 2022.

Due to coronavirus, it was not possible to carry out as many on-site inspections this year as desired and planned. Instead, opportunities for supplementary written checks are being explored and are used extensively wherever possible.

In addition to monitoring the bodies and companies I supervise, my most important task is to advise and inform the federal government, the Bundestag and German citizens.

I am happy to fulfil this role and, in doing so, to explore new

avenues. Last year, for example, two Pixi books for children on the subject of data protection were publis-

hed in cooperation with the Carlsen publishing house. When I presented the books in schools, I was surprised how interested even primary school children are in this topic. Our service provider is barely able to keep up with deliveries of the Pixi book orders. This strengthens my conviction that you cannot start early enough with data protection.

Of course, I cannot manage all these issues and tasks on my own, but I am supported by around 275 highly motivated and professional employees, whom I would like to thank at this point for their daily support.

My thanks also go to “Erzaehlmirnix”, whom I have asked - as an alternative to the characters of various cartoonists in the previous activity reports - to enhance my report this time with their exclusive and refreshing takes on various data protection topics.

Prof. Ulrich Kelber

2 Recommendations

2.1 Summary of the recommendations of the 30th Activity Report

I recommend that the federal government address institutionalisation of the DSK and improve the mandatory cooperation between the German data protection supervisory authorities announced in the coalition agreement by taking the corresponding legislative measures as soon as possible. (No. 3.1.1; 5.7)

I recommend reviewing the methods and basic data for reporting vaccinations and vaccination rate monitoring. (No. 4.1.9)









I recommend that the BMG provide for - and, if necessary, create - a suitable authority for the operation of the implant register, which can take over registration operations in the long term in a legally secure and data protection-compliant manner without conflicts of interest. (No. 5.10)

I recommend structuring the development of the “common data infrastructure” for the genome sequencing model project in a decentralised way and providing for ad hoc data access instead of double data storage. (No. 6.6)

I recommend that company data protection officers’ right to inspect the security files kept in a company, the addressee for a complaint in the non-public sector, the scope of measures relating to security checks pursuant to Section 33 of the Security Clearance Check Act (SÜG) and the transfer of data in the so-called visit control procedure be regulated in the SÜG. (No. 6.20)

I continue to recommend legislation to abolish the anti-terrorism filing system and the right-wing extremism filing system in view of the fact that they have proven to be of little value. (No. 8.1.1)

2.2 Recommendations of the 29th Activity Report

| Recommendations of the 29th Activity Report | Status of implementation |
|--|--|
|  <p>I recommend that the bodies under my oversight involve me at an early stage in time-sensitive projects. In this way, data protection and thus the protection of data subjects' rights can be taken into account adequately from the outset. (see 29th AR No. 4.1.4, 4.1.8, 4.1.9)</p> | <p>After discussions on individual projects, there has been some improvement in the early provision of documents. Unfortunately, this does not apply to all projects.</p> |
|  <p>I recommend that the Bundesrat elect a deputy for the Joint Representative pursuant to Section 17(1) of the Federal Data Protection Act (BDSG). (see 29th AR No. 10.1)</p> | <p>The election was held on 25 June 2021.</p> |
|  <p>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 should be specified for the use of the ID number. The data cockpit should be further developed into a real inventory data information system in the near future. (see 29th AR No. 5.1)</p> | <p>Apart from the development of the data cockpit, none of my recommendations were followed.</p> |
|  <p>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 ruling and make any necessary adjustments. (see 29th AR No. 4.3)</p> | <p>Even though it is clear that there is an awareness of the requirements of the ECJ's Schrems II decision for the most part in the bodies I supervise, adjustments are often fraught with complex issues. In my inspections, I will support and further monitor the adjustment work that is already evident.</p> |
|  <p>I recommend that the laws, projects and measures implemented in the context of the coronavirus pandemic under heavy pressure and within very short deadlines be evaluated deliberately and carefully when the pandemic situation comes to an end. (see 29th AR No. 4.1.3, 4.1.4)</p> | <p>No evaluation has not yet been carried out. This should be done without delay as soon as an endemic situation is reached.</p> |
|  <p>I recommend that "digital health applications" be transmitted to users in the secure telematics infrastructure or on machine-readable storage media. In addition, a new app store should be created for the provision of "digital health applications" in the telematics infrastructure and operated by participants in the health system under an obligation of confidentiality. (see 29th AR No. 5.6)</p> | <p>„Digital health applications" are not (yet) transmitted to users of the secure telematics infrastructure or on machine-readable data media. Nor has an app store operated by participants in the health system under an obligation of confidentiality been created as yet for the provision of "digital health apps".</p> |
|  <p>I recommend clarifying that the exercise of data protection rights must not lead to increased penalties in disciplinary proceedings. (see 29th AR No. 6.10)</p> | <p>No clarification has been provided in this context as yet.</p> |
|  <p>I recommend that European data protection law be implemented immediately and in full. This should not be used as a pretext to introduce controversial regulations with new powers of intervention for the security authorities (see 29th AR No. 6.7).</p> | <p>The Federal Police Act (BPolG) has still not been adapted to the European requirements.</p> |

Recommendations from older activity reports and their status can be found at www.bfdi.bund.de/tb-empfehlungen.

3 Committees

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

The DSK is the association of the independent data protection supervisory authorities at federal and state level. It pursues the goal of protecting fundamental data protection rights, achieving uniform application of European and national data protection law and jointly promoting its further development.

The chair of the DSK changes annually. In 2021 the Saarland State Commissioner Monika Grethel took on this role. Due to the pandemic, all conferences were held in video format. Two resolutions were adopted on the subject of the coronavirus pandemic and four resolutions on various individual issues, namely the processing of positive data by credit agencies, processing of the “vaccination status” date and non-application of technical and organisational measures at the request of data subjects.

In addition, the DSK developed guidance on the protection of personal data when transmitted by email and for providers of telemedia from 1 December 2021, and application information for requirements for certifications under data protection law.

3.1.1 Working Group DSK 2.0

Cooperation between the independent data protection supervisory authorities at federal and state level should be further improved. The Working Group DSK 2.0 has presented initial results in an interim report and made proposals on how this goal can be achieved.

There is agreement within the DSK that it must develop further, become faster and more flexible and get involved in current public debates on data protection policy at short notice. With this in mind, it had set up a Working Group DSK 2.0 at management level in June 2020 to evaluate its collaboration, including the working methods of the DSK, and to develop proposals for restructuring (cf. 29th AR No. 3.1.6).

In 2021 the Working Group summarised the initial results in an interim report and submitted it to the DSK. In addition to taking stock, the interim report contains concrete proposals in three areas: “the DSK as a European player”, “bolder/faster positioning” and “binding majority decisions”. Specifically, it is proposed, among other things,

- to form a presidium of the DSK
- to establish specific spokesperson functions
- to establish a joint office

The WG DSK 2.0 will continue its work on this basis, examining in particular the legal framework conditions for closer cooperation while preserving the independence of the supervisory authorities.

I will continue to work to develop the DSK and to harmonise supervisory practice within the German data protection supervisory authorities even more.

I recommend that the federal government address institutionalisation of the DSK and improve the mandatory cooperation between the German data protection supervisory authorities announced in the coalition agreement by taking the corresponding legislative measures as soon as possible.

3.1.2 Positive data held by credit agencies

Processing of so-called positive data from contracts for mobile services and permanent trading accounts is only possible on the basis of effective consent. Even a so-called “energy supplier pool” must not make consumers transparent.

The Conference of the Independent Federal and State Data Protection Supervisory Authorities (DSK) had already stated in 2018 that credit agencies are generally not allowed to collect positive data on private individuals on the basis of the balancing of interests under Art. 6(1) sentence 1 point (f) GDPR.

In the public perception, the activities of credit agencies are predominantly associated with the storage and disclosure of so-called negative data. This is generally information about negative payment experiences or experiences in relation to interest and repayment of loans, defaults on instalment payments or private insolvency. The reporting of such data to credit agencies, their storage and disclosure are generally based on the balancing of interests pursuant to Art. 6 (1) sentence 1 point (f) GDPR. Accordingly, these data processing operations are permitted if there is a legitimate interest either of the credit agency or of its contractual partners and if the legitimate interests of the consumers concerned do not take precedence.

What is less well known is that there is also an interest on the part of the credit agencies and their contractual partners in processing so-called positive data. Positive data are pieces of information about existing contracts that are being fulfilled correctly by consumers. This positive data may also be included in the calculation of the probability of default (credit score). According to the data protection supervisory authorities, apart from certain exceptions in the banking sector this information can only be processed on the basis of the data subject's effective consent. In the case of such positive data, the data subject's legitimate interest in determining the use of their data usually takes precedence. Even the transmission of such data to a credit agency by their contractual partners cannot be based on Art. 6(1) sentence

1 point (f) GDPR: as long as an individual complies with their contractual obligations, there is no reason to hold data on their contracts or payment history without their consent.

At the time of its resolution in 2018, the DSK had already envisaged dealing with the processing of positive data in the case of continuing obligations at a later point in time, and that time fell within the reporting period. In particular, the question was whether a different assessment was required for the widespread practice of transmitting and processing positive data about contracts for mobile phone services and continuous trading accounts of private individuals. This relates, for example, to the widespread practice of paying off mobile phones in monthly instalments over the term of a mobile phone contract. Continuous trading accounts, on the other hand, refer to contracts where the data subject receives goods on credit using a customer card provided by a merchant, for example, and pays for the purchased goods in arrears through monthly debits or by other means.

The DSK came to the conclusion that there are legitimate interests for the transmission of positive data by mobile service providers and commercial enterprises to

improve the quality of credit ratings and to protect the economic stakeholders from credit risks. However, the DSK is also of the opinion that the interests, fundamental rights and freedoms of data subjects regularly outweigh this legitimate interest of the controllers or third parties in processing the positive data. The DSK was unable to identify any special circumstances justifying the processing of positive data in these cases on the basis of balancing of interests. Credit agencies have argued that the processing of positive data is particularly advantageous for consumers when there is otherwise little information available about the person. But this argument is not convincing. On the one hand, it does not justify processing against the will of the person concerned. On the other hand, this argument holds water only if the logic is that a lack of data about a person often results in a negative assessment, even though no conclusions can be drawn from the absence of data.

The transfer and processing of positive data about mobile service contracts and continuous trading accounts by contractual partners and credit agencies are permitted only on the basis of the consent of the data subject. The general requirements for this must be respected. In particular, granting of consent may not be made a condition of the conclusion of the contract.

At the same time as the discussions about the processing of positive data were ongoing during the reporting period, credit agencies and energy suppliers were considering the creation of a so-called energy supplier pool. Positive data of contractual partners were also be stored in this central data pool and transmitted to other energy suppliers. Information about the number of contracts concluded and the respective contract duration can indicate whether a longer contractual relationship with an electricity supplier is likely or whether new customer offers are exploited regularly. Consumers who regularly choose the cheapest offer on the market and want to switch suppliers to do so could then be excluded from attractive offers by utility companies, even though they have only exercised their rights as customers.

I welcome the fact that the DSK has also taken a clear position on the so-called energy supplier pool. The desire to record "bargain hunters" in a data pool in order to identify them as such when initiating a contract and to exclude them from offers does not constitute a legitimate interest within the meaning of Art. 6(1) sentence (1) point (f) GDPR. In addition, the legitimate interests and fundamental rights of customers outweigh this. The DSK did not accept that an explicitly desirable behaviour - in this case the search for the cheapest energy provider - should lead to negative consequences for consumers.

3.1.3 Microsoft Working Group

There is a predicament for controllers: software such as Microsoft 365 is used in many places, but it is also widely criticised in terms of its data protection. How can a conflict with data protection of this sort be avoided? The DSK has started an intensive dialogue with Microsoft to provide more clarity and recommendations for controllers.

As early as the end of 2020, the DSK opened up a dialogue with Microsoft in order to achieve improvements together in the contractual basis for the company's on-line services in terms of data protection law. Under the leadership of the supervisory authorities of Brandenburg and Bavaria (LDA), the supervisory authorities of Berlin, Schleswig-Holstein, Saxony, Mecklenburg-Western Pomerania, Baden-Württemberg,

Hesse and my organisation are now involved in this Working Group. The focus will be on questions regarding commissioned processing pursuant to Art. 28 GDPR and the practical impact of the ECJ's case law on international data transfers (case C-311/18 "Schrems II").

The DSK had already voiced some criticism in advance, e.g. where Microsoft also uses personal data for its own purposes when providing services. This requires a viable legal basis for the provision of this data under the contractual relationship of controllers/customers with Microsoft. Verification of a viable legal basis in turn requires knowledge of the specific purposes and the personal data used.

One of the aims of the dialogue is to create this transparency so that a legal assessment can be arrived at on this basis. In my view, this transparency should of course be reflected in the contractual foundations. Only in this way can controllers/customers fulfil their accountability obligation under Art.

5(2) GDPR. In general, however, the DSK is also discussing other proposals for contractual improvements, including the use of subcontractors.

I would like to conclude this dialogue process with regard to the questions on commissioned processing pursuant to Art. 28 GDPR as soon as possible and publish it in the form of DSK recommendations for action by controllers/customers who want to use the relevant Microsoft products.

In a further step, the dialogue round will deal with the concrete effects of the Schrems II ruling. The new legal requirements and changing customer preferences are paving the way for more Europe-centred data processing in this context. With the so-called "EU Data Boundary" initiative, Microsoft is also announcing the option of

offering European customers processing and storage of their data exclusively within the European Union. I will continue to follow these developments closely.

3.1.4 Important resolutions and decisions

3.1.4.1 Coronavirus: There is a need to introduce legislation covering evidence of vaccinations, test results and recoveries

Processing of health data such as vaccination records or body temperature measurements is regulated by law. The strict requirements of Art. 9(2) GDPR must be observed.

In its resolution, the DSK called for the introduction of corresponding legislative procedures. Processing of health data for private sector purposes must comply with the requirements of the European General Data Protection Regulation. The term health data also includes information about vaccination status and results of coronavirus tests. The particularly strict protection of the General Data Protection Regulation only allows processing in exceptional circumstances. Without a legal basis, processing would only be possible with consent. There is a particular problem here regarding the voluntary nature of such consent in the employment context. In order to achieve legal clarity, certainty and consistent solutions, legal regulations are needed.

With a view to creating the legal clarity demanded by the DSK, I have and will continue to advise the federal ministries involved closely and push for legal regulation.

3.1.4.2 Processing of "vaccination status" data of employees by the employer

Processing of "vaccination status" data of employees may only take place with explicit legal authorisation. This is the case even during the COVID-19 pandemic.

As a matter of principle, employers may only process "vaccination status" data with explicit legal authorisation. The DSK resolution also clarifies that Section 26(3)

sentence 1 BDSG cannot be considered as such. Processing of health data such as vaccination status is only permitted in exceptional cases (see Art. 9(1) GDPR).

The processing of such data can only be based on the consent of employees if it was given voluntarily and is thus legally valid, see Section 26(3) sentence 2 and (2) BDSG. In a relationship of superiority and subordination, as is usually the case in an employment relationship, there are doubts about the voluntary nature and thus about the lawfulness of the consent.

I had to pursue this problem for some time with legislators before a legal regulation was put in place.

3.1.4.3 Measures for the protection of personal data during transmission by email

When sending emails, there are risks associated with breach of confidentiality and integrity of personal data. Controllers and processors must be able to assess what damage a breach of confidentiality and integrity can cause. If requirements for secure transmission cannot be met, another - more secure - communication channel must be chosen.

In its guidance on the protection of personal data in the case of transmission by email, the DSK has addressed the requirements for procedures for sending and receiving emails. It deals with the risks associated with breach of confidentiality and integrity of personal data. It takes typical processing situations as a starting point in order to demonstrate practical use cases. In particular, end-to-end encryption and transport encryption are considered suitable methods for minimising risk. Through the risk-based approach of its guidance, the DSK provides data controllers and processors with a suitable tool for dealing with the transmission of emails.

You can find the guidance under the following link:
www.bfdi.bund.de/orientierungshilfen

3.2 European Data Protection Board

3.2.1 General report

In the reporting period, the European Data Protection Board (EDPB) further intensified its work on uniform application of the General Data Protection Regulation throughout Europe. Additional guidelines were adopted, recommendations made and opinions expressed. Cross-border cooperation was also strengthened further. Initial dispute resolution procedures, including an emergency procedure, were negotiated.

The European Data Protection Board (EDPB) is an independent European body that contributes to the consistent application of data protection rules across the European Union and promotes cooperation between EU data protection authorities. I have already explained these tasks in more detail in my previous Activity Reports. As the joint representative of all German supervisory authorities, the BfDI is a member of the Board. More details can be found on my website.¹

¹ www.bfdi.bund.de/edsa

The operations of the EDPB in 2021 were also affected by the impact of the COVID-19 pandemic. With one exception, all plenary sessions took place in the form of video conferences. In the process, the EDPB consolidated the high frequency of its plenary sessions and met a total of 15 times. In addition, there are numerous meetings of the EDPB's expert subgroups.

One focus of the work in this reporting period was again on the development of guidelines pursuant to Art. 70 GDPR for uniform implementation of the GDPR in Europe. In addition, the Board also adopted opinions using the consistency mechanism under Art. 64 GDPR. In my last Activity Report, I referred to initial decisions relating to world-leading tech companies. There have been further developments here, including a first decision about the so-called emergency procedure.

The EDPB has also started to implement its strategy for the years 2021 to 2023.

Guidelines, recommendations and guidance

During the reporting period, the EDPB has adopted numerous guidelines, recommendations and guidance documents, on which I have regularly worked as rapporteur or co-rapporteur. Some of these have been subject to public consultation to ensure transparency and participation.

- The **Guidelines 01/2021 on Examples regarding Data Breach Notification** look at examples from the supervisory practice of relevant supervisory authorities. These include the aspects of risk assessment in cases of data breaches, the role of technical-organisational measures according to Art. 32 GDPR and suggestions for measures that data controllers should take after data breaches.
- The **Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive (JHA Directive)** set the framework and minimum requirements for the adoption of an adequacy decision on the basis of EU law.
- The **Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications** explain the relationship with the planned E-Privacy Regulation and issues related to the processing of personal data for new purposes.
- The **Guidelines 02/2021 on Virtual Voice Assistants** include the most important references to legal conformity ("compliance"). They also give practical recommendations to stakeholders on how to comply with them.

- The **Guidelines 9/2020 on relevant and reasoned objections under Regulation 2016/679** provide guidance on what is meant by a “relevant and reasoned objection” by supervisor authorities to proposed decisions by lead supervisory authorities in cross-border supervisory cases. The procedures and the criteria to be taken into account when assessing an objection are explained.
- The **Guidance on certification criteria assessment** [Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation] aims to refine elements from the EDPB Guidelines 1/2018. The aim is to establish uniform assessments in connection with the approval of certification criteria.
- The **Guidelines 03/2021 on the application of Article 65(1)(a) GDPR** describe the process of dispute resolution by the EDPB. They refer exclusively to cases involving the failure of a cooperation procedure under Art. 60(4) GDPR and are intended to bring these procedures to a decision.
- The **Guidelines 8/2020 regarding the targeting of social media users** are intended to clarify the distribution of roles and responsibilities between social media platforms and companies or other users of the targeting functions of these social media platforms, against the background of several ECJ rulings. They also aim to illustrate the impact of data processing operations on (fundamental) rights and freedoms of data subjects with practical examples.
- The **Recommendations 02/2021 on the legal basis for the storage of credit card data solely for the purpose of facilitating further online transactions** aim to provide uniform Europe-wide requirements for the lawfulness of data storage of credit card data in online commerce. They ensure that the legal position is clear and prevent competitive disadvantages.
- The **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data** are intended to assist data exporters in identifying and implementing appropriate additional measures. This is to achieve a consistent level of protection. They include several amendments resulting from public consultation. They also place particular emphasis on the practices of the authorities of a third country.
- The **Guidelines 04/2021 on codes of conduct as tools for transfers** have the purpose of clarifying the conditions for approval of codes of conduct by a competent supervisory authority and declaration of their

general validity within the EEA by the Commission as a transfer tool.

- The **Guidelines 7/2020 on the concepts of “controller” and “processor” in the GDPR** have the main objective of clarifying the meaning of the terms. In addition, the different roles and the distribution of (legal) responsibilities between these actors are clarified.
- The **Guidelines 10/2020 on restrictions under Article 23 of the GDPR** are intended to emphasise the conditions for the application of such restrictions by Member States or EU legislation in the light of the Charter of Fundamental Rights and the General Data Protection Regulation. They analyse the criteria for the way in which restrictions are applied, the assessments to be followed, the way data subjects can exercise their rights after the restrictions have been lifted and the consequences of breaches of Article 23 GDPR.
- The **Guidelines 05/2021 on the interplay between the application of Art. 3 and the provisions on international transfers** explain three basic criteria. They provide examples to clarify whether a processing operation is a transfer to a third country or to an international organisation and whether, consequently, the provisions of Chapter V of the GDPR must be observed.

Opinions on adequacy decisions

The EDPB gives an opinion in proceedings relating to the decision as to whether a third country or an international organisation has an adequate level of protection for the processing of personal data. In its assessment, the EDPB uses

- **the GDPR adequacy referential,**
- **the recommendations of the EDPB 2/2020 on the European Essential Guarantees for surveillance measures** and
- the decisions of the ECJ and the ECtHR on access by public authorities.

In 2021, the EDPB expressed its opinion on adequacy in two third countries (see also 3.2.2.):

- In the **Opinions on adequacy in the United Kingdom** (Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom and Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data

in the United Kingdom), the EDPB notes that the EU and UK data protection frameworks are very similar in key areas. This applies e.g. to

- bases of lawful and fair processing for legitimate purposes
- purpose limitation, data quality and proportionality
- data storage, security and confidentiality,
- transparency
- special categories of data and
- automated decision-making and profiling.

Nevertheless, the EDPB recommends that individual points be closely examined and monitored, e.g. in the case of the exception in the area of immigration and its effects on the restrictions applicable to the rights of data subjects.

- In the **Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea**, the EDPB concentrates on general aspects of the GDPR. In addition, the EDPB focuses on access by public authorities to personal data transferred from the European Economic Area (EEA) to the Republic of Korea for law enforcement and national security purposes. This also includes the remedies available to persons in the EEA. The EDPB examines whether the safeguards provided for in the Korean legal framework are effective.

Opinions in the consistency mechanism / decisions in the cooperation procedure

The EDPB has drafted almost 40 opinions in the consistency mechanism.

These largely concern:

- binding internal data protection rules submitted by Member States (Art. 47 GDPR)
- accreditation of certification bodies (Art. 43(3) GDPR)
- bodies for monitoring compliance with codes of conduct (Art. 41 GDPR).

At the request of the Hamburg supervisory authority, the EDPB issued a first binding decision in the emergency procedure pursuant to Art. 66(2) GDPR after the latter had ordered interim measures against Facebook Ireland Ltd.

The Hamburg supervisory authority had ordered a ban on the processing of WhatsApp user data by Facebook Ireland Ltd. for its own purposes. This came after a change to the terms of use and privacy policy for European users was implemented by WhatsApp Ireland Ltd. The EDPB decided by a majority that the requirements for proving a breach and an emergency had not been met. No definitive action was therefore taken.

In a second procedure, the EDPB issued a dispute resolution decision on the basis of Art. 65 GDPR. This was to address the lack of consensus on certain aspects of a draft decision by the Irish supervisory authority as the lead supervisory authority in relation to WhatsApp Ireland Ltd and the subsequent appeals by some of the authorities affected. The EDPB concluded that the Irish supervisory authority should amend its

draft decision on breaches of transparency, the calculation of the fine and the deadline for implementing the instruction.

Implementation of the EDPB Strategy 2021-2023

I explained the **EDPB Strategy 2021-2023** in my last Activity Report. Implementation has already begun - for example:

- In order to promote harmonisation and facilitate legal conformity (compliance), the guidelines, recommendations and guidance are being implemented.
- The EDPB is setting up a Support **Pool of Experts** to assist with effective enforcement and efficient cooperation between national supervisory authorities. This is used at EDPB level to support investigations and enforcement actions that are of common interest to EDPB members. In addition, the EDPB has resolved to launch its first coordinated action (**Coordinated Enforcement Framework**) on the use of cloud-based services by the public sector. The results of these national measures are collated and analysed.
- The EDPB bases its fundamental rights approach to new technologies on its **Statement on Digital and Data Strategy**. In doing so, it essentially expresses all the overarching concerns relating to the legal acts (Data Governance Act, Digital Services Act, Digital Markets Act and Artificial Intelligence Act). In addition to a lack of protection of the fundamental rights and freedoms of individuals, there is only fragmented supervision (see also 4.2 and 5.9).

Cross-references:

3.2.2 Focus on third country transfers, 3.2.4 Guidelines on accountability, 3.2.6 Guidelines on dispute resolution, 4.2 Artificial intelligence, 5.9 EU digitalisation legislation

3.2.2 Third country transfers / Schrems II decision

3.2.2.1 Supplementary Measures Taskforce / Implementation of Schrems II

In 2021 the ECJ's "Schrems II" ruling (case C-311/18) has continued to preoccupy supervisory authorities in the EU and at national level. An important step with regard to the implementation of the results of the Schrems II ruling was the work of the Supplementary Measures Taskforce set up by the EDPB. In addition, the supervisory authorities were confronted with questions regarding the implementation of the Schrems II decision in the course of their advisory and supervisory activities, which need to be resolved.

I. The Schrems II ruling

In my last two Activity Reports I reported on the Schrems II procedure. On 16 July 2020 the ECJ announced in its Schrems II ruling that the provisions of the EU-US „Privacy Shield“ are invalid. No more data transfers may be made to the area governed by US law on the basis of the regulations of the Privacy Shield. At the same time, the ECJ's declaration of invalidity did not extend to the transmission instrument of the standard contractual clauses. The court found that these may need to be extended to include "supplementary measures" to ensure that the data in the third country essentially enjoys equivalent protection to that in the EU. It follows from the ruling that the standard contractual clauses do not provide sufficient protection against access to personal data from the EU by intelligence services or other US security agencies. A precise verification of the supplementary measures is necessary in each individual case in this context.

The impact of the ruling on other third countries and on other transfer instruments pursuant to Art. 46 GDPR will be addressed by the European Data Protection Board (EDPB) in the context of the work of the Expert Subgroup on International Transfers (see No. 3.2.2.2). Supplementary Measures Taskforce - Recommendations of the EDPB on supplementary measures

As already mentioned in my last Activity Report, the recommendations on "supplementary measures" ("Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of

protection of personal data" - version 2.0) were accepted by the EDPB on 10 November 2020. The EDPB was able to adopt these recommendations in their final version on 18 June 2021². The final adoption by the EDPB was preceded by a public consultation. The results of the consultation were evaluated by a drafting team, which included myself and other national supervisory authorities.

The recommendations are intended to assist data exporters in assessing whether supplementary measures are required when transferring data to third countries. The recommendations contain practical examples for different transfer scenarios. Furthermore, a list of some of the possible supplementary measures, such as data encryption, are included in an annex.

II. II. Implementation / Monitoring

In the Schrems II ruling, the ECJ set out a clear allocation of tasks. Companies and public bodies are obliged to check the lawfulness of their data transfers to third countries themselves and to adjust them if necessary. They are advised and monitored by the supervisory authorities in doing so. As already stated in my last Activity Report and in Section 3.2.2.2, the supervisory authorities have developed guidance for controllers and processors (data exporters) at national and European level. In October 2020 I provided guidance on the impact of the ECJ's ruling on international data transfers in an information letter to federal public bodies and companies under my supervision.³ In the letter, I summarised the key statements of the ruling. Furthermore, I have pointed out the obligation of the data exporting body to check the Schrems II principles when transferring data to third countries. I introduced monitoring measures in my area of responsibility to implement the Schrems II requirements during the reporting period.

I am supporting data controllers and processors with up-to-date information on this subject on my website.^{4,5}

The complex legal consequences resulting from the Schrems II ruling will continue to place considerable demands on the German and European supervisory authorities in their work. In the long term, a remedy could involve uniform, rights-based international standards for global data transfers that also cover the critical aspect of government access to personal data.

² Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021, available at: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasures-transfer-tools_en.pdf.

³ Information letter of the BfDI, available at: <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2020/circular-information-trems-II.html>

⁴ Information on the BfDI website, available at: www.bfdi.bund.de/schrems-II

⁵ Schrems II ruling of the ECJ of 16.07.2020, Case C-311/18, available at: <https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIdex=1&dir=&occ=first&part=1&text=&dodang=DE&-cid=40595668>

3.2.2.2 Focus on third country transfers

If data are transferred to a third country or to an international organisation, controllers or processors must first check whether the general requirements for data transfer under the GDPR are met. The additional requirements under Chapter V of the GDPR must also be taken into account. The so-called Schrems II ruling of the ECJ (Case C-311/185) set new standards. The significant impact of the ruling on data transfers to third countries places high demands on controllers, processors and supervisory authorities. They have shaped the work of the International Transfers and Borders, Travel and Law Enforcement Expert Subgroups (ITS and BTLE ESGs) in the year under review.

In cooperation with the supervisory authorities of the countries in the ITS and BTLE Expert Subgroups of the European Data Protection Board (EDPB), the focus of my activities has been as follows:

- developing guidelines and recommendations for data transfers to third countries and international organisations;
- providing opinions on adequacy decisions and other decisions of the European Commission relevant to data protection.

I. Adequacy decisions

According to Art. 45 GDPR and Art. 36 JHA Directive, the European Commission may determine that a third country or an international organisation ensures an adequate level of data protection.⁶ If a data transfer takes place within the scope of an adequacy decision, no special authorisation by the data protection supervisory authorities is required. The data transfer does not need to be accompanied by any further safeguards from Chapter V of the GDPR or Chapter V of the JHA Directive. Notwithstanding this, it remains necessary to check that the general data protection requirements for the corresponding data processing are met. The Board issued opinions on the adequacy decisions for the United Kingdom and South Korea during the reporting period.

United Kingdom

The European Commission began the adoption procedure on the adequacy of personal data protection by the UK on 19 February 2021 (cf. 6.11). The EDPB issued

two opinions on both draft adequacy decisions in the adoption procedure¹. It notes that the UK's data protection framework is largely based on the European Union's data protection framework. However, it also stresses that some points need to be monitored more closely. This includes the exemption regulation regarding immigration and its impact on the rights of data subjects.

There is also a need to monitor possible restrictions on the transfer of personal data from the European Economic Area to the UK (e.g. based on future adequacy decisions on the UK or international agreements between the UK and third countries).

Furthermore, the EDPB criticises various regulations and practices in the security sector, which need to be monitored and examined further. These include, for example, the interception of mass data and independent assessment and monitoring of the use of automated data processing tools.

The EDPB expects legislation in the UK to evolve and requires that adequacy be continuously monitored and time-limited. The EDPB welcomes the sunset clauses in the two adequacy decisions adopted by the European Commission on 28 June 2021 under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (JHA Directive), which expire on 27 June 2025.

Republic of Korea

On 16 June 2021 the European Commission initiated the procedure for adopting the adequacy decision for data transfers to the Republic of Korea. The basis for the processing of personal data in the Republic of Korea is the national Personal Information Protection Act (PIPA), the core elements of which are consistent with the level of data protection in the EU.

In its opinion of 24 September 2021, the EDPB did not express any fundamental objections to the adequacy decision. However, it asks the Commission to clarify certain concepts and rules of Korean law.⁷ The adequacy decision was adopted by the European Commission on 17 December 2021.⁸

II. New standard data protection clauses of the European Commission

As already stated in my last Activity Report, the ECJ had found the EU-US Privacy Shield to be invalid in the Schrems II ruling (ECJ ruling of 16 July 2020: Case

⁶ EDPB Opinions on draft UK adequacy decisions, available at: https://edpb.europa.eu/news/news/2021/edpb-opinions-draft-uk-adequacy-decisions_en

⁷ Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea, version 1.0, adopted on 24 September 2021; available at: https://edpb.europa.eu/system/files/2021-09/edpb_opinion322021_republicofkoreaadequacy_en.pdf

⁸ COMMISSION IMPLEMENTING DECISION of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act: https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

C-311/18). As a result, data transfers from the EU to the US can no longer take place on this basis. In its ruling, the ECJ did not fundamentally question the instrument of standard contractual clauses (SCCs), but stipulated that these would have to be supplemented by so-called “supplementary measures” (see 3.2.2.1 above) if necessary. This is to ensure that the data in the third country essentially have equivalent protection to that in the EU. According to the court’s findings, the standard contractual clauses may not be sufficient as protection against possible access by intelligence services or other security authorities to personal data from the EU.

On 4 June 2021 the European Commission issued revised standard data protection clauses (SCCs), which take into account the requirements of the Schrems II ruling, but do not make an examination of the legal situation and practices of the authorities unnecessary in individual cases.⁹ In doing so, the Commission has adopted a modular approach that is intended to provide more flexibility in the design of third-country transfers. An 18-month transition period is provided for users of the Commission’s old standard contractual clauses to switch from the previous clauses to the new ones.

The German supervisory authorities had developed their own position on the draft of these new SCCs, which was brought to the EDPB. It is reflected in many places in the joint opinion of the EDPB and the European Data Protection Supervisor (EDPS) of 14 January 2021.¹⁰ The European Commission’s new standard contractual clauses on commissioned data processing (see 3.2.4).

III. Approved codes of conduct

The EDPB has developed guidelines in the ITS ESG, with the active participation of my authority as co-rapporteur, to treat approved sector-specific codes of conduct as an adequate guarantee under Art. 46 GDPR for the transfer of personal data to a third country. In contrast to the codes of conduct, which specify the requirements of Art. 28 GDPR (cf. 3.2.3), these are special codes of conduct that are intended to make data transfers to third countries easier. In particular, data importers in the third country - which are not subject to the GDPR - may join these codes of conduct in order to provide appropriate safeguards for data transfers. The guidelines give practi-

cal advice on the requirements and procedure up to the adoption of these codes for the participants. They are also intended to serve as a reference for all international supervisory bodies, the EDPB and the Commission with regard to consistent evaluation of the codes.

The input from the public consultation, which ended on 1 October 2021, is currently being evaluated. The guidelines are expected to be adopted by the EDPB early next year.

IV. Certification as an instrument of data transfer to third countries

In Art. 46(2), the GDPR defines the instrument of certification as a further instrument for data transfers to third countries. In the reporting year, the ITS ESG dealt with the preparation of guidelines for this instrument of transfer. I have taken on the role of the main rapporteur in the ITS ESG here. As the EDPB has already published general guidance on certification and accreditation under the General Data Protection Regulation (GDPR) in 2018, these guidelines focus on the specific aspects of certification as an instrument for data transfers. They are intended to provide guidance for application in practice.

The guidelines are soon to be submitted to the EDPB for adoption and put out to public consultation.

V. Binding internal data protection rules - Binding corporate rules (BCR)

Binding corporate rules (BCRs) are another appropriate guarantee of Chapter V of the GDPR for a transfer to third countries. At the ITS ESG level, a large number of BCRs are reviewed and individual issues clarified. Furthermore, the ITS ESG deals with the further development of the EDPB’s BCR acceptance procedure with regard to efficiency (quality assurance, acceleration, simplification).

Cross-references:

3.2.2.1 Supplementary Measures Taskforce, 3.2.3 Completion of consistency mechanism CoC, 3.2.4 Guidelines on accountability and new standard contractual clauses, 6.11 Brexit

⁹ See in detail the press release of the Conference of the Independent Federal and State Data Protection Supervisory Authorities of 21 June 2021, available at: https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf

¹⁰ Joint opinion 1/2021 of the EDPB and the EDPS on the European Commission Implementing Decision on standard contractual clauses between controllers and processors for the aspects referred to in Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725, available at: https://edpb.europa.eu/system/files/2021-04/edpb-edpsjointopinion01_2021_sccs_c_p_de_1.pdf

3.2.3 Completion of consistency mechanism CoC EU Cloud and CISPE

On 19 May 2021 the European Data Protection Board adopted the positive opinions on the two thematically closely related codes of conduct “EU Cloud CoC” and “CISPE CoC”. These are the first EU-wide codes of conduct on which the EDPB has adopted an opinion under the consistency mechanism.

For the first time, the European Data Protection Board has adopted two positive opinions on codes of conduct (CoC) as part of a consistency mechanism, confirming that they meet the requirements of the General Data Protection Regulation.

Codes of conduct are rules of behaviour that specify the application of the GDPR. The need for specification of this sort arises from the fact that the regulation is vague in many places and contains general clauses. Codes of conduct can be used as an aid to interpretation and therefore serve to ensure legal certainty. The GDPR links certain “positive” consequences for the companies that have joined the code of conduct to compliance with the code of conduct approved by the competent authority. For example, compliance with approved codes of conduct may be used as a consideration in demonstrating that controllers are fulfilling their obligations (Art. 24(3) GDPR).

It may also be used as a factor for demonstrating sufficient guarantees of the compliance of the processor (Art. 28(5)) or compliance with the security of processing requirements referred to in Art. 32(1) (Art. 32(3)). It should also be taken into account in the data protection impact assessment (Art. 35(8)). Another point worthy of mention is that compliance is taken into account when imposing fines (Art. 83(2) sentence 2 point (j) GDPR).

The EU Cloud CoC addresses all services of the cloud market and in this respect consolidates the requirements of Art. 28 GDPR on commissioned processing and the associated provisions of the GDPR. Cloud service providers are processors. The EU Cloud CoC provides practical help and defines specific requirements for cloud service providers. Like the EU Cloud CoC, the CISPE CoC is a European code of conduct for cloud service providers. Unlike the EU Cloud CoC, however, it only addresses specific features of providers offering Infrastructure as a Service.

Codes of conduct are not only an instrument of self-regulation, but also serve to provide transparency for data subjects. I therefore very much welcome the fact that the business community is also making its contribution to the consolidation and manageability of the GDPR in this way.

3.2.4 Guidelines on accountability and new standard contractual clauses

The European Data Protection Board (EDPB) adopted the final version of Guidelines 07/2020 on the concepts of “controller” and “processor” in the GDPR in July 2021. In addition, the European Commission issued new standard contractual clauses on commissioned processing in June 2021, on which the EDPB had previously commented.

In 2020 the EDPB had adopted the consultation version of the Guidelines 07/2020 (see 29th AR No. 3.2.1). After the end of the public consultation, the guidelines were slightly revised and clarified.

The terms “controller”, “joint controller” and “processor” are of central legal importance for the actors involved in data processing. The guidelines provide guidance on how to distinguish between these terms. The annex to the guidelines contains a flow chart that enables the participants to check their role with regard to data processing. The guidelines are available for download from the EDPB website¹. The German version will be discontinued from the beginning of 2022.

Another important document in the area of commissioned data processing is the new standard contractual clauses issued by the Commission as an implementing decision pursuant to Art. 28(7) GDPR (Implementing Decision [EU] 2021/915, OJ EU L 199, p. 18). The Commission provides a template for a processing agreement (Art. 28(3) GDPR) using the standard contractual clauses. It is important to note that these standard contractual clauses only apply to internal European and thus, of course, also to internal German data processing. If data are transferred to third countries, the new standard data protection clauses pursuant to Art. 46(2) point (c) GDPR apply (see No. 3.2.2.2).

Cross-references:

3.2.2 EDPB focus on third country transfers,

3.2.5 Guidelines on right of access to data under Art. 15 GDPR

3.2.5.1 Right of access to data held by social benefit institutions

Although the provisions of the GDPR have already been in force since 25 May 2016 and have been directly applicable law since 25 May 2018, a large number of social service providers are still unable to take proper account of the right of access under data protection law as a right of data subjects.

Pursuant to Article 15(3) sentence 3 GDPR, the information covered by this right of access is to be provided by the controller in a commonly used electronic format, insofar as the data subject has made the request for information electronically and there is no reason not to provide it in this way. In the reporting period, several complainants asserted this legal claim in their electronic application for information against the German Pension Insurance Federation (DRV Bund)). However, the corresponding information pursuant to Article 15(3) sentence 3 GDPR was not provided by the DRV Bund in the legally required electronic format. This led to numerous submissions, as a result of which I asked the DRV Bund to comment. The DRV Bund then informed me that it is currently unable to provide a suitable electronic procedure through which information can be requested and provided in accordance with Art. 15(3) sentence 3 GDPR. This is a persistent violation of the GDPR. In addition, the DRV Bund has had sufficient time since the GDPR came into force (25 May 2018) to implement a common electronic information procedure for providing information pursuant to Art. 15(3) sentence 3 GDPR. Regulatory measures are currently being prepared.

3.2.5.2 Provision of information by health insurance funds under Art. 15 GDPR

During the reporting period, I received numerous complaints revealing uncertainties on the part of health insurance funds in dealing with the right of access to data of those insured with them under Art. 15 GDPR.

The right of access pursuant to Art. 15 GDPR is a central instrument of data protection for creating transparency in data processing. Although the GDPR has now been in force since 25 May 2018, there is still a great deal of uncertainty among many health insurance funds with regard to the practical implementation of the right of access to data. This is shown by the many complaints under Article 77 GDPR from people covered by such insurance who requested my assistance in enforcing their rights.

The following examples are typical of some sources of error on the part of the health insurance funds in processing requests for access to information:

→ Refusal to provide information with reference to Section 83(2) of the German Social Code Book X (SGB X)

Section 83(2) SGB X restricts the right to information at national level by requiring the rightful claimant to specify in principle the type of social data about which information is requested ("should" clause). This is the rule for large organisational units - such as health insurance funds - because they have complex data processing systems. The alleged lack of detail in the request for information by the data subject is therefore not an absolute reason to exclude the provision of information. However, if the social data is not automated or not stored in automated data processing systems, i.e. in analogue paper form, the "should" becomes a "must". In other words, in this case, the health insurance fund only has to provide information if the applicant provides information that is precise enough for the social data to be found (Art. 83(2) sentence 2 SGB X). In addition, the health insurance fund can weigh the interest in obtaining the information and the effort involved in finding the social data against each other and, if the latter is disproportionate, refuse to provide the information. Accordingly, the health insurance fund cannot be expected to search in large paper archives for the information requested, for example. However, in view of the extent of digitalisation in the health insurance funds, this regulation is likely to be applicable only rarely.

→ Exclusion of correspondence with the insured person

Insofar as the person requesting information pursuant to Art. 15(3) GDPR requests copies of the personal data which are the subject of processing, the controller occasionally excludes from this the correspondence conducted with the claimant. This is done by relying on Recital (EC) 62 of the GDPR, according to which the obligation to provide information does not apply if the data subject already has the information. There is a misunderstanding here, in that the recital does not refer to Article 15 GDPR, which is relevant here, but to Articles 13 and 14 GDPR (information obligations of the controller). The claim under Article 15 of the GDPR therefore also includes correspondence with the data subject.

→ No differentiation between right to access and right to inspect files

In some cases, I found that requests for information were refused on the grounds that there was no legi-

itimate interest in obtaining the information. However, the data subject does not have to demonstrate a legitimate interest. As a matter of principle, their claim to information under Art. 15 GDPR is not at the discretion of the controller, provided that there are no grounds for exclusion. The reason for the incorrect interpretation of the law by the health insurance funds was often the incorrect classification of the requests for information as requests for access to files according to Section 25 SGB X. This right is in fact subject to stricter prerequisites and requires, among other things, knowledge of the file contents in order to be able to assert the legal interests of the data subject as the legitimate interest. In order to avoid procedural delays, I therefore advise data subjects to refer explicitly to Art. 15 GDPR when submitting a request.

→ **Refusal to fulfil a claim in electronic form**

Some data subjects have complained that health insurance funds and other social benefit institutions do not provide copies of personal data in an electronic format. However, the applicant is entitled to this if the application itself was also submitted electronically (Art. 15(3) sentence 3 GDPR). The GDPR does not accept absence of the technical requirements or disproportionate effort as an objection in the case of electronic fulfilment of a claim. The health insurance providers are obliged to provide this form of information.

→ **Missing deadlines**

During the reporting period, I repeatedly received complaints from those insured that their health insurance fund did not respond to their requests for information within the one-month period specified under Art. 12(3) GDPR. Internal communication and procedural shortcomings are often the reason for this. In most cases, I was able to settle the matter promptly.

3.2.6 Guidelines for dispute resolution procedures before the EDPB

Guidelines for dispute resolution procedures before the EDPB describe procedures for reaching a binding decision for European data protection authorities.

The Guidelines 03/2021 on the application of Article 65(1) point (a) GDPR describe the process for a dispute resolution procedure by the EDPB pursuant to Article 65(1) point (a) GDPR. The aim of the dispute resolution procedure is to resolve disputes between the lead supervisory authority and the other supervisory authorities in-

volved by means of a binding decision of the EDPB. Such disputes may arise if European supervisory authorities have not been able to reach a consensus in cross-border processing of personal data within the framework of the cooperation procedure provided for by the GDPR. In such cases, the matter must be submitted to the EDPB, which then issues a binding decision, thus taking into account the goal of consistent application of the law even in individual cases. The guidelines describe, among other things, the procedure and the conditions under which the EDPB can issue a binding decision, as well as its decision-making powers. They thus establish important rules and have already been applied in the dispute resolution procedures carried out in 2021.

3.3 Global Privacy Assembly

3.3.1 General Report

In the year under review, the BfDI was a member of the steering committee of the Global Privacy Assembly (GPA). This Executive Committee performs important tasks that are essential for the GPA and its voice in the world. This year's GPA plenary session dealt with numerous data protection issues and adopted landmark resolutions.

As I reported in my last AR, I was elected to the Executive Committee (ExCo) of the GPA in October 2020. In addition to the five elected members, the previous and current hosts of the annual conference are members of the Executive Committee¹¹.

The ExCo, as the governing body of the GPA, has an overview of the topics of the individual working groups and how the objectives of the GPA are being advanced. The mandate and policy priorities are set in the GPA by means of resolutions. In the reporting year, the implementation of the Strategic Plan 2019-2021 was ensured and the course was set for the strategic plan for the coming years (2021-2023).

Another important task of the ExCo is external representation of the GPA. For example, it can issue joint statements on global issues. This was the case in the reporting year when health data were being processed in relation to national and international travel. ExCo did not generally oppose processing, but pointed out the importance of key data protection principles and practices.

The highlight of the GPA's work is the annual conference, which could only take place digitally in the reporting year due to COVID-19 restrictions. It was organised by the Mexican regulatory authority. The motto was:

¹¹ The names of the members of the ExCo, including their curricula vitae, are published on the GPA's website: <https://globalprivacyassembly.org/the-assembly-and-executive-committee/executive-committee/>

“Privacy and Data Protection: A human centric approach”; in other words, people should be at the heart of data protection. Among the wide range of items on the programme, COVID-19 and new technologies - especially AI - played a significant role.

The GPA also adopted important resolutions that I helped to draft. The strategic plan for the years 2021-23 is of particular importance here. International data transfer, which is increasing steadily, is becoming more and more important. However, the increasing flow of data must not lead to a softening or even an abolition of data protection. The GPA wants to develop practical approaches to ways of protecting individuals whose personal data are processed. This is to ensure that in times of technological progress and data-based business models, the GPA voice continues to be heard. Another resolution comes from the COVID-19 working group of the GPA. The focus of its work was initially on measures as an immediate response to the pandemic. Following on from this, the group is looking more to the future, beyond the narrow reference to the COVID-19 pandemic.

The mandate of the group is being extended to include all aspects of data processing for purposes of general interest. An important decision for the GPA as an organisation was the decision to establish a GPA secretariat financed by membership fees. Finally, the resolution on “Government Access” should be mentioned, which addresses the problem of access

to private data by intelligence services and security authorities and outlines data protection principles for this (see No. 3.4.3).

The GPA Annual Conference 2022 will be hosted by the Turkish Data Protection Authority (KVKK).

3.3.2 Reference Panel

In March 2021, the Global Privacy Assembly - a worldwide association of data protection authorities - created the “Reference Panel”, a new body of independent experts. I became the first chair of the Panel.

The Global Privacy Assembly (GPA), known until 2019 as the International Conference of Data Protection and Privacy Commissioners, had adopted a number of measures at its 40th conference in Brussels in 2018 to modernise itself and better meet the demands of the digital age. Along with a new name -

- Global Privacy Assembly - these measures included the establishment of a panel of independent experts representing different sectors, e.g. academia, non-governmental organisations, the private sector and public authorities. This new body of external experts has the task of bringing additional expertise and external perspec-

tives into the GPA. This is to ensure that the GPA's work is relevant and useful to all the bodies and stakeholders involved in digital society.

After the 42nd Annual General Meeting of the GPA in autumn 2020 had accepted the concept and name for the new body -

- GPA Reference Panel - the selection process for suitable panel members began at the beginning of the reporting year under the leadership of a “GPA Reference Panel Assessment Group” set up for this purpose, which was led by the chair of the GPA, the UK Information Commissioner (ICO), and the work of which I supported. A total of 16 leading data protection experts from Germany and Europe were appointed to this international group. I would like in particular to thank the two members from Germany, Mr. Andreas Mundt, President of the Federal Cartel Office, and Prof. Franziska Böhm from the Karlsruhe Institute for

Technology (KIT), for their willingness to participate in the GPA Reference Panel.

In my capacity as a member of the GPA Executive Committee, of which I have been a member since October 2020, I have taken over as chair of the GPA Reference Panel. Its first task was to assist the host of the 43rd annual meeting of the GPA in autumn 2021, the Mexican data protection authority INAI, in drawing up the programme for the meeting. Another essential task of the GPA Reference Panel is to review the reports and papers of the GPA's thematic working groups in the sense of a “peer review”, if this is requested by the chairs of the working groups concerned or a team of authors of such a report. I welcome the fact that there was a lively demand for this from the GPA working groups even in the first period of the Panel's existence. For example, various members of the GPA Reference Panel analysed a comprehensive report of the Policy Strategy Working Group - Workstream 3 on the topic of “Data protection and other fundamental rights and in relation to other fundamental rights” and responded in detail to the authors.

In my view, it is crucial for the Global Privacy Assembly to think “outside the box” and connect with civil society as well as key players in the digital age. Only then will the GPA continue to keep its finger on the pulse and be able to address new developments at an early stage and promote data protection-friendly solutions. As chair of the GPA Reference Panel, I want to play my part in achieving these goals.

Cross-references:

3.3.1 General report

3.4 Other international bodies

3.4.1 G7

The UK Data Protection Commissioner invited the data protection authorities of the G7 countries to a roundtable discussion in the reporting year. The background to this invitation was that the United Kingdom chaired the G7 Summit in 2021. During the talks, possibilities for continued closer cooperation in this group were discussed.

More and more data is being generated, collected and used worldwide. In an increasingly globalised and digitalised world, data flows across the borders of countries and continents. Data protection supervisory authorities must cooperate internationally in this area to preserve data protection. When the data of German and European citizens leave the areas governed by their laws, they must not be unprotected. To improve this protection, deepening and broadening of international cooperation is essential.

In September 2021, the data protection and privacy authorities of the G7 countries met for the first time for a joint roundtable discussion at the invitation of the then UK Data Protection Commissioner, Ms Elizabeth Denham. The World Economic Forum and the OECD also participated in this new international format. The meeting was linked to the UK chairing the 2021 G7 Leaders' Summit.

In April 2021, the digital and technology ministers of the G7 countries agreed on a roadmap for cooperation to promote free and reliable flow of data (Data Free Flow with Trust). The aim here is to identify commonalities in the regulation of international data transfer and to share good regulatory practices and opportunities for cooperation. The roundtable was a contribution by data protection authorities to this important issue.

The 2021 G7 digital and technology ministerial declaration on data free flow with trust is based on

- the 2019 Osaka Leaders' Declaration of the G20 countries,
- the 2020 G20 Leaders' Riyadh Declaration.

Data free flow with trust has been a topic in the final declarations of the G7 and G20 meetings for several years. This once again shows its growing importance.

The roundtable discussed possibilities for closer cooperation between the data protection authorities of the G7 countries. In a joint communiqué¹², core approaches to the following topics were set out:

- Data protection and competition
- Online tracking
- Artificial intelligence
- Redesigning remedies for the digital age
- Pandemic-driven technological innovations ^ "Government Access" and the
- development of a framework for international data transfer.

Continued dialogue between the authorities and a roundtable on the individual areas were agreed for 2022, and I would like to organise this during the German G7 Presidency. In view of the importance of digitalisation, I ask the federal government, as part of its G7 Presidency, to continue the dialogue with the data protection authorities in the G7 forum.

Cross-references:

3.4.3 Data protection principles for state access to personal data in the international sphere, 4.2 Artificial intelligence - regulation as a task for society as a whole, 6.3 Cooperation between antitrust and data protection supervisory authorities

3.4.2 Berlin Group

The International Working Group on Privacy in Technology, which brings together independent experts, has been in existence since 1983. In March 2021, I took over as its chair from the Berlin Data Protection Commissioner.

In March of the year under review, I took over as chair of the "International Working Group Data Protection in

Technology" (IWGDPT) on a permanent basis. Since the group was founded in 1983 at the instigation of the then Berlin Data Protection Commissioner and initially met frequently in Berlin, the IWGDPT also became known as the "Berlin Group".

The distinctive feature of the IWGDPT - apart from its long tradition - is its independence and diversity. In addition to members of data protection authorities, experts from the fields of science and research, from non-governmental organisations and data protection-related think tanks also work here. It also includes authorities and institutions involved in the regulation of data protection-related areas and services.

The IWGDPT is independent of the GPA and determines its own thematic focus and direction. Nevertheless, it has a close relationship with the GPA. For example, the chair of the IWGDPT regularly reports on the Group's

¹² Brief announcement of the BfDI of 14 September 2021, available at: www.bfdi.bund.de/kurzmeldungen

activities in the plenary meeting of the GPA annual conference.

The IWGDPT was able to continue its work during the reporting period despite the coronavirus pandemic, albeit with restrictions. For example, the Group finalised a working paper on sensory networks, continued work on a paper on voice-controlled devices and started new work on smart cities and facial recognition technology. In my new role as chair of the IWGDPT, I will work hard to continue the intensity of dialogue and the high quality of the IWGDPT's working papers and recommendations.

Cross-references:

3.3.1 Global Privacy Assembly

3.4.3 Data protection principles for government access to personal data in the international sphere

Common data protection principles for access by law enforcement and security authorities to personal data of private entities are to be agreed in various international forums. Such common principles for government access can make an important contribution to legally satisfactory design of cross-border data exchange and raise the level of data protection outside the EU as well.

State access to personal data processed by private entities was the focus of various data protection law initiatives in 2020.

Under the heading of “Government Access”, access by law enforcement and security authorities in the context of cross-border data processing was dealt with in several international forums. This applies in particular to the work within the framework of the Global Privacy Assembly (GPA) and the Organisation for Economic Cooperation and Development (OECD). Building on this, the data protection supervisory authorities of the G7 countries have also discussed the topic of government access. The background is the effort to agree on common data protection principles for government access at the international level. These efforts are also prompted by the Schrems II ruling of the ECJ. In assessing the level of data protection in third countries, the court focuses on the protection of personal data from access by the security authorities.

Access by the security authorities to data held by private bodies is a sensitive issue. It affects issues of national

security in individual states. At the same time, it shows the importance of free data traffic for the global digital economy. Developments in recent years have clearly shown that an absence of or inadequate international data protection guarantees are not just a risk to the protection of personal data. There is also a significant economic impact.

For European data protection law, these initiatives are a challenge. On the one hand, it is desirable to create common international data protection principles. On the other hand, European

data protection law provides a binding legal framework for the transfer of personal data to third countries. This results in an area of tension for my work: agreement of international principles can make an important contribution to enabling cross-border data exchange and raising the level of data protection outside the EU in a sustainable way. However, European data protection standards must not be undermined in the process.

At its annual conference in October 2021, the GPA adopted a resolution on strengthening data protection principles for government access.

I actively participated in drafting the “Resolution on government access to data, privacy and the rule of law: principles for governmental access to personal data held by the private sector for national security and public safety purposes”. Within the framework of the OECD, so-called “Principles on government access to personal data held by the private sector” are being negotiated, but have not yet been adopted.

I welcome the fact that the GPA adopted the common data protection principles in October. At the same time, I hope that the work within the OECD can be taken forward in terms of data protection, taking into account the results arrived at by the GPA.

At the G7 level, I have supported a further intensive exchange of views. This is intended to support the principles developed by the GPA and the OECD initiative in terms of data protection policy.

Cross-references:

3.2.2.1 Supplementary Measures Taskforce/Implementation of Schrems II, 3.3.1 General Report, 3.4.1 G7

4 Main topics

4.1 Coronavirus

4.1.1 Coronavirus warning app

Since 16 June 2020, the federal government's coronavirus warning app (CWA) has enabled its users to warn one another quickly about risky encounters in a privacy-friendly manner. In addition to contact tracking, other functions have since been added. The reliance on the operating system manufacturers Apple and Google prevents further improvements in terms of data protection. The Robert Koch Institute (RKI) has evaluated whether the CWA fulfils its purposes.

I continued to advise the RKI after 16 June 2020 on the introduction of the new functions, including contact tracking when visiting certain locations (event registration) and the integration of test and vaccination certificates into the CWA. In addition, I was responsible for data protection supervision and dealt with complaints from the public. Many complaints related to the fact that the CWA could not be obtained directly from the RKI but only via the platforms of Apple and Google, as well as the "compulsory installation" of Google/Apple Exposure Notification (GAEN), which is necessary for distance measurement, but which is part of the operating systems and therefore does not fall within my legal area of responsibility.

Data protection facilitates accepted and needs-based solutions

With almost 39 million downloads by the end of 2021, the CWA is the largest and one of the most widely accepted apps of its kind in Europe. Data protection plays an important role in the trust that the CWA enjoys. It in no way prevents its success, in fact it is a success factor.

The CWA also proves that privacy-friendly solutions do not have to come at the expense of effective functioning: not one appropriate planned function had to be restricted or even omitted for reasons of data protection.

Data protection needs "digital sovereignty"

Without the GAEN of the operating system manufacturers Apple and Google, the CWA would not have been feasible last year. The general criticism of the use of GAEN and in particular the accusation of unauthorised access to data was initially not substantiated by clear evidence. On 12. April 2021, however, the company "appcensus" published a vulnerability in Google's API for exposure notifications. According to this, installed apps could access the GAEN data. Although Google subsequently assured me that it had closed the loophole, it is not known whether it had been exploited.

Unfortunately, GAEN did not remain the only function of the two operating system manufacturers used in the CWA. The integrity check of the companies Apple and Google was integrated into the CWA for data collection to evaluate the CWA. It is not known which data are sent to the two operating system manufacturers for verification. The plan is also to enable the function of exporting and re-importing the CWA user data, which might be helpful if users change their smartphone, with the help of functions specific to the operating system. Apple and Google could then access the CWA data.

The reasons for using the services of the operating system manufacturers Apple and Google ranged from "absolutely necessary" (GAEN), through "necessary in terms of validation and preferable to user registration" (during evaluation), to "clear user benefit" (data import and export).

I have always made it clear to the RKI in various statements that it is preferable not to use the services of the operating system manufacturers wherever possible and I have suggested alternatives. The fact that this has not met with any response so far remains, in my view, the biggest shortcoming in the CWA's data protection. I believe it is necessary to make the follow-up and further development of the CWA as independent as possible from the operating system manufacturers Apple and Google

in order not to reinforce the lack of digital sovereignty in the EU.

Does the CWA fulfil its purposes?

The RKI specified when the CWA was launched that its purposes should be evaluated. The RKI fulfilled this task with two reports in April and September 2021. As a result, I can definitely see potential for improvement in future developments.

In order for a PCR test result for the SARS-Cov-2 virus to reach the CWA quickly and directly, the user must register the test with a QR code (QR code procedure). In addition, the test laboratory must be able to process this QR code. Even in 2021, this was not the case for all laboratories. Users then had to request a “tele-TAN” by phone to share their positive test result. This more complex and, from the point of view of data protection, rather undesirable procedure (users have to leave their telephone number) reduces the rate of sharing of positive test results. The RKI has not yet evaluated whether the “tele-TAN” procedure will still be necessary in the future and what measures are planned to make it obsolete.

The QR code procedure has proven itself in practice: according to the RKI, around three quarters of those who used these procedures received their results within 24 hours. In the vast majority of cases, this fulfils the requirement to share the test results in a timely manner.

One purpose of the CWA is to warn other users of having come into contact with an infected person. In these cases, the receiving CWA displays a “red tile”. In the evaluation report, the RKI stated that “the vast majority of critical contacts are correctly detected by the coronavirus warning app”.

The RKI’s surveys of CWA users confirm this thesis, at least in part: users who took a SARS-CoV-2 test in response to a CWA “red tile” had a positive test result more often than the average of all those tested.

I note that the evaluation report does not include findings about the possibilities and limitations of contact tracing using the CWA. Should contact tracing also play an important role in future pandemics from an epidemiological point of view, this would have to be done urgently, including as a way of increasing the accuracy of warnings

In summary, from my point of view the CWA has become a successful reference tool for combating the pandemic by means of smartphone app, both nationally and internationally. My conclusion is therefore positive, not least because - after initial hesitation - other useful functions such as event registration and vaccination and test verification via the CWA have been added.

Nevertheless, I also see limits to the use and impact of such apps. An evaluation should include shortcomings and opportunities for improvement as well as the possible role of a CWA in an overall approach to pandemic response where it interacts with other measures. Here in particular, there still seems to be plenty of potential for improvement.

4.1.2 SORMAS

In order to move finally from paper and fax to efficient and data protection-compliant digital contact tracing in health authorities, intensive monitoring of the project was necessary.

The SORMAS software is a contact person management system for the SARS-CoV-2 pandemic, on which I reported in my 29th Activity Report (No. 4.1.3). The software is intended to support the health authorities in identifying and monitoring contacts by recording symptom information of contacts without telephone queries and by sharing data on case reports with other health authorities. In addition to digital receipt of laboratory reports, case data is also to be reported digitally to the state authorities. At the Minister Presidents’ Conference on 16 November 2020, it was decided to use SORMAS in health authorities throughout Germany.

In consultation with the data protection supervisory authorities of the states involved, I conditionally approved the operation of SORMAS-X in health authorities in January 2021 after a joint discussion of the documents submitted. The prerequisite for this was a written assurance that the documents would be improved and completed during ongoing operations. This should enable risks to be identified in the course of the risk assessment and necessary technical and organisational measures to be taken. It should be done as quickly as possible, using adequate resources. The data protection impact assessment was only submitted in draft form. A cryptography concept was also necessary. The consultation was extended again from July 2021 and a working group was set up with my participation and that of several state data protection commissioners. The background was that the progress on the part of the Helmholtz Centre for Infection Research (HZI) over a longer period of time did not meet the expectations that the state commissioners and I had of such a project. For example, deadlines for the submission of documents for which there is still a need for significant consultation, such as the erasure concept, the data field table and the data protection impact assessment, were repeatedly postponed for several months. At the end of the reporting period, the HZI’s cooperation with the federal and state data protection supervisory authorities improved. I expect the consul-

tation on this extremely agile project to be completed during the first half of 2022.

4.1.3 EU digital COVID certificate

Originally, the focus here was on easing travel restrictions at the European level. By the end, data protection-friendly evidence of COVID-19 certificates were part of everyday life.

On 17 March 2021, the EU Commission presented a draft regulation on the Digital Green Certificate. The EU Regulation aims to facilitate cross-border travel for EU citizens during the coronavirus pandemic within the EU.

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted a joint opinion on this issue on 31 March 2021. Under this, any measure adopted at national or EU level involving the processing of personal data should comply with the general principles of effectiveness, necessity and proportionality. Data processing operations should also be based on an adequate legal basis in the Member States. At the same time, the EDPB and the EDPS asked the EU Commission to clarify that Member States should accept all three types of certificates (vaccinated, recovered or tested). If they did not do so, it would constitute discrimination on the basis of health data and thus a violation of fundamental rights.

The EU Digital COVID Certificate Regulation entered into force on 1 July 2021. Three certificates are defined: vaccination, testing and recovery. Member States must offer the certificates in paper and digital form. Use of the certificates is voluntary. They are non-discriminatory, as they do not create travel restrictions in Europe, but rather facilitate cross-border movement for holders by dispensing with further measures by individual Member States during the coronavirus pandemic (e.g. quarantine regulations) as appropriate. Neither tracking (simultaneous tracking) nor tracing (subsequent tracking) takes place. The certificates are used for authentication and to determine the status of the holder when crossing the border. Personal data is not stored by the controlling bodies.

The regulation and thus the certificates are limited in time. As soon as the WHO declares the coronavirus pandemic over, the EU Commission will repeal the regulation with a legislative act. The regulation itself allows the use of the certificates for one purpose only - facilitating freedom of travel. It also opens up the possibility of further use by Member States (e.g. access to events, public facilities, etc.). German legislation has made use of this and introduced temporary regulations in the Infection Protection Act, for example for access to

health and social care facilities, local and long-distance transport and in the hotel and restaurant sector.

In Germany, the certificates are generated technically on behalf of the Robert Koch Institute (RKI). No data are stored in the process. The certificates can be displayed in the CovPassApp and the Coronavirus Warning App. A check of the validity of the certificates can be carried out with the CovPassCheck app. I supported the development of these applications throughout all programme versions in terms of data protection law and gave detailed advice not only to the BMG but also the RKI as the controller for the apps.

Cross-references:

4.1.1 Coronavirus warning app

4.1.4 Coronavirus Notification Regulation

The Coronavirus Notification Regulation is more complex than it needs to be. Less data would have allowed for faster processing.

On 29 June 2021 - with a deadline for comments of 1 July 2021 - I received the first draft of the Federal Ministry of Health (BMG) of a "Regulation on the extension of the notification obligation in accordance with Section 6(1) sentence 1 number 1 of the Infection Protection Act (IfSG) to hospitalisations relating to the coronavirus disease-2019". Behind the unwieldy title lies an additional duty for hospitals and health authorities. The aim is to determine the incidence of hospitalisation as a guide for protective measures. Hospitals must report the admission of patients by name to the health authority, even if it is already aware of the coronavirus infection. Subsequently, the health authorities have to check the notification, assign it and then report it under the usual procedure with an identification number to the state authority, which forwards the notification to the Robert Koch Institute (RKI). I had considerable doubts as to whether the requirements on which authorisation is based (Section 15(1) IfSG) had been met. According to these, the BMG may extend the notification obligation under Section 6 IfSG if the epidemic situation so requires. However, it was not clear why an additional notification of the health authority should be necessary. The justification related to the number of hospital admissions - i.e. purely statistical data. This information is probably less relevant to the work of the health authority than to the RKI's assessment of the pandemic situation. For reasons of data minimisation, it would have been appropriate for the hospitals to report the admission of patients statistically - i.e. anonymously, without personal details - directly to the RKI. I had therefore recommended to the BMG in my comments that it should follow the now established procedure for reporting intensive care patients. This can

be done using the numbers alone and just a few other details. Nevertheless, the cumbersome procedure was retained and it is therefore not surprising that notification delays are being reported time and again.

4.1.5 The Federal Emergency Brake and the Exemption Regulation

Pandemic control virtually turns health data into a free pass. Digital solutions mitigate the risks only to a limited extent. Clear confidentiality measures would have been a good start. Such obligations to provide evidence are permissible only to the extent and for as long as they are necessary to avert danger.

In the last Activity Report, I reported on the changes to the Infection Protection Act caused by coronavirus through the first, second and third Pandemic Protection Act (29th AR, 4.1.4). As the pandemic progressed, there were new amendments to the law and to regulations, regrettably also with unnecessarily short deadlines for consultation and review.

Federal Emergency Brake

I only found out about the so-called “Federal Emergency Brake” in the draft of the „Fourth Act for the Protection of the Population in the Event of an Epidemic Situation of National Significance”, a bill of the coalition fractions (BT- Drs. 19/28444), from the agenda for the Health Committee meeting of 13 April 2021. I was not involved in advance. The protective measures themselves, such as contact restrictions and operating bans, are not relevant to data protection. However, Section 28c of the draft law also contained a power to issue regulations which included easing of restrictions or exemptions for immunised people and those testing negative. The associated evidence and knowledge of it constitute processing of health data and are permissible under Art.

9 GDPR only under special conditions and with special requirements for the protection of data subjects. However, this is not mentioned in the draft or its explanatory memorandum. The Act was published on 22 April 2021 (Federal Gazette (BGBl.) 2021 I, p. 802).

Exemption with evidence

On the basis of the authorisation to issue ordinances, on 4 May 2021 the federal government published the draft of an “Ordinance on the regulation of easing of and exemptions from protective measures to prevent the spread of COVID-19 (COVID-19 Protective Measures Exemption Ordinance - SchAusnahmV)” (BT-Drs. 19/29257), which again I only became aware of through the agenda of the Health Committee. The fact that I was not involved beforehand breaches Section 21(1) of the Joint Rules of Procedure of the Federal Ministries (GGO). The ordinance

issued on 8 May 2021 (BAnz AT 08. Mai 2021 V1) contains specifications on how the proof of immunisation or negative testing must be provided and which requirements must be fulfilled. The ordinance then mentions the regulations of the “Federal Emergency Brake” in Section 28b IfSG that do not apply to those who can provide this proof. With this regulation, personal health information became an entrance requirement and business owners, hoteliers, restaurant owners and associations became - more or less conscientious - ticket inspectors. Even if the CovPassCheckApp is used for a data protection-friendly check, the certificate means that the person requesting to see it learns the name and date of birth of the person presenting it. I would therefore have expected an accompanying requirement for confidentiality on the part of those carrying out the checks.

Obligation to provide evidence as a protective measure

With the Reconstruction Aid Act 2021 of 10 September 2021 (BGBl 2021, p. 4147) - Art. 12 - an obligation to present proof of vaccination, recovery or testing was then also included in the catalogue of possible measures in Section 28a IfSG as a direct protective measure. Again, the statement of grounds for the draft law lacked a reference to the fact that the evidence is health data, which are subject to special protection under Art. 9 GDPR. The obligation to provide evidence leads to situations that are uncomfortable for both those providing the evidence and those checking it. This encroachment on the right to informational self-determination was not accompanied by stipulations or explanations, despite my advice. This was left to the federal states. There was not even a suggestion that an order implementing these measures would have to undergo special scrutiny and that the data would have to be treated confidentially. According to Art. 9(2) GDPR, the processing of health data is only possible as an exception under certain conditions. The fact that the pandemic constitutes such an exceptional situation should have been made more transparent. I therefore pointed out to the BMG that pandemic response measures must be continuously reviewed and that legal obligations to process personal data must be lifted as soon as possible. Further draft laws and ordinances then came to me for which the

ministerial administration mostly gave me only a short time window, in some cases only hours, to examine and comment on them. Where I was able to identify data protection problems within the short deadlines, I raised them. Nevertheless, I was and am aware that under the given circumstances a comprehensive examination and evaluation of the draft laws and ordinances was not possible. This is all the more reason for me to monitor their further legislative development and subsequent implementation in practice. Possible legislative deficiencies

cies are likely to be reflected not least in an increased number of complaints and submissions and also in an increased risk of failure to pass judicial review. Already in the reporting period, the number of complaints and submissions I received in the health sector has reached a new record high.

Cross-references:

4.1.3 Digital vaccination certificate

4.1.6 Coronavirus Testing Ordinance

The same applies to citizen testing centres: when processing health data, special safeguards are required - such as a professional obligation to maintain confidentiality. If staff who are not doctors are to carry out any of the work, alternative specifications are necessary.

The “Ordinance on the right to testing with regard to direct pathogen detection of Coronavirus SARS-CoV-2” (Coronavirus Test Ordinance - TestV) was first issued in May 2020 and amended thereafter - at times once a month. I was first included in the departmental coordination in January 2021. The draft amending ordinances subsequently submitted had unreasonably short comment periods, usually by the same day or the next day, in individual cases by the next week. In my review, it was crucial for me to know who processes the data of those being tested and what rules apply to their storage and transmission.

There was no cause for concern in the early versions: initially, only doctors’ practices and later also pharmacies were involved in the testing, in addition to the public health authority, i.e. persons who are subject to a professional duty of confidentiality. In addition, the process was intended to run without collecting the details of those tested. When public testing - which is free of charge for those tested - was introduced, the circle was expanded to include “other appropriate third parties”: the health authority may also appoint “other providers who guarantee proper implementation, in particular after training in accordance with Section 12(4)”. Since the test providers process health data in addition to name and address, and a positive test also triggers the obligation to notify the public health authority, I had expected that the state authorities would set guidelines for data protection and data security for the test centres when implementing the regulation. However, this was not consistently the case. The addition of “in particular” apparently gave the impression that training was the essential criterion for permissible appointment. In any case, a large number of rapid test centres were subsequently established - in tents, containers, empty event rooms and shop premises. Whether the data processing of the respective controllers was in compliance with the requirements of the

GDPR for health data was sometimes doubtful; various mishaps became known, some of them significant. It was not until the Amendment Ordinance of 12 November 2021 that the requirement that the other service providers must also be obliged to maintain confidentiality was included, after I pointed the problem out.

Ambiguities were also caused by the - unchanged - obligation to keep the order and performance documentation. For doctors, this requirement corresponds to standard practice. However, what it meant for “appropriate third parties” and whether this was a sufficient basis for storing personal health data was doubtful.

It also led to uncertainty among users and discussions on the part of the data protection authorities. However, under the pressure of suspected billing fraud, the June version of the TestV contained a specific list of documentation to enable auditing of billing. Even the test result, an item of health data that requires special protection, is intended to be kept until the end of 2024. The point of this is not clear: payment is made regardless of the test result and verification of reliable notification of positive tests is only meaningful if it is carried out promptly. Storage would therefore be necessary for a few months at most. In response to my comments, the October version at least provides for a shorter deadline of the end of 2022 for test results.

After the abolition of public testing, eligible people had to claim their right to free testing and prove a medical impediment to vaccination or that they were pregnant. Here I made it clear to the BMG: pregnant women are also entitled to a certificate containing only the necessary information; they do not have to use their maternity record, which includes a multitude of information. And a certificate of a medical contraindication should not contain any diagnosis, as this is not relevant here.

Cross-references:

4.1.8 Infection Protection Act

4.1.7 The “Epidemic Situation Continuation Act”

Pandemic obligations and interventions without a pandemic situation? The time limit on the pandemic-related regulations was removed by the Epidemic Situation Continuation Act and decoupled from the existence of the epidemic itself. This also applies to the transfer of certificates based on the obligation to register under the Entry Regulation.

On 2 February 2021 the Federal Ministry of Health (BMG) sent out draft formulation guidance for the “Draft Act on the Continuation of the Regulations Concerning the Epidemic Situation of National Significance” - (Epidemic Situation Continuation Act)”, once again with an

extremely short deadline for comments of 4 p.m. on 3 February 2021. The formulation guidance included the maintenance beyond the end of the epidemic situation of the regulations that were enacted as a result of the declaration of an epidemic situation of national significance and that would largely cease to apply when it was lifted, at the latest, by 31 March 2021. The epidemic situation itself was intended to apply for a limited period and require a resolution to extend it.

This intended temporal restriction of the epidemic situation paved the way for the review and made reconsideration of the pandemic-related regulations by the German Bundestag a requirement under constitutional law, which is something I welcome. For various powers granted under the ordinance, on the other hand, the additional time limit previously set was to be dropped, so that they would automatically apply for the same length of time as the epidemic situation itself. This also applied to the Coronavirus Entry Regulation. According to this regulation, which was amended several times, there was a registration requirement for entrants regardless of the means of transport used. Various personal details and information about where the person would be living had to be submitted to the health authority. However, it is conceivable that, under certain circumstances, this obligation would not make a substantial contribution to pandemic control, even if the official declaration of an epidemic situation continues or is extended.

I therefore argued that only by setting a time limit for the regulation, regardless of the epidemic situation, is it possible to ensure a regular review of whether the data transfer obligations are necessary and comply with data protection requirements.

A revised version of the formulation guidance was issued in the early afternoon of Saturday, 6 February 2021, with a deadline for comments of Sunday, 7 February 2021. If no feedback was received by then, the BMG would - rather surprisingly - assume approval. Such an approach, involving an extremely tight deadline over a weekend, is unprecedented and makes my task of advising the federal government and the Bundestag unnecessarily difficult. Such an approach cannot be reconciled with the regulations of the Joint Rules of Procedure of the Federal Ministries (GGO) either. This procedure was also not appropriate to the constitutional significance of the envisaged regulations, as some of them allow for extensive encroachments on citizens' legal positions protected by fundamental rights.

I therefore approached the Health Committee and again raised my concerns about automatic renewal and the need for an ongoing review of necessity.

To my regret, my comments were not taken into account. In July 2021, the fourth Pandemic Protection Act instead provided for a further change: according to this, the ordinance can even apply for a maximum of one year beyond the duration of the epidemic situation. In principle, the end of the epidemic situation implies that the regulations introduced in response to the pandemic become dispensable. The extent to which the obligations and interventions should still be necessary after the epidemic situation has ceased to exist therefore requires careful ongoing review.

Coronavirus Entry Regulation

The Coronavirus Entry Regulation was revised on 12 May 2021 and applied for the duration of the epidemic situation. Unfortunately, I was not involved at all before this new version was adopted and only became aware of it after the fact. Subsequently, regulations were already being discussed in the press, even though the departmental coordination had not been completed.

According to the new version of the regulations, those entering the country also had to submit a certificate proving that they had been vaccinated, had recovered or been tested to the competent health authority via the portal for digital entry registration. The fact of the existence of the certificate (the "whether") is already confirmed in the application. Submission was previously only necessary on request by the authority.

Unfortunately, contrary to Sections 62, 43 GGO, the justification for the amendment is inadequate in the description of the regulation and there is no explanation of why a random check should no longer be sufficient. As far as this expansion of precautionary data transfers on entry is concerned, it was therefore not evident that the benefit of the new regulation would justify the greater extent of intervention. In the July version, the regulation was then limited until the end of 2021, regardless of the existence of the pandemic situation.

In the following revised version in September, in which my participation was regrettably overlooked again, the deadline remained unchanged. A continuous review of whether the data transmission associated with the registration obligation is appropriate and necessary for combating the pandemic is nevertheless required.

4.1.8 Second IfSG Amendment Act: retrospective digital recording of vaccinations and 3G in the workplace

Retrospective recording of data and 3G in the workplace as one of the data protection challenges of the pandemic response - Germany is digitalising vaccination certification with risks surrounding its reliability and is

assigning an essential role in the pandemic response to employers.

As soon as the Fourth Population Protection Act of 22 April 2021 came into force, the next amendment to the Infection Protection Act was already being undertaken. On the afternoon of Friday, 23 April 2021, the draft of an “Act to amend the Infection Protection Act and other laws” was submitted, once again with an extremely short deadline for comments of Monday, 26 April 2021. The aim of the amendment was to allow supplementary entries on the vaccination certificate and issuing of digital vaccination certificates by pharmacists. This was apparently intended to help vaccinated people obtain the EU Digital Certificate as quickly as possible, without placing an undue burden on vaccination centres and GP practices. The vaccination campaign was already in full swing: members of risk groups had already received their vaccination through vaccination teams and vaccination centres before the technical specifications and the necessary connections and transmission channels for generating the digital vaccination certificate were available.

This approach is understandable. However, the regulation goes far beyond this: it is general in nature and thus not limited to coronavirus vaccinations. Retrospective registration or confirmation by a person who has not carried out the vaccination themselves always involves a risk as far as the accuracy of the content is concerned.

On the other hand, only a vaccination certificate that certifies that vaccination has actually been carried out can serve to protect against infection. At that time, there was already a considerable number of forged vaccination certificates in circulation. With retrospective registration by pharmacies under their own electronic signature, the person making the registration assumes

responsibility for the accuracy of the content. I considered the risk of generating a considerable number of incorrect digital vaccination certificates to be considerable in this way and the interest in forged certificates to be high because of the associated advantages.

This significant risk has not been addressed in any way by the draft law. It was not until the “Act to amend the Infection Protection Act and other laws on repeal of the declaration of an epidemic situation of national significance” of 22 November 2021 (BGBl 2021, p. 4906) that the criminal offences in the Criminal Code were adapted so that action could be taken against known forgeries. Unfortunately, there was no consideration of any other support for vaccination centres and medical practices which - in line with my recommendation - would ensure reliable, accurate retrospective recording by the vaccinating institution itself. Similarly, contrary to my

recommendation, retrospective recording was generally allowed; it was not limited to special cases - such as vaccinations before the possibility of digital recording, special exemptions or even to coronavirus vaccinations - only or restricted in time. Data processing that is prone to risks is adopted as the approach here. These points should be on the agenda for the expected evaluation of the Infection Protection Act.

3G in the workplace

In the same legislative procedure of 22 November 2021 (BGBl 2021, p. 4906), regulations on the processing of so-called 3G data (“vaccinated, recovered, tested” - in German: “geimpft, genesen, getestet”) in the workplace were included for the first time. Long before that, I advised the federal ministries responsible to create legal bases in line with data protection that allow processing of 3G data in the workplace.

However, the legal regulation now includes an obligation to check the 3G status before access is granted to the workplace. Employers are allowed to process the sensitive 3G data from their employees’ vaccination, convalescence or testing records to the extent necessary for the purpose of controlling access to the workplace and documenting compliance with the legal access requirements. In addition, the data may be processed for adaptation of hygiene concepts based on the risk assessment.

The deadlines for comments were again very short in this legislative procedure.

I would have liked to have had much earlier participation in consultation, which would have been easy to arrange according to my early information. I consider

data protection-compliant application of the legal requirements to be indispensable: employers must carefully consider which of their employees’ sensitive health data they absolutely have to collect, store or otherwise process and under which conditions for the respective purpose. The principles of data minimisation (Art. 5(1) point (c) GDPR) and storage limitation (Art. 5(1) and 17 point (e) GDPR) and the special requirements for processing of sensitive health data according to the Federal Data Protection Act and the General Data Protection Regulation must be taken into account. If, for example, the exact 3G status of employees is collected by means of visual inspection or CovPassCheck app before access to the building, it is not usually necessary for access control to store the 3G status of the individual for an extended period of time. To fulfil the documentation obligation, it is sufficient to establish verifiable processes for the way in which the 3G status of employees is checked by employers.

As a rule, personal 3G data of employees are not required for adaptation of company hygiene concepts. It must be considered whether the processing purposes can also be achieved with anonymised, pseudonymised or aggregated data. It is also important that collection is carried out by people who are under a confidentiality obligation vis-à-vis the employer, for example not by immediate superiors, and that the 3G data are protected by technical-organisational measures to prevent unauthorised knowledge by third parties. This also includes colleagues. As soon as the purpose for storing the health data has ceased to exist, they must be deleted. The storage period can therefore turn out to be much shorter than the maximum of six months from collection which is permissible under Section 28b(3) sentence 9 IfSG.

Cross-references:

4.1.3 Digital COVID certificate

4.1.9 Digital vaccination rate monitoring

The difficulty of keeping track of vaccinations in the pandemic by digital means or: (Too) many roads lead to the Robert Koch Institute. The notification obligation introduced with measles protection and expanded under the pandemic does not entirely fulfil its purpose and should be fundamentally revised, together with the notification procedure.

With the Third Population Protection Act (Third Act for the Protection of the Population in the Event of an Epidemic Situation of National Significance of 18 November 2020, 29th AR No. 4.1.4), Section 13(5) of the Infection Protection Act (IfSG) provided for an obligation of the associations of statutory health insurance doctors and the vaccination centres to report data on vaccination and vaccination consequences, which would have to be transmitted to both the Robert Koch Institute (RKI) and the Paul Ehrlich Institute (PEI).

The duplication, which I criticised as being unnecessary and not in line with data minimisation, did not actually occur in practice: the data are sent to the RKI, which forwards them in aggregated form to the PEI. A correction of the corresponding legal regulation did not take place, although I had urged this in my statement on the Epidemic Situation Continuation Act (see No. 4.1.7). Incidentally, the Federal Ministry of Health (BMG) had actually already promised to review the basic data and transmission procedure in connection with the Measles Protection Act (cf. 28 AR No. 5.6). Instead, the concept is being further expanded on the basis of questionable regulation.

In March, an amendment to the Regulation on the Entitlement to Protective Vaccination against the SARS-CoV-2 Coronavirus (Vaccination Regulation) extended the group of those entitled to administer vaccinations and obliged to submit notifications to include medical practices and company doctors. The draft Amendment Regulation was sent to me on 22 March with a deadline for comments of 25 March.

The short deadline also made proper examination difficult here, as did the inadequate explanations in the explanatory memorandum. The different reporting channels made this necessary: some of the notifications are sent directly to the RKI in aggregated form, some are sent to the Association of Statutory Health Insurance Physicians on a person-by-person basis, some use the electronic reporting system of the Federal Association of Statutory Health Insurance Physicians, and some use the German Electronic Reporting and Information System pursuant to Section 14 IfSG (DEMIS), which is provided by the RKI. The question here was whether an aggregated, anonymous and direct transmission would have sufficed overall. In fact, despite - or because of - the comprehensive regulation, there is known to be considerable uncertainty about the actual vaccination rate.

As early as 2020, I had begun advising the RKI on the technical implementation of the reporting procedure, which was to be run in cooperation with Bundesdruckerei. The vaccination details are recorded in the vaccination centres via a web application provided by Bundesdruckerei; alternatively, an interface provided by Bundesdruckerei can be used to integrate the data into the software used in the respective vaccination centres. The pseudonymisation procedure used, in which Bundesdruckerei is not acting on behalf of the RKI in using this interface but on behalf of the vaccination centres, was in need of review so that a reliable separation of tasks could be ensured.

I recommend reviewing the methods and basic data for reporting vaccinations and vaccination rate monitoring.

Cross-references:

4.1.7 The "Epidemic Situation Continuation Act"

4.2 Artificial intelligence - Regulation as a task for society as a whole

Artificial intelligence (AI) is a key technology of digitalisation. Algorithm-based decision-making processes and learning systems are extending to all areas of life and promise solutions that would be almost unthinkable without AI. It is an essential social and political task to shape this technology in such a way that it puts people and their rights at the centre, while at the same time enabling innovative developments and broad use in many areas.

The innovation value resulting from applications of AI is undeniable. However, their increasingly widespread use does not only bring advantages. It can also lead to fundamental and profound violations of basic rights. For example, AI-based medical procedures help to detect cancers at an earlier stage. Voice and facial recognition software that identifies people based on their biometric characteristics can be used to fight crime and solve criminal offences. However, it can also be used repressively to monitor and control citizens.

At the same time, AI is changing the interaction between human beings and technology in the world of work. For example, assistance systems can relieve employees of strenuous or dangerous tasks and support them in complex processes and decisions. Despite these opportunities, AI must not find its way into the world of work at any price. This is because its application in the working environment, for example in job application procedures, is associated with a particularly high risk for the personal rights of applicants and employees. Specific legal regulations for the use of AI in this area are necessary, but are so far conspicuous by their absence. In the Advisory Council on Employee Data Protection (see No. 4.3), I have therefore argued for the use of AI in an employee context to be regulated by law in Germany.

AI can often be easily integrated into existing systems and applications. Such systems and applications often already contain information that can be analysed biometrically, such as photos, videos and voice recordings. With little effort, it can be supplemented by AI in such a way that biometric evaluations become possible. The use of AI, especially for biometric data analysis, must therefore be examined very carefully for its individual, but also overall effects on society. Especially in relation to the use of AI, it is important to recognise the importance of data protection in respecting freedom of association, freedom of opinion and expression and freedom of association.

So there is definitely a tension in many areas. Data protection can make an important contribution to balancing interests here: through aspects such as risk assessment, transparency, verifiability and intervenability, it helps to ensure that progress can be shaped in such a way that AI is simultaneously efficient, innovative, compliant with data protection and oriented towards the common good. Data protection is thus a decisive criterion for the success of AI applications.

AI can hardly be thought of in terms of national borders any more. Such globalised technology also requires increased international cooperation. In order to create an appropriate framework here and to influence the design process in the sense of positive development of technology in which the rights and interests of the individual are protected, I am actively involved in national and international committees that deal with AI development.

AI at the international level

Last year, the European Commission presented the world's first draft of a legal framework on AI. The comprehensive draft regulation aims to promote the development of AI, ensure a high level of protection for public interests and create a basis of trust for AI systems. In an opinion on the draft regulation, the European Data Protection Board (EDPB) has argued that the use of AI should be prohibited if the personal identity and dignity of human beings are not respected. As part of the EDPB's rapporteur team, I have strongly argued here for the primary importance of data protection in the design of AI (see No. 4.2.1). The EDPB will publish guidelines for the use of facial recognition technology by police and law enforcement agencies in 2022. Here, too, I am actively involved as one of the rapporteurs.

Furthermore, I am involved in the so-called "Working Group Artificial Intelligence" of the Global Privacy Assembly (GPA). This is a sub-working group of the International Data Protection Conference, which regularly discusses data protection policy and data protection AI issues and draws up resolutions and recommendations on them. Last year, a resolution was passed on the handling of AI, which sets out the fundamental requirements for its development and use that are necessary to meet the appropriate accountability obligations. I am currently working closely within this committee on a paper that deals with the risks to the rights and freedoms of the individual from AI systems. The aim here is to raise awareness of both the individual and the societal risks for data protection and ethics in connection with AI.

Further cooperation in the field of AI was agreed during the G7 Regulatory Cooperation Roundtable. In this context, the data protection supervisory authorities of the G7 member states met for the first time in September 2021

with the British Data Protection Commissioner Elizabeth Denham as chair (see No. 3.4.1). In a joint communiqué, the central importance of human dignity in the design of AI was emphasised. There was agreement that the essential principles of purpose limitation and data minimisation must apply and that AI must be transparent, understandable and explainable. On this basis, there was agreement to continue to promote the development of interoperable concepts for regulation across all legal systems and against the backdrop of a human-centred approach in a separate working group on AI.

Without automated, intelligent analysis and decision-making systems, the amount of data that accumulates in a digitalised world cannot be used efficiently. It is our task, together with politics, society, science and business, to put this use of AI-based systems on a sustainable footing. The aim is to create a framework that enables use of AI that is compatible with democratic principles, complies with the law and is oriented towards the common good.

Cross-references:

3.4.1 G7, 4.2.1 AI draft regulation, 4.3 Interdisciplinary Advisory Board on Employee Data Protection

4.2.1 AI draft regulation

In its opinion on the European Commission's draft regulation, the EDPB underlines the primary importance of data protection in the use of AI.

On the EDPB, and especially as part of the rapporteur team, I have actively campaigned for the use of AI to be banned if it does not respect the personal identity and dignity of human beings or if it poses high risks to the life and health of individuals. In addition, I have strongly supported the call for a general ban on the use of AI for automatic recognition of personal features in publicly accessible spaces. The use of AI must not impinge on the foundations of our social interaction.

With the draft legal framework on AI, the Commission is pursuing a risk-based approach, which is also welcomed in principle by the EDPB in its opinion. For high-risk applications, certain quality requirements are envisaged, e.g. logging and documentation requirements, extensive user information, high quality of data sets or even human supervision to minimise risks.

The EDPB welcomes these requirements, but sees a need for change in the proposals, which it makes clear in its opinion.

There is concern, for example, that international law enforcement cooperation does not fall within the scope

of the proposal. Among other things, the fact that the European Commission is to be given a superior position in the European Committee on Artificial Intelligence is also questioned. In our view, what is needed is a European body that is independent of political influence. To ensure the independence of the committee, it should be given more autonomy and be allowed to take initiatives itself.¹³

The fact that the European Commission has initiated the fundamental work on a regulatory framework as we move in this direction is an important step. However, a lot of work will be needed before the proposal will produce a well-functioning legal framework that will effectively complement existing rules on data protection, such as the General Data Protection Regulation, in protecting fundamental human rights while promoting AI innovation.

In the draft presented, the aspect of AI in the health sector is only mentioned marginally. Only the risks of using AI for health are often emphasised. Positive effects and opportunities arising from the use of AI in the health sector are to be regulated in a separate legal act on health data in the European area (see Recital 45). The presentation of a draft legal act on the European health data space was initially planned for autumn 2021, but was then postponed to spring 2022.

Fundamental questions arise that can only be answered meaningfully in a broad social dialogue. In addition, the interaction between the new AI regulation and existing law, in particular the General Data Protection Regulation, and questions regarding the arrangements for supervision and law enforcement must be clarified. I will continue to advocate this.

Cross-references:

3.4.1 G7, 4.3 Interdisciplinary Advisory Council on Employee Data Protection

4.2.2 AI consultation process

The use of artificial intelligence (AI) must always be measured against the yardstick of constitutional law. The consultation process on the use of AI in law enforcement and security is intended to involve the public in forming an opinion.

In the area of law enforcement and security, the use of AI is being researched, tested and partly put into practice. The data protection and constitutional requirements have not yet been clarified. They must therefore be consolidated. The use of AI can have a significant impact on the work of security agencies and freedoms for data subjects. A broad public debate is therefore necessary. I have thus launched a consultation process

¹³ The opinion is available at https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_de

on the use of AI in law enforcement and security. I have put forward the following theses for discussion:

- AI requires detailed empirical stocktaking and a comprehensive socio-political discussion in order, on the one hand, to clarify the impact of this technology on citizens' freedoms and, on the other hand, to determine the necessity of its use for law enforcement and security purposes. All the risks must be set against the benefits. Possible discrimination and supra-individual consequences, both for specific groups of people and for democratic processes and the rule of law as a whole, must be effectively excluded. Legislation should include all currently existing powers of law enforcement and security authorities in an overall account ("overall surveillance account").
- The use of AI cannot be based on general police legislation. Rather, the use of AI fundamentally requires specific legal regulation.
- Compliance with the general data protection principles is an indispensable prerequisite for the permissible use of AI under data protection law.

The use of AI must not diminish the effective exercise of data subjects' rights.

- AI must be explicable. The quality of the data sets already used for training purposes must be ensured.
- The core area of private life and the guarantee of human dignity must not be affected by the use of AI.
- AI must be subject to comprehensive control by data protection supervisory authorities.
- The use of AI must be preceded by a comprehensive data protection impact assessment.

After evaluating the comments received, I will report on the results.

4.3 Interdisciplinary Advisory Council on Employee Data Protection

An employee data protection law is urgently needed!

Already in my last Activity Report (see 29th AR, No. 2.3; 7.2), I recommended making prompt use of the option granted by the GDPR to enact national regulations on employee data protection. For many years, the federal and state data protection supervisory authorities have been calling for an employee data protection act. Today, this is all the more urgent: the rapid progress of digitalisation in companies and administrations is leading to profound changes in the world of work. Data-driven

processes now characterise the everyday work of many employees. Data sets that are being created in companies and administrations are increasing in number and becoming ever more detailed. Combined with the new possibilities of data linking and evaluation, this offers opportunities for a more efficient organisation of work. On the other hand, employees are simultaneously exposed to the risk of losing their privacy, even to the point of total surveillance.

The Interdisciplinary Advisory Board on Employee Data Protection set up by the Federal Ministry of Labour and Social Affairs in summer 2020 (see 29th AR, No. 7.2), of which I am also a member, is examining, among other things, the extent to which regulations are necessary to protect the rights of employees in the digital world of work. The abridged version of the Advisory Board's report was submitted to the Federal Minister of Labour and Social Affairs in January 2022.

As part of my Advisory Board activities, I have argued for the creation of employment data protection regulations. In many situations, the current version of Section 26 BDSG is not sufficient to ensure effective, legally secure protection against intrusive data processing in the digitalised world of work because it requires interpretation. The use of artificial intelligence in application procedures, employee screening and GPS tracking are just a few exemplary aspects of the challenges in the digitalisation of the world of work. They make the regulatory loopholes visible and better protection of workers more important than ever. Legal certainty for all parties involved is essential. An employee data protection act is needed that regulates specific data processing in the employee context and key points in the employment relationship. These include, for example, a ban on total surveillance, limits on behavioural and performance monitoring, information about prohibiting use as evidence and the deployment of new technologies, in particular algorithmic systems. In addition to strong data protection supervision, instruments of individual protection are also important, e.g. with regard to the enforcement of data subjects' rights as well as collective protection.

I welcome the fact that the Coalition Agreement 2021 contains a commitment to the creation of regulations on employee data protection in order to achieve legal clarity for both employers and employees and to protect personal rights effectively, and I very much hope that this opportunity will finally be seized in the 20th legislative term.

5 Legislation

5.1 Telecommunications legislation on TKG/TTDSG

After a long wait, the Telecommunications Modernisation Act has been in place since December 2021. At the same time, other laws in the telecommunications sector are being adapted to European law.

In my last Activity Report (No. 5.10) I was able to report on a first draft law.

The new Telecommunications Act (TKG) was revised as part of the Telecommunications Modernisation Act (TKMoG) and came into force on 1 December 2021 at the same time as the Telecommunications Telemedia Data Protection Act (TTDSG). In this context, the previous data protection provisions have been omitted from the new TKG and transferred to the TTDSG. The amendment also serves to implement Directive (EU) 2018/1972 on the European Electronic Communications Code.

The term telecommunication service is significantly expanded here and now also includes messenger services, email services and video conferencing services. Since 1 December 2021, the BfDI has in principle had uniform responsibility at national level both for breaches of the General Data Protection Regulation (GDPR) and for breaches of the protection of traffic data (see in detail Sections 29, 30 TTDSG).

Until now, the term telecommunications service was defined in Section 3 No. 24 TKG (old version) as “services usually provided for remuneration which consist wholly or mainly in the transmission of signals via telecommunications networks, including transmission services in broadcasting networks” (the so-called technical approach). Both legislation at the European level and German legislation have now taken a functional approach, as it makes no difference from the perspective of end users whether they

are using, for example, text messaging or a messenger service. The new definition can be found in Section 3 No. 61 TKG: “Telecommunications services [are] services

normally provided for remuneration over telecommunications networks which, with the exception of services providing or exercising editorial control over content via telecommunications networks and services, include the following services.

- internet access services, (Section 3 No. 23 TKG)
- interpersonal telecommunications services (within the meaning of Section 3 No. 24 TKG)
- services consisting predominantly in the transmission of signals such as transmission services used for machine-to-machine communications and for broadcasting;”

In particular, the concept of interpersonal telecommunications services will therefore define both internet telephony and so-called over-the-top services, such as messenger services and group chats, web-based email services and video conferencing services as telecommunications services in the future.

In the course of departmental coordination on the TKMoG, I pointed out the data protection shortcomings of the draft law in numerous statements. Some far-reaching attempts by telecommunication providers to collect and forward personal data to security agencies were prevented as a result. Nevertheless, the law still contains numerous regulations that need to be critically assessed, two of which I would like to highlight by way of example.

Section 172(3) TKG stipulates that number-independent services must store the identifier of the service, the name, the address, the date of birth and the date of allocation of the identifier, insofar as they collect this data. Originally, the plan was to make the collection of even more data mandatory. However, a general obligation to collect identification data, as provided for in Section 111(1) TKG (old version), would have counteracted the fundamentally anonymous usability of the services in question. Despite the intended security purpose, a collection obligation of this sort appeared disproportionate and I rejected it. I have argued for a standard compa-

rable to the previous regulation under Section 111(2) TKG (old version) which applies to electronic mail. This provides for a storage obligation for individual items of data collected, but no additional collection obligation. Nevertheless, the obligation to store the date of birth, for example, has introduced an additional piece of data that at least limits the anonymous usability of the services. Especially for certain professional groups, such as lawyers and journalists, anonymous usability of modern means of communication such as email and messenger services is an important part of their daily work. The extension of the statutory provision in Section 172(3) TKG does not follow - as one might think - from the Code for Electronic Communications, which was transposed into national law with the amendment to the Act, but results solely from a desire to amend German law. I see this critically from another point of view: the adoption of and adaptation to terminology such as that provided for in Directive (EU) 2018/172 or otherwise envisaged in relation to the other parts of the TKG is not automatic. These terms essentially serve other objectives, such as market regulation, frequency policy, end-user protection, the institutional structure or a basic provision of telecommunications services. This is to be distinguished from the expansion of the powers of the security agencies, e.g. with regard to the right of access to data within the framework of the information procedures according to Section 173 and Section 174 TKG, for example by expanding the circle of obligated telecommunications providers.

This does not follow automatically from changes in market regulation or to ensure a basic supply. Extensions of powers must be justified in detail during the legislative process. For this purpose, relevant facts and sources of knowledge must be presented (see Section 43(1) Nos. 1 and 2 of the Joint Rules of Procedure of the Federal Ministries). However, this did not happen in the case of the new TKG.

As another example, I would like to point to the provision of Section 170(11) TKG (new version): this requires providers of electronic communications services to ensure that encryption initiated by another European provider is lifted for its users. The encrypted calls would thus be recorded. First of all, it should be noted that under no circumstances may the requirement under Section 8(3) TKÜV be exceeded. If an encrypted call has to be routed out unencrypted, this automatically means a weakening of the encryption. This causes a deterioration in data security. Encryption is the basis for protecting the privacy of every individual and almost every economic activity in the digital world. In order to strengthen the secrecy of correspondence, post and telecommunications and the fundamental right to gua-

rantee the confidentiality and integrity of information technology systems, it must be possible to protect data effectively from access by unauthorised persons. The use of cryptography is a fundamental instrument here. I am critical of any attempt to reduce the level of protection, especially the level of encryption. In addition, it is to be expected that the agreements to be reached between the companies will in turn lead to foreign companies also demanding that they be allowed to monitor the calls of German citizens when they are abroad.

The “Telecommunications Telemedia Data Protection Act” (TTDSG) also came into force on 1 December 2021. This contains the data protection regulations previously found in the TKG, together with regulations on telemedia from the Telemedia Act (TMG). It is gratifying that the legislation has been adapted to include my demands in relation to cookies. The new Section 25 TTDSG finally implements the ePrivacy Directive correctly, as the requirement of consent is standardised in the law as the norm. More clarity has also been created with regard to my responsibilities. Unfortunately, there are also some shortcomings in the law. This happens when a legislative procedure is initiated at the last minute before the end of the legislative period. For example, some terms such as “participant” and “user” are not used consistently, and some cross-references in the law are incorrect. I have pointed out these errors several times in my statements to the lead ministry and parliament - in some cases, unfortunately, in vain. A rectification process therefore had to follow shortly after promulgation of the law.

“Recognised consent management services” are a new addition. They should enable internet users to manage their consent, e.g. for cookies, in a user-friendly way. The TTDSG sets only a very rough framework for this. The details still have to be set out in a legal ordinance. Only then will it become clear whether this can make a contribution to stopping the flood of “cookie banners”.

5.2 Lobby Register Act

The Lobby Register Act is intended to bring more transparency to the representation of interests in the Bundestag and government from 2022.

The Act on the Introduction of a Lobby Register for the Representation of Interests vis-à-vis the German Bundestag and vis-à-vis the Federal Government of 16 April 2021 (Lobby Register Act - LobbyRG) comes into force on 1 January 2022. Contrary to initial drafts, the law applies not only to representation of interests vis-à-vis the German Bundestag, but also vis-à-vis the federal government.

The law represents a step forward for freedom of information. The previous transparency regulations of the

German Bundestag only referred to interest groups and did not establish binding regulations. The regulations on access to information at the federal level, such as the Freedom of Information Act (IFG) and the Environmental Information Act (UIG), have so far also left out the basic parliamentary area. In addition to a registration obligation for an extended group of interest representatives, the new law now establishes binding principles for representing interests with integrity.

The 37th Conference of Freedom of Information Officers in Germany had adopted a resolution on the establishment of mandatory lobby registers on 12 June 2019 with my participation. This fundamental requirement has now been fulfilled by the law. I am following with interest attempts to introduce more far-reaching regulations.

5.3 Open Data Act

With the passing of the 2nd Open Data Act, the scope of application of the open data regulations of the E-Government Act was expanded with regard both to the bodies obliged to publish data and the data to be published.

Changes in the provision of open data

The aim of the regulations of the Act to Amend the E-Government Act and to Introduce the Act for the Use of Public Sector Data (so-called “2nd Open Data Act”) is to expand the scope of open data provided by the federal administration. The scope of application of Section 12a of the E-Government Act (EGovG) was therefore extended to all federal authorities with the exception of self-governing bodies. In principle, the federal authorities are obliged to provide unprocessed machine-readable data that they have collected for the fulfilment of their roles under public law in machine-readable form. Another innovation is the obligation of federal authorities to create a body that coordinates the identification and provision of open data internally. At last, research data are now also covered by the obligation to make data available.

Section 12a EGovG continues to provide for extensive exemptions to these regulations, however. For example, there is no obligation for main customs offices or comparable local federal authorities or the secret services to set up a coordinating body. In addition, designated agencies are not covered by the obligation to provide data.

To my regret, the exemptions in Section 12a EGovG concerning data that do not have to be made available have been extended even further. As a result, the exemptions represent a reasonable compromise between the interest in making open data available as widely as possible and the protection of, in particular, personal or personally

identifiable data. It remains to be seen whether the new regulations will come to life so that there is an active and broad provision of open data. The evaluation provided for in the law should be taken as an opportunity to obtain a clear overview of the implementation of the law. In particular, the introduction of sanction options should be examined in order to emphasise the obligation to provide data and the right to the provision of data should be regulated by law.

The Act also enacted the revised version of Directive (EU) 2019/1024 (PSI Directive). The Information Reuse Act (IWG) was replaced by the Data Usage Act (DNG). The DNG also applies to the federal states and municipalities and to certain companies providing public services. It regulates the further use of public data provided on the basis of other legal regulations.

5.3.1 Open Data Strategy of the federal government

With its Open Data Strategy, the federal government has for the first time defined guidelines for proactive provision of administrative data. Apart from the initiative itself, the explicit commitment to data protection is positive.

The federal government's Open Data Strategy is intended to create the framework for improving the “open data ecosystem” at federal level. The provision of open data is described as an important element in open governance, which is likely to strengthen trust in political institutions. The data stock of the federal authorities should be opened up further and made available for use free of charge, and the scope and quality of the data provided should also be increased. Finally, the Open Data Strategy also aims to promote the provision of open data by business, science and civil society.

The Open Data Strategy formulates six guidelines to shape measures for the provision and use of open data. Among other things, emphasis is placed on realising the economic potential of open data, improving data literacy in government, making open data available and using data responsibly and for the common good while respecting data protection and data sovereignty.

Three highlighted areas show examples of possible applications. Data-driven economic growth includes, for example, the development of apps and other data-based and user-related solutions. The Open Data Strategy anticipates great potential for economic growth and job creation here. The use of open data is also an opportunity for civil society and environmental initiatives to find technical solutions to concerns that have not yet been addressed. Last but not least, efficiency gains in administration are to be expected. Sharing data reduces the work involved in carrying out searches and eliminates

the need for data to be collected more than once. The development of digital administrative services could also have a beneficial effect on the tax burden on citizens.

Finally, specific measures are listed, which are assigned to three fields of action. Some of these measures have already been implemented (including amendments to Section 12a of the E-Government Act, see No. 5.2.) or are currently being implemented (e.g. the establishment of the Competence Centre for Open Data (CCOD) in the Federal Office of Administration).

I welcome the plans and initiatives of the Open Data Strategy and hope that the concept of “open by default” will become a matter of course for more and more public authorities.

I am pleased that the aspect of data protection has been explicitly included in the guidelines. Data protection and open data are not mutually exclusive, but complement each other. A faulty understanding of data protection should not tempt us to restrict the provision of open data as a precaution. Data protection is not an excuse for lack of openness.

An expansion of the provision of open data, in particular via technical interfaces (API), should be promoted further. As envisaged in the Open Data Strategy, interaction with social initiatives that have already shown what results can be achieved by simple means could also yield useful suggestions here.

5.4 Amendments to the Central Register of Foreigners Act

With the Act on the Further Development of the Central Register of Foreigners, the Central Register of Foreigners (AZR) is to be expanded to become the central filing system for foreigners. The data for specialised procedures under aliens law should be kept up-to-date, synchronised and made available digitally to the authorities involved. Duplicate data storage should thus be avoided in the future.

Storage of documents in full text

With the Act on the Further Development of the Central Register of Foreigners, it will be possible in future to store documents as full text versions in the Central Register of Foreigners, including decisions under asylum and residence law and foreign identity papers. However, storage may only take place insofar as no special statutory processing regulations or legitimate overriding interests of the foreign person conflict with this. As part of my participation in the legislative process, I have expressed my criticism of full-text storage without corresponding

technical and organisational security measures (see my statement to the Interior Committee of the German Bundestag of 30 April 2021, www.bfdi.bund.de/stellungnahmen). Arrangements could have been made for access authorisation and restrictions on access to the full text. In response to my criticism, the preferred solution was to make information relating to the core area of personal life unidentifiable in the documents. It will involve a lot of work for me to check whether the relevant redactions are made in an appropriate manner.

Storage of foreign personal identity numbers

Despite my criticism, the storage of foreign personal identity numbers has been included in the law. These are personal ID numbers that remain with you throughout your life and are issued in many states. In my opinion, the need to store this data in the AZR has not been convincingly justified. In the course of the legislative process, it was at least clarified that the foreign personal ID number transmitted by the registration authority may be used only for the purpose of unique identification of an individual.

I am pleased that some of my suggestions have been included and the bill has been amended. I will take a look at how this is implemented in practice by the federal authorities in future inspections.

5.5 Federal Police Act

The Federal Police Act (BPolG) has still not been adapted to the mandatory requirements of European law in the form of the JHA Directive. A draft by the then government factions in the German Bundestag, which would at best have taken European law into account only in part, but at the same time would have created constitutionally problematic new powers of intervention for the Federal Police, failed in the Bundesrat.

In my 29th Activity Report, I already reported that the mandatory requirements under European law had not yet been implemented in the BPolG, although this should have been done by 6 May 2018 (see 29th AR No. 6.7). The then government fractions subsequently introduced their own draft amendment in the Bundestag last year. There was no formal departmental consultation in the federal government, in which I would have been involved, for this parliamentary initiative, which was based on formulation guidance from the federal government. I was therefore able to raise my data protection concerns with the Committee on the Interior and Home Affairs only at a late stage in the hearing of the draft bill.

I made it clear to the committee that I consider the extension of the powers of the Federal Police to be con-

stitutionally questionable because the Federal Police is a special police force with a limited range of responsibilities for railway stations, airports and national borders; otherwise, the responsibility lies with the federal states. I also consider the proposed authorisation of preventive surveillance of telecommunications in the draft and, above all, the possibility of so-called “source telecommunications surveillance” to be highly problematic. For the latter, security loopholes left open deliberately would have to be exploited, which would lower the security level for digital communication as a result.

Moreover, the European legal requirements on the supervisory powers of the data protection authorities were only partially implemented in the draft. This would have imposed unnecessary hurdles for me to exercise my data protection control.

Since the draft ultimately failed in the Bundesrat because of the votes of the federal states, it remains to be seen how the BPolG will be revised in the new legislative period.

5.6 Amendments to the BND Act come into force

In the course of the parliamentary consultation process, the coalition fractions ultimately made only marginal changes to the federal government’s original proposals for implementing constitutional court requirements in the BND Act.

The law, which largely comes into force on 1 January 2022, will thus at best bring structural adjustments to the landscape of control over the Federal Intelligence Service (BND).

On 25 March 2021, the Bundestag passed legislative amendments to the existing BND Act with the aim of implementing the requirements of the Federal Constitutional Court of 19 May 2020 (Case No. 1 BvR 2835/17) and the Federal Administrative Court of 13 December 2017 (Case No. BVerwG 6 A 6.16 and 6 A 7.16). The Bundesrat approved the law on 26 March 2021.

The first regulations, in particular regarding the Independent Control Council, have already come into force on 22 April 2021. The other provisions come into force on 1 January 2022.

The amendment proposal of the CDU/CSU and SPD parliamentary groups, which was presented after the expert hearing in the Committee on the Interior, resulted in only a few substantive amendments to the BND Act. The slight increase in the intervention thresholds for the targeted collection of data from confidential relationships

in the context of strategic foreign telecommunications reconnaissance and intervention in information technology systems should be emphasised. It is now possible to intervene in confidential relationships if the facts give rise to legitimate suspicions of certain criminal offences or dangers. An obligation to document confirmation of the fact that individuals belong to the protected group in relationships of confidentiality relationships was also stipulated. According to the BND Act, this group includes the clergy, defence lawyers, other lawyers and journalists whose confidential relationship would fall under the protection of Section 53(1) sentence 1, nos. 1, 2, 3 and 5 and sentence 2 of the Code of Criminal Procedure.

Otherwise, only structural adjustments were made to the landscape of control over the Federal Intelligence Service. The amendment placed the Parliamentary Control Committee at the centre of various information flows between the control bodies. There was no provision for content-based interaction between the G10 Commission, the Independent Control Council and my authority, which I advocated.

Despite some adjustments, the criticism I voiced in the course of the BND legislative process remains largely valid. In this connection, I refer to my public statement to the Committee on the Interior and Home Affairs of the German Bundestag on the Federal Government’s draft bill to amend the BND Act of 18 December 2020, see www.bfdi.bund.de/stellungnahmen

5.7 Evaluation of the BDSG

The DSK’s statement on the evaluation of the Federal Data Protection Act (BDSG) carried out by the Federal Ministry of the Interior (BMI) revealed a need for legislative action in certain areas. This applies, for example, to the regulation on employee data protection and the enforcement powers of the BfDI in relation both to the GDPR and the JHA Directive, and vis-à-vis the intelligence services.

In the reporting period, the Federal Ministry of the Interior carried out an evaluation of the Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and the Implementation of Directive (EU) 2016/680 (Data Protection Adaptation and Implementation Act EU - DSAnpUG-EU2) in accordance with the mandate in the explanatory memorandum to the act. The core of this law is the new BDSG, which has been adapted to the European legal requirements under the GDPR and the JHA Directive.

The main data protection regulations in the scope of application of the GDPR result directly and uniformly throughout the EU from this regulation. However, the

BDSG contains clarifications and modifications based on the opening clauses of the GDPR. In the area of the police and justice, the BDSG serves to implement the corresponding directive (JHA Directive). Here, too, the essential substantive regulations result from the basis in European law, although this only provides for minimum harmonisation.

The German supervisory authorities were involved by the BMI as part of the evaluation of the BDSG and have issued a comprehensive statement¹⁴. Some key points of the DSK statement are:

- With regard to the legal basis for processing and further processing of personal data and the provision of Section 29 BDSG on the rights of the data subject and supervisory authority powers in the case of secrecy obligations, the BDSG is shown to be partly in breach of EU law (Section 4(1) sentence 1 no. 3, Section 23(1) no. 2 and Section 29(3) sentence 1 BDSG) and in large parts to be unclear and too vague.
- Section 26 of the BDSG in its current version does not fulfil its role of employee data protection. In practice, the wide scope for interpretation leads to ambiguities for all parties involved. In order to meet the special challenges of safeguarding the fundamental data protection rights of employees, these would have to be regulated more clearly (see 4.3 above).
- The increase of the threshold in Section 38(1) BDSG for the appointment of data protection officers to 20 employees has neither reduced bureaucracy nor otherwise eased the burden on companies and associations. In fact, the effect has been the opposite (see 28th AR No. 5.1).
- As a result of the restrictions on the rights of data subjects in Section 32 to 37, the BDSG does not meet the requirements of European law and calls existing data protection standards into question. The rights of data subjects (information, disclosure, erasure, objection, automated individual decision-making/profiling) are restricted to an unacceptable extent.
- It is urgently necessary to expand the powers of the supervisory authorities under the BDSG by enabling the enforcement of measures by coercive means and ordering of immediate enforcement against public bodies.
- The BfDI also remains limited to the instruments of warnings and complaints in the area of the JHA Directive and outside the scope of EU law, at least insofar as more far-reaching powers are not regulated by specific provisions of police law. Art. 47(2) of the JHA

Directive, on the other hand, contains the obligation to grant effective remedial powers. The regulation in the BDSG does not fulfil this requirement. The still incomplete implementation in specialist law clearly shows that effective remedial powers for the JHA area should be regulated consistently in the BDSG. For the reasons mentioned above, I have been calling for remedial powers and sanctions comparable to those of the GDPR and the JHA Directive for some time now (see 27th AR No. 1.2.1).

In a supplementary opinion, I also advocated clarifying in the legal text of Section 18 BDSG that a common position of the German supervisory authorities in European matters is already required in the cooperation procedure (Art. 60 ff GDPR) and not only in the consistency mechanism (Art. 63 ff). The German supervisory authorities should always speak with one voice at the European level in order to accelerate European opinion-forming processes and better represent German positions there. This is seen differently by some of the supervisory authorities of the federal states.

The BMI published its report on the evaluation of the BDSG in October 2021.¹⁵ The comments of the German supervisory authorities are mentioned extensively, but unfortunately only some are included in the conclusions. In the current legislative period, I will continue to advocate the changes to the BDSG outlined above.

I recommend that the federal government address institutionalisation of the DSK and improve the mandatory cooperation between the German data protection supervisory authorities announced in the coalition agreement by taking the corresponding legislative measures as soon as possible.

5.8 IT Security Act

The IT Security Act 2.0 introduced many new roles and powers for the Federal Office for Information Security (BSI).

Through a series of dialogues, the BSI and my organisation are working together on their implementation in a way that complies with data protection requirements.

On 27 May 2021, the “Second Act to Enhance the Security of Information Technology Systems” - or IT Security Act 2.0 for short - was published in the Federal Law Gazette. It was preceded by a lengthy legislative process of about two years, which was nevertheless characterised by unreasonably short periods for comments.

¹⁴ Opinion of the DSK on the evaluation of the BDSG of 02.03.21, available at <https://www.datenschutzkonferenz-online.de/stellungnahmen.html>

¹⁵ Available at <https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf>

Many of my suggestions were taken up and implemented in the legislative process. However, some important requests were unfortunately not adopted: for example, my clear plea against an extension of the storage of so-called log data from 3 to 12 months was not only rejected, but even extended to 18 months. In my view, this raises very significant questions of proportionality.

For the BSI, the IT Security Act leads to a considerable increase in responsibility and work.¹⁶ In the same way, the additional workload of my office in advising and monitoring the BSI in relation to data protection law is also increasing.

It was important to me to support the BSI proactively in the implementation of the new requirements of the IT Security Act 2.0 from the very beginning. In line with the principle of “data protection from the outset”, we initiated a very successful joint dialogue process in order to make all the new processes and systems of the BSI data protection-compliant during their development and to operationalise the cooperation between the two institutions in the best possible way.

5.9 EU digital legislation

With its proposed regulations on the European single market for data, the EU Commission has presented further steps towards an EU-wide regulatory framework for digital space. The BfDI supports the negotiations on the individual legal acts both nationally within the framework of departmental consultations and through initiatives of the European Data Protection Board (EDPB).

Building on its data strategy published at the end of 2020 (COM/2020/66 final), the EU Commission presented several proposals for regulations in the reporting period that are intended to form a “single legal framework for data access and responsible data use” in the EU. In essence, these are two legal acts with the aim of regulating existing big data platforms and legal acts to promote data access and exchange. The Digital Services legislative package, comprising the Digital Services Act (DSA) and the Digital Markets Act (DMA), sets out basic rules for digital services aimed at creating a safe, predictable and trustworthy online environment and fair markets for these services in the EU. The Data Governance Act (DGA) aims to increase the availability of public sector data for research and business in the EU, to establish so-called data intermediaries and to promote mechanisms for data use for the common public good.

The DGA is to be supplemented by the draft of the so-called Data Act (DA) at the end of 2021. The EU Commis-

on published an Inception Impact Assessment for this planned legislation in May 2021¹⁷. From this it can be seen that concrete access rights to data, including personal data, could possibly be created in order to promote so-called data markets. It is clear that for both the DGA and the DA the focus of the EU legislation is on improved framework conditions for digital business models and forms of processing, and at the same time on data analysis through so-called artificial intelligence (AI). Both forms of processing, however, pose considerable challenges to the previous concept of data protection. It is therefore all the more important to keep a careful eye on these so-called

data markets with regard to the risks in the form of mass exchange of data, including personal data, and their use, especially for purely commercial purposes.

The EU Commission regards the GDPR, which has been in force since 2018, as a first step on the way to ensuring a “solid framework for trust in the digital environment”. It will not be affected by the new legal acts. However, there are many ambiguities in relation to the GDPR and the impacts on it. The legal acts have further interfaces that will have a very significant impact on data protection in the EU as a whole. The aim of my advice is to point out these problematic points and to work towards regulation that is as data protection-friendly as possible. It is important to keep in mind whether and to what extent these new, far-reaching EU legal acts could also give rise to a need for further legal regulation to protect citizens’ data protection rights.

DGA

The DGA pursues the creation of framework conditions for a so-called data economy in three distinct areas of action.

Firstly, conditions are created for the dissemination of data by public bodies for general use (open data). In the future, public authorities should also release personal data for commercial use, for example, and the concept of open data will thus be expanded considerably.

However, the creation of the legal bases for permissible transfers is to be left to the Member States, and the GDPR as a whole is to remain unaffected.

Secondly, data sharing services, so-called data intermediaries or data brokers, are defined. These services should bring data providers and data users together under neutral mediation. In the area of so-called PIMS (Personal Information Management Systems), i.e. service providers that support citizens in exercising their data protection rights, potential for further development

¹⁶ The main content of the law can be found at https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

¹⁷ See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-data-bases_en

of data protection is evident in this context. Overall, the conditions under which such data intermediaries may be operated and for which purposes are points that remain largely open in the discussion. Only when there is more detail will concrete evaluation be possible. The risks of the development of a trade in personal data via data intermediaries which is inadmissible according to data protection principles must be countered.

Thirdly, a framework is established to encourage Member States to create organisations that facilitate so-called data altruism. The trust in such organisations should be strengthened in such a way that citizens voluntarily contribute their personal data for public welfare purposes, such as research. Here, too, it is important to ensure that data protection principles are upheld in the legal design. In all regulatory approaches, the problem arises that a separate supervisory structure is to be created alongside the data protection supervisory authority, even though their responsibilities will overlap.

Together with my European colleagues and the European Data Protection Supervisor (EDPS) on the EDPB, I have drafted a comprehensive opinion on this and other critical points¹⁸.

DSA

The DSA redefines what rights and obligations content providers have on the internet. It sets out due diligence requirements on content restrictions and illegal content and creates transparency for consumers with regard to online purchasing, advertising and recommendation systems. I would have liked to see a bolder approach, especially with regard to personalised advertising, and I support a ban on certain tracking and profiling practices. Since data protection questions often have to be answered when implementing the DSA, e.g. in the context of the proposed access of researchers to data from large online platforms, it is imperative to involve the data protection supervisory authorities at both national and European level.

DMA

The DMA has as its general objective fairness and contestability under competition law in the digital sector and is specifically directed at the regulation of the large central platform services. It is intended to supplement competition law, which in principle only applies after an infringement of rights, in taking action against the large providers of central platform services by ex ante regulation. If a central platform service meets the criteria set by the DMA for classification as a so-called gatekeeper, additional conduct obligations are imposed on it by the

DMA in order to prevent unfair practices. These conduct obligations also contain data protection-related requirements, such as the prohibition on merging personal data with those from third-party services or several central platforms operated by a company if no effective consent under the GDPR has been given. For efficient and effective enforcement of the regulations on the gatekeepers, it is an indispensable prerequisite that appropriate provisions are made in the DMA for cooperation between the enforcement authority and the data protection supervisory authorities. In doing so, I advocate that EDPB and EDPS also be included in this cooperation. Furthermore, as part of my advice, I ensure that the level of protection of the GDPR is maintained in the DMA where it makes reference to data protection obligations.

Conclusion

Against the background of the present drafts on the DGA, DMA and DSA and the course of the negotiations of the Member States and the European Parliament on these legislative acts so far, I, as co-rapporteur, supported the initiative of my Dutch colleague to identify and collate the general points of criticism concerning all three legislative acts in the joint opinion of the EDPB of 18 November 2021¹⁹.

5.10 Developments in health registers

When legal regulations are put into practice, the devil is often in the detail. In the case of the organ donor register, the detail relates to authentication. And with the implant register, it was not easy to reconcile the operating regulation and provision of the necessary server capacities with the legal requirements. At the Centre for Cancer Registry Data, use of the data set, which has been expanded significantly, also includes commercial research. In the case of a request for data use, the new scientific committee has to assess, among other things, the re-identification risk.

Organ and Tissue Donor Register (OGR)

Last year, I had already advised the Federal Institute for Drugs and Medical Devices (BfArM) on the technical implementation of the regulations relating to the online register for documenting the declaration on organ donation (29th AR, No. 7.3). The register is scheduled to start operation in March 2022. In the reporting period, a large number of other individual questions arose, with which Bundesdruckerei approached me as a processor for the BfArM.

¹⁸ Opinion 03/2021, available at https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en

¹⁹ Statement on the Digital Services Package and Data Strategy, available at: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-digital-services-package-and-data-strategy_en

The law stipulates that the declaration can be made at passport and identity card offices, such as municipal citizens' services offices. Terminals set up there are designed to meet this need. In practice, however, this appeared to be too time-consuming. As a result, the person making the declaration will soon only be able to authenticate themselves there. They will then receive a number under which they can log in to the register portal and make the actual declaration. I consider this to be permissible under data protection law because authentication as part of the originally intended declaration submission has a legal basis ("minus"). On the other hand, I did not consider authentication by means of ALVi, the alternative personal insurance ID (which does not require the use of the electronic health card), to be permissible. This procedure has only a narrowly limited scope of application. It is used only for the electronic patient file, electronic medication plan and electronic patient summary file applications. For "card-free" authentication of insured persons on the organ donor register, only use of the so-called digital identity according to Section 291(8) SGB V can be considered, which will be available from 2023. In addition, authentication by means of the online function of the identity card is possible.

The data set in the organ donor register is intended to map the information on the organ donor card in card format.

Since I was informed that pre-existing conditions are often entered in the free text field of the ID card, another problem was the need to protect this data. Previously, OGR data had not been considered as particularly sensitive data. In order to prevent the entry of such health data from raising the protection category and thus creating more technical work, I have recommended getting rid of the field completely or offering commonly used entries with no health information for selection instead of the free text field.

Implant register

For the implant register, I was primarily concerned with the hosting service providers for the register and the trust office. The institutions entrusted with hosting provide server capacity and handle the data processing. The BMG had commissioned Bundesdruckerei's D-Trust GmbH with the hosting for the register office located in the BMG. The Robert Koch Institute (RKI) was still looking for a host for its trust office that could be connected to the telematics infrastructure (TI) used for transmission. The law stipulates that the trust office must be separate from the register office. This therefore requires different bodies to provide the hosting. However, there are few providers with sufficient free server capacity to meet the strict security requirements that arise here

from the protection category and the enormous amount of data. I was therefore asked several times if it would be possible to cut back on the requirements in order not to jeopardise the scheduled start of the register. Also under discussion was the possibility of the trust office being hosted by Bundesdruckerei GmbH, the parent company of D-Trust GmbH, which was already hosting the register. I could only warn against this: with such a large register, compliance with data protection requirements is an indispensable basis for maintaining the trust of data subjects. Fortunately, a solution was ultimately found that allowed the contracts to be awarded in a data protection-compliant manner.

Another topic of the consultation was the data flows between those involved. Initial flowcharts did not comply with the requirements of the Implant Register Act. Even before these consultations were concluded, I was surprised to receive the draft of the Implant Register Operating Regulation, which contained some points that were still the subject of discussion. Among other things, I was able to prevent direct data exchange between the register and the hospital by using a record identifier. The data set identifier is classified as personal data, so that transmission is only permissible with the involvement of the trust office. Finally, the planned data retrieval procedure gave rise to criticism among the health insurance providers. The law stipulates that the health insurance funds should communicate changes relating to the people they insure (change of health insurance provider, death, etc.). According to the draft regulation, however, the register is required to check the information with all health insurance funds on a regular basis. Here I was able to reach a position where notification by the health insurance providers is the norm and retrieval initiated by the register office remains limited to special cases. The register office is still located in the BMG, although this is not a suitable register authority, as is also evident from the explanatory memorandum to the law. This is unproblematic only until the actual operation of the register starts.

I will monitor the situation and have urgently recommended that the BMG establish a suitable authority that can take over permanent operation of the register in a legally secure and data protection-compliant manner.

Centre for Cancer Register Data

I had already reported on plans to expand the data set held at the Centre for Cancer Register Data (ZfKD) in the RKI (29th AR No. 7.3 p. 69). What was critical for me was the large circle of those entitled to use the data, since private individuals, including companies in the pharmaceutical industry, are also granted access on request. In the departmental vote, however, I was able to argue

successfully in favour of involving a scientific committee in the decision on each application, in addition to the advisory board. Since this committee examines the re-identification risk, among other things, it is also to include data protection experts.

Further regulations were based on those for the Research Data Centre at the BfArM in Section 303e SGB V: anonymised data are transmitted for the most part, access to pseudonymised data sets is only permitted under the control of the Centre for Cancer Register Data, misconduct is sanctioned and approved applications are published in a directory. The law came into force at the end of August (Act on the Consolidation of Cancer Register Data of 18 August 2021, BGBl. I, p. 3890). I will keep an eye on the way applications are processed to ensure that, despite the right of access for commercial research, the protection of data subjects is maintained.

I recommend that the BMG provide for - and, if necessary, create - a suitable authority for the operation of the implant register, which can take over registration operations in the long term in a legally secure and data protection-compliant manner without conflicts of interest.

5.11 Data collection powers of the health insurance providers in sickness benefit case management

The Act on the Further Development of Health Care (GVWG) clarified that there are limits to the health insurance providers' data collection powers when considering whether to commission an expert opinion from the Medical Service (MD). My legal opinion, which I have held for years, was thus confirmed.

In my 29th AR (No. 7.15), I had reported that in discussions with the National Association of Statutory Health Insurance Funds and the Federal Ministry of Health (BMG), it was still not possible to reach a consensus on the scope of the data collection powers of health insurance providers before commissioning the MD to assess incapacity for work. Now, with an amendment to Section 275 SGB V in the GVWG, which came into force on 20 July 2021, the legislation confirms my restrictive legal view on the data collection powers of the health insurance funds, which I have held for years.

The newly inserted paragraph 1b specifies the data collection powers in advance of appointment of the MD commission and limits them by means of a definitive list. Thus, for the purpose of determining whether an expert opinion by the MD is to be obtained in the case of incapacity for work, health insurance funds may in principle only process the data relating to the insured person that has already been lawfully collected pursuant to Section 284(1) SGB V - and is thus already available - to the extent necessary in each case. If the processing of data already available to the health insurance funds is not sufficient to assess whether the MD should be called in to examine the incapacity to work, the health insurance funds may, notwithstanding the above, only collect and process data from those insured in accordance with Section 275(1b) sentence 2 SGB V about

- whether a resumption of work is foreseeable and, if so, when it is likely to occur;
- specific upcoming diagnostic and therapeutic measures that prevent a resumption of work

to the extent necessary in each case.

The legislation also takes account of my considerable data protection concerns with regard to the telephone enquiries made to those insured by various health insurance providers, some of which contained inadmissible questions about health, social or family problems and exerted inadmissible pressure on insured persons who were unable to work (see also 29th AR, No. 7.15). According to Section 275 (1b) sentence 3 SGB V, health insurance funds may only collect the above permissible information from insured persons in writing or electronically after a foreseeable return to work and concrete upcoming diagnostic and therapeutic measures. Collection of information by telephone is only permissible if the insured persons have previously consented to telephone collection in writing or electronically. The health insurance providers must record every instance of telephone collection of information from the insured person. Those covered by the insurance must be informed of this and, in particular, of the right to information pursuant to Art. 15 of the GDPR.

I expressly welcome the legal clarifications and will focus my attention in the coming reporting period on the implementation of the requirements by the health insurance funds in accordance with the law.

Cross-references:

6.6 Model project genome sequencing

6 Individual topics

6.1 Electronic patient file

Health insurance providers are taking legal action against data protection supervisory measures imposed by me to enforce a design of the electronic patient record (ePA) that conforms to European law and thus against equal rights for all insured persons.

In my 29th Activity Report (AR) (No. 4.2), I reported on the fact that the design of the ePA based on the Patient Data Protection Act (PDSG) was contrary to European law. Access management in particular is not compatible with European law. The national legal requirements stipulate that access is only possible according to the “all-or-nothing” principle. From 1 January 2022 only users with an appropriate mobile end device will be able to grant detailed, i.e. document-specific, access. Insured persons who do not have their own suitable device or do not wish to use one are not covered by this. They can only grant limited access rights to categories of documents through the service provider, e.g. in a medical practice, or grant proxy rights to a third party with a suitable technical device, but in doing so they must disclose all their data to this person. In addition, those who cannot or do not want to use a suitable end device and do not want to make use of the proxy solution will also not have any ongoing insight into their own ePA, which they are supposed to maintain themselves.

These legal requirements severely curtail the sovereignty of those covered by the relevant insurance and constitute a violation of the principles of personal data protection applicable to the processing of personal data, namely:

- Lawfulness, fair processing, transparency (Art. 5(1) point (a) GDPR),
- Purpose limitation (Art. 5(1) point (b) GDPR),
- Data minimisation (Art. 5(1) point (c) GDPR),
- Integrity and confidentiality (Art. 5(1) point (f) GDPR)

They are also a violation of Article 25(1) GDPR, according to which the controller must implement appropriate technical and organisational measures, taking into account the state of the art. These must be designed to implement the aforementioned processing principles effectively and incorporate the necessary safeguards in processing to comply with the requirements of the GDPR and protect the rights of the data subject.

As the warning I issued in November 2020 to the statutory health insurance funds subject to my data protection supervision (see also 29th AR, No. 4.2) did not bring about any change, I pushed ahead with the announced data protection supervisory procedure and in September 2021 instructed five large statutory health insurance funds in accordance with Article 58 (2) point (d) GDPR:

1. they were required to organise access management of the ePA in such a way that insured persons can give their consent to those authorised to access the data according to Section 352 SGB V to access specific documents and data sets, and groups of documents and data sets of the ePA without barriers (“specific access management”). This can be achieved for insured persons who do not have a suitable device as a user interface (front-end non-users), in particular by means of the decentralised infrastructure of the service providers or by other technical facilities of the service providers, on their business premises or in cooperation with other health insurance funds or agencies.
2. Access management for the ePA must be designed in such a way that front-end non-users can also access the personal data concerning them (both documents and data records of the ePA and log data) without appointing a representative. This can also be achieved in particular by means of the decentralised infrastructure of the service providers or by other technical facilities of the service providers, on their premises or in cooperation with other health insurance funds or agencies.

3. For insured persons who use a suitable device as their user interface (front-end users), point 1 must be implemented by 31 December 2021, at the latest within one month of any final judgement taking legal effect.
4. For front-end non-users, the implementation of points 1 and 2 must take place within one year.

The health insurance funds to which these instructions were directed have taken legal action.

6.2 Data strategy of the federal government

The federal government has presented a data strategy in 2021 in which it brings together its measures to promote the digital economy. Further developments in data protection should also be taken into account in this context.

The federal government adopted a so-called data strategy at the beginning of 2021. In doing so, it has followed the example of the European Commission, which already presented a definitive EU data strategy on 19 February 2020 (see COM(2020) 66 final). The national data strategy (like the EU data strategy) focuses on measures to promote a European digital economy. One overarching goal is to secure digital sovereignty.

Both the Federal Chancellery (BKAmt) and the German Bundestag have given me the opportunity to comment. I welcomed the federal government's efforts, while calling for some improvements. Creating strategies means defining clear goals and developing an overarching plan.

According to the data strategy, innovative and responsible provision and use of data in Germany and Europe is to increase significantly - in business and science, in public interest research and in civil society and administration. At the same time, fair participation is to be ensured on the basis of European values, data monopolies are to be prevented and misuse of data is to be countered consistently. These objectives still seem appropriate to me, not least because of the clear commitment to the European General Data Protection Regulation (GDPR). One interesting example of how these efforts are being implemented is the Gaia-X project to build a secure and trustworthy European infrastructure for pooling and sharing data, which is already running. Early publication of a data strategy and a transparent approach enable both the public and me in my supervisory role to better understand what impact digital policy plans may have on data protection.

At the same time, I have criticised a number of points. Overall, despite some verbal commitments, the data strategy has proposed little that is concrete or new in terms of data protection. Instead, reference is made to a large number of projects that are already underway. What seems to me to be missing is an alignment and integration of the economic vocabulary relating to data (such as data sharing, responsible data use and data access) with the concepts of data protection law. Accordingly, even in the European legislative projects created on the basis of the EU data strategy (DGA, DSA), ambiguous formulations appear, where it is not clear whether data protection applies or only processing of non-personal data is being regulated. Re-identification risks are not addressed in anonymisation procedures, which could play a major role in data exchange between companies, for example. And ultimately, there is a lack of a data protection alignment of the planned data economy with regard to the new processing standard involving big data in combination with AI applications. Both the individual and supra-individual risks associated with mass data exchange (e.g. abolition of the anonymity of publicly accessible spaces; statistical pre-judgements applied across the board) require further investigation, legal support and strengthening of supervisory instruments. In any case, approaches that focus solely on the marketability of existing data protection concepts such as consent or pseudonymisation appear doubtful. And even promising new concepts such as the so-called data trust (data intermediary) still require further consolidation before their compatibility with data protection requirements can be accurately assessed.

Cross-references:

5.9 EU Digital Legislation

6.3 Cooperation between cartel and data protection supervisory authorities

The rapid advance of digitalisation with its ever-increasing impact offers many new opportunities, but also a variety of risks that need to be addressed. Data protection and antitrust law have a very special role to play here in the context of regulation. For efficient and consistent enforcement of the existing regulations, cooperation between the authorities is essential.

The market activities of the major international companies in the internet industry in particular show us how digitalisation is increasingly permeating and shaping social and economic life. What might have seemed unthinkable not so long ago has become commonplace in

many cases. This shows opportunities, but the risks associated with them must not be neglected and must always be taken into account. Data-driven business models of companies with their immanent processing of personal data increase the risks of their market power and pose a threat to the right of informational self-determination for every individual.

In its proceedings against Facebook initiated in 2019, the Federal Cartel Office (BKartA) has for the first time tackled this problem area under competition law and prohibited Facebook from combining personal data

from its subsidiaries WhatsApp and Instagram without effective consent under data protection law. I have been following these proceedings closely from the outset and have provided assistance on issues of data protection. I have also given my colleagues on the European Data Protection Board (EDPB) regular updates about this. In the meantime, the Upper Regional Court (OLG) of Düsseldorf has referred questions of interpretation of the General Data Protection Regulation (GDPR) to the European Court of Justice (ECJ), including on the relationship between data protection and antitrust supervision. I am of the opinion that artificial precedence should not be given to any one supervisory area here. Rather, these issues should be the focus of all competent supervisory authorities and consistent supervisory practice should be made possible through regular interaction.

The amendment to the Act against Restraints of Competition (GWB-Digitalisation Act), which came into force in Germany in 2021, makes it possible to punish abusive business practices, which in many cases are also out of line with data protection requirements, quickly and effectively. For example, the GWB now clarifies that denying access to competition-related data can constitute prohibited conduct by companies that dominate markets. In this context, however, it is essential to note that, in addition to the right of access under competition law, the prerequisites under data protection law for processing the data must also be met. In addition, the BKartA has been given additional powers to be able to examine the market relevance of large technology companies and has already initiated a number of investigations in this connection, in which data processing also plays a central role. The new legal basis introduced with Section 50f GWB for the exchange of data and

cooperation between the competition, consumer protection and data protection authorities is an important instrument here, which the BKartA and I have been using successfully.

In the context of cooperation between cartel and data protection supervisory authorities, Germany is thus taking on a kind of pioneering role, which must also be

implemented at the European and international level. I am therefore strongly in favour of enabling such cooperation in the Digital Markets Act (DMA) currently being negotiated at European level. In addition, I am actively supporting both the activities to promote stronger cooperation between antitrust and data protection supervisory authorities within the framework of the Global Privacy Assembly (GPA), and the interaction between the data protection authorities of the G7 countries in order to encourage other supervisory authorities to cooperate accordingly.

6.4 Restart of the Research Data Centre at the Federal Institute for Drugs and Medical Devices

In order for the data from the health insurance funds and from electronic patient files to reach the Research Data Centre in a data protection-compliant manner, a wealth of technical specifications must be implemented, including the procedure according to which the trust office carries out pseudonymisation of these data.

According to the regulations of Sections 303 a ff. SGB V and the Data Transparency Ordinance (DaTraV), the billing data of the health insurance funds are collected pseudonymously in the Research Data Centre (FDZ) at the Federal Institute for Drugs and Medical Devices (BfArM), where they can be used for research purposes, among other things. I have already dealt with the expansion of the content of the regulations, which have been in place since 2012, and with the ordinance issued for implementation in recent years (28th AR No. 5.6; 29th AR No. 5.7). According to the regulations under the Patient Data Protection Act (PDSG), data from the electronic patient record (ePA) can also be released to the Research Data Centre from 2023 onwards (under Section 363(1) to (7) SGB V; 29th AR No. 4.2).

During the reporting period, the focus was on the technical implementation of these regulations. In addition to the BfArM as the “registry”, the Robert Koch Institute (RKI) as the trust office, gematik GmbH as the controller responsible for transmission through the telematics infrastructure (TI) and the Federal Ministry of Health (BMG) itself were involved. In addition to hosting the FDZ, one focus was the proper formation of the so-called cross-period pseudonym (PüP). This PüP is formed by the trust office and is used to allocate health insurance data over years. A procedure also had to be developed for allocation of the data from the ePA to the same cross-period pseudonym. An asymmetric cryptographic procedure is to be used to generate the transmission pseudonym. With regard to the data from the ePA, the procedure uses

a public key of the RKI, which is stored in the ePA app, and a working number in order to forward the data in encrypted form to the trust centre first. For the release from the ePA, it also had to be determined where the consent is documented, while the scope of the release must also be recorded. In addition, it had to be ensured that if consent was revoked, the data would be erased immediately. The topic of the FDZ will continue to preoccupy me in the coming year, when I will be addressing the concrete arrangements for data transfer from the ePA to research in the form of Medical Information Objects (MIO).

6.5 Use of the health insurance number in the telematics infrastructure

The use of the health insurance number (KVNR) as unique identification of insured persons in various applications within the telematics infrastructure (TI), such as the TI messenger, is a data protection-friendly solution. However, this is only possible with a clear legal basis.

The Digital Modernisation of Care and Nursing Act (DVPMG), which came into force on 9 June 2021, created, among other things, the legal basis for the implementation of a messenger service for communication between insured persons and service providers within the TI (Section 342(2) No.

4 SGB V). gematik GmbH was commissioned with the development of this TI messenger ("TIM"). It requires the implementation of a procedure for unambiguous addressing of those who are insured. Discussions between the BfDI, the Federal Ministry of Health (BMG) and gematik resulted in a consensus that the most data protection-friendly solution would be the creation of a non-re-identifiable matrix address from the health insurance number (KVNR). The alternative of the creation of a register of all participating insured persons would entail greater data protection risks. This conclusion also corresponds with the legislative justification for Section 342(2) No. 4 SGB V, which excludes the creation of a new list of insured persons and instead proposes the use of a pseudonym from the KVNR. Other applications within the TI, such as electronic patient files and e-prescriptions, also use the KVNR to identify the insured.

However, the processing is only permissible under data protection law on the basis of a clear legal authorisation standard, which currently does not exist. In particular, processing of the KVNR by the service providers in the context of a voluntary application of the TI cannot be

subsumed under any of the case groups listed in Section 18 SGB IV, a standard which regulates the permissibility of processing the insurance number. SGB V also does not provide any special legal regulation for the use of the KVNR for the purposes described.

In order to establish a legally compliant and secure situation, it is imperative to create a clear legal basis for processing of the KVNR within the TI. However, since the options for identifying insured persons do not represent alternatives in terms of data protection friendliness, I have informed the BMG that I will put up with the current state of affairs for the time being, but expect in return a corresponding legal basis to be created at the earliest possible opportunity.

Processing of the KVNR in connection with TI applications also proves to be problematic in another respect. For example, Section 362(1) SGB V stipulates that private health insurance companies (PKV) and other providers will in future use the unchangeable part of the KVNR for those they insure according to Section 290(1) sentence 2 SGB V for the use of TI applications and for notifications under the Implant Register Act (IRegG). For this purpose, the KVNRs must be created in advance by the trust office in accordance with Section 290(2) sentence 2 SGB V. In order to exclude double allocation, the allocation procedure checks whether a KVNR has already been allocated to the insured person in question. For this purpose, a so-called clearing procedure involving the health insurance funds is set out in the "Guideline on the structure and allocation of a health insurance number and regulations of the health insurance number directory according to Section 290 SGB V". In the process, data relating to those who are insured, such as the KVNR, pension insurance number, surname, first name(s), gender, date of birth and place of birth, are shared between the health insurance funds.

If the PKV and the other providers specified in Section 362 SGB V use the KVNR in future for the participation of those they insure in TI applications, their inclusion in the clearing procedure is required. However, there is no clear legal basis for this either. The BMG shares this view and has assured me that it will introduce a corresponding standard for these powers in the next appropriate legislative procedure. A discussion draft has already been submitted to me, which now requires coordination between the BMG, BMJ and myself.

Cross-references:

5.10 Developments in health registers, 6.1 Electronic patient record

6.6 Genome sequencing model project

An additional source of data is being made available to research in a “fast-track” procedure; technical and data protection concerns are being disregarded in favour of a quick resolution.

The draft of the Act on the Further Development of Health Care (GVWG) of 1 January 2021 submitted by the federal government - still without a regulation on genome sequencing - comprised about 170 pages covering 15 articles of amendments to a wide variety of laws; in Article 1 on the SGB V alone, there are as many as 72 items with proposed amendments to various paragraphs. Supplementary amendments to this appeared as early as March 2021 in the parliamentary consultation procedure, which ran to 88 pages. Amendment 3 included the draft of a new Section 64 d SGB V on the “Genome sequencing model project”. The regulation is intended give those covered by statutory health insurance the right to personalised medicine in the case of rare and oncological diseases. This means that genome sequencing will be used for diagnosis and to find therapies. Another important aspect of the regulation was the establishment of a so-called “common data infrastructure” in which genome data can be stored and used. Unfortunately, the wording lacked substance and was too vague in many respects, which I pointed out in my statement of 29 March 2021. Essential points were not covered by the regulation: there was a lack of detail on organisation and development of the data infrastructure, responsibility under data protection law, the design of the procedures, e.g. for the use of data, and on responsibilities generally. Regulations on data security and the relationship to the Gene Diagnostics Act were also conspicuous by their absence.

In view of the shortage of time - the Health Committee was about to meet without any opportunity to respond to the glaring deficiencies and without any readjustments - I addressed a letter directly to the Health Committee of the Bundestag on 9 April 2021. It listed in detail the missing regulations and ended with the recommendation to postpone the project in order to allow a technically and legally complete regulation to be drafted.

Contrary to my recommendation, the regulation of the model project was not put on hold. A revised version submitted shortly afterwards contained specifications on data flows, a trust office and an application procedure for data access, which were based on the regulations of Sections 303a ff SGB V for the Research Data Centreat the Federal Institute for Drugs and Medical Devices (BfArM). Another revision of 19 May 2021 took into account further relevant points raised by me and provided details

of the bodies responsible for the trust office - the Robert Koch Institute (RKI) - and the data infrastructure - the BfArM.

The original goal-oriented approach of a distributed data infrastructure fell by the wayside in this congested process. A decentralised structure is the state of the art in this context. A needs-based, partial exchange of data or data access is sufficient for the purposes of the model project and avoids continuous duplication of data storage - as is now the case at the BfArM. Decentralised data storage has further advantages: it corresponds to the principle of data minimisation and also facilitates the fulfilment of data security requirements in technical terms.

So there is still a lot of potential for improvement and I hope that this will be exploited in the new legislative period.

Cross-references:

5.11 Data collection powers of the health insurance funds in sickness benefit case management

I recommend structuring the development of the “common data infrastructure” for the genome sequencing model project in a decentralised way and providing for ad hoc data access instead of double data storage.

6.7 Prenatal testing in Hong Kong

The performance of prenatal tests must not be outsourced to laboratories in third countries for reasons of cost where there are considerable risks with regard to compliance with data protection regulations.

During the reporting period, international press reports (<https://www.reuters.com/investigates/special-report/health-china-bgi-dna>) revealed that a group of Chinese companies is operating laboratories in Hong Kong, among other places, which examine genetic sample material. They are also commissioned to a not inconsiderable extent - the main reason for this is the cost factor - by German service providers to evaluate non-invasive prenatal blood tests (NIPT), a service used by pregnant women. I am aware, for example, that such a prenatal test is offered in Germany by a company based in Hesse, which forwards the sample material obtained to the Chinese laboratories. According to the press reports, there are concrete indications that the Chinese company is also using the samples for its own research projects, which may also be conducted in cooperation with the Chinese military.

Apart from the improper use of the data, which would be inadmissible in any case, the transfer of personal data to third countries for which there is no adequacy decision by the European Commission and for which adequate protection of personal data is not ensured in any other way is also inadmissible, especially when it comes to such sensitive data.

The Data Protection Commissioner for Hesse, who is responsible for the data protection supervision of the aforementioned laboratory is currently reviewing compliance with data protection. It was agreed with the company that no further samples would be sent to the Hong Kong-based laboratory until the review has been completed.

In the meantime, NIPTs have been approved as a statutory health insurance benefit in pregnancies with special risks on the basis of the decision of the Federal Joint Committee of 19 September 2019 as an amendment to the maternity guidelines (BAnz AT 20 December 2019 B6).

I have contacted both the Federal Joint Committee and the National Association of Health Insurance Funds (GKV-SV) and pointed out the existing problem to them. At the same time, I called on them to take measures to ensure the security of the genetic data of those insured in connection with the offer of NIPTs, which are particularly sensitive in accordance with Art. 9 GDPR.

As a first step, I was able to ensure that the maternity guidelines were supplemented by a reference to compliance with data protection requirements when doctors commission laboratories. The results of the review by the Data Protection Commissioner of Hesse remain to be seen and may also result in a need for further action on my part.

6.8 Implementation of the right to correct a diagnosis under Section 305 SGB V

After initial difficulties, the implementation of the newly regulated diagnosis correction entitlement involving the statutory health insurance funds has been successful.

In my 29th Activity Report (No. 7.14), I reported on the amendment of Section 305(1) SGB V, which was intended to help insured persons enforce their right to rectification guaranteed by Art. 16 GDPR in respect of their health insurance fund by means of a right to correct a diagnosis, including at national level. At the beginning of this reporting period, I was still receiving complaints from

insured persons whose health insurance companies had not resolved their claim for correction of diagnostic data within the legally stipulated period of four weeks, despite the formal requirements having been met (proof of incorrectness by medical certificate). According to individual health insurance funds, the delay was due to the complex technical implementation of the legal requirements, which required a certain lead time, but which had not been provided by the law.

I understood the point of view of the health insurance funds, initially refrained from taking any data protection supervisory measures in cases of delayed rectification of diagnoses and accepted transitional solutions - for example, in the form of notification of the insured persons that the medical confirmation of incorrect diagnosis could be added to any (incorrect) patient receipt already obtained until the correction claim had been completely resolved technically and that both documents could be transmitted to third parties (e.g. insurance companies) in full for the time being.

No further complaints reached me in the third quarter of this reporting year. I am therefore assuming that the technical implementation of the diagnosis correction right has been successfully completed. I will check this in the context of forthcoming on-site inspections in health insurance funds.

6.9 Reimbursable digital health applications

In future, it will no longer be sufficient merely to submit a self-declaration of data protection conformity from the manufacturer for reimbursable health applications; it must be proven by a certificate.

The Federal Institute for Drugs and Medical Devices (BfArM) maintains a list of reimbursable digital health applications (DiGA) in accordance with Section 139e(1) SGB V and Section 33a SGB V and decides on applications from DiGA manufacturers for inclusion in the list. The manufacturers of digital health applications currently demonstrate compliance with the data protection requirements according to Section 139e(2) sentence 2 no. 2 SGB V using a self-declaration according to Annex 1 to the Digital Health Applications Regulation (DiGAV).

However, this procedure is inadequate from the point of view of data protection law, as compliance with data protection requirements cannot be assumed with certainty on the basis of a manufacturer's declaration alone. In this respect, I successfully campaigned for a change regarding this evidence within the framework of

the legislative procedure for the Digital Care and Nursing Modernisation Act (DVPMG).

As of 1 April 2023, the previous practice of self-declaration will be replaced by the provision of evidence by means of a data protection certificate pursuant to Article 42 GDPR.

With regard to the data protection certificate, the BfArM, in agreement with me and in consultation with the Federal Office for Information Security (BSI), has been commissioned with amending the regulation of Section 139e(11) SGB V within the framework of the DVPMG by developing test criteria. These are intended to translate the applicable and abstract legal data protection requirements of the GDPR and Section 4 of the DiGA Regulation into application-orientated testing points. The test criteria will be defined for the first time by 31 March 2022.

I expect to be able to reach agreement with the BfArM in the first quarter of 2022.

6.10 Digitalisation of public administration

The digitalisation of public administration remains a priority concern for government officials at the federal and state levels. With the self-imposed implementation deadline of 31 December 2022 in mind, they are stepping up their activities enabling them to offer administrative services to citizens electronically via their portals.

Federal Portal and federal user account

The Federal Administration Portal (Federal Portal) provides access to administrative services, especially those of the federal government, but also those of the federal states and municipalities, for both citizens and organisations (e.g. companies). The Federal Portal, which is still under construction, was available in 2021 in a basic version that was successively expanded and improved by the responsible agency, the former Federal Ministry of the Interior, Construction and Community (BMI).

In order to be able to carry out identification and authentication for digital administrative services, a user account is required. Since April 2021, this has been provided by the BMI at federal level only in the form of a citizen account (Federal User Account for natural persons). At the same time, the previous “company account” component of the Federal User Account has been disabled and company accounts that had already been created were erased. For legal entities, associations with legal capacity, natural persons in their function as traders, professionally self-employed persons and for public

authorities, a so-called uniform organisation account is to be introduced as a user account.

I have been in regular and continuous contact with the BMI about the data protection issues in the course of development of the Federal Portal and Federal User Account projects to date, including the planned further developments and optimisations. This is a good example of practical and effective consultation of the federal government that could serve as a model for other projects.

E-legislation and e-scanning

The “Electronic Federal Legislation Procedure” (E-legislation) project is part of the Consolidated Services in Federal Government. Here, federal legislative procedures are to be designed on a uniform IT basis in such a way that coordination processes can take place without media discontinuity. To this end, a common platform is being developed on which the organisational units of the federal ministries involved in law-making can create legal texts in a uniform structure that complies with the Manual of Legislative Procedure. These documents are then to be submitted on the platform by the respective lead department of the federal government to the departmental coordination processes, in which I will also be involved.

In the operation of this platform, personal data of employees of the participating authorities are also processed. Those responsible for the project chose an iterative approach in which a version of the product with limited functions was available at an early stage of development.

In several releases each year, the functions have been and are being expanded. This approach has made close data protection consultation necessary. Planned changes to the processing of personal data had to and still have to be examined and evaluated at short notice, so that continuous, constructive collaboration with the BMI, which is also in charge of this project, has been established here as well. With regard to the first product release in April 2021, the consultation focused on the question of responsibility under data protection law and, for the release of the updated version in October 2021, on data protection by default (privacy by design), as well as an examination of the processing of special categories of personal data. My comments in this regard were taken up and implemented by the BMI.

Also part of the service consolidation is the e-scanning measure, which involves the digitalisation of incoming documents and inventory files. Here I advise the steering committee established by the BMI in June 2021. Although this project is still in its early stages, I can already see that a constructive consultation process is also underway here.

6.11 Brexit - Data transfer with the United Kingdom

On 28 June 2021, the European Commission adopted the adequacy decisions for transfers of personal data to the United Kingdom under the General Data Protection Regulation (GDPR) and the Prosecution of Criminal Offences Directive (JHA Directive). With the recognition of the adequate level of data protection, data transfers from the European Economic Area (EEA) to the UK within the scope of the decisions do not require specific authorisation by data protection supervisory authorities and do not need to be accompanied by any further safeguards under Chapter V of the GDPR or Chapter V of the JHA Directive.

On 31 December 2020, the transitional period ended, during which the United Kingdom was already no longer a member of the European Union (EU), but EU law and thus the GDPR still applied. On 1 May 2021, the Trade and Cooperation Agreement between the EU and the UK came into force, which had already been applied provisionally since the beginning of 2021 to bridge the period between the expiry of the transitional period on 31 December 2020 and the entry into force on 1 May 2021. On this basis, personal data could continue to be transferred to the UK without any special safeguards until 30 April 2021 (extended until 30 June 2021), even though the UK had to be considered a third country under the GDPR as of 1 January 2021 because of Brexit.

In parallel to the transitional period, the European Commission launched the adoption procedure for the adequacy decisions for the United Kingdom on 19 February 2021. The European Data Protection Board (EDPB) passed two opinions on these drafts at its meeting in 13. April 2021²⁰.

On 28 June 2021 the European Commission adopted both adequacy decisions for transfers of personal data to the UK under the GDPR and the JHA Directive²¹. With this recognition of the adequate level of data protection, data transfers from the EEA to the UK within the scope of the decisions do not require specific authorisation by data protection supervisory authorities and do not need to be accompanied by any further safeguards under Chapter V of the GDPR or Chapter V of the JHA Directive. Both adequacy decisions are valid until 27 June 2025, unless they are extended before then (see 3.2.2.2 above).

Scrutiny of whether the general data protection requirements for specific instances of data processing are met remains necessary independently of this.

Cross-references:

3.2.2.2 Focus on third country transfers

6.12 Outing of asylum seekers

Data on sexual orientation are special categories of personal data the processing of which is also problematic in the context of asylum law.

A petitioner contacted me about several cases and described what he saw as the outing of homosexual asylum seekers or supporting persons in the context of the questioning of witnesses by so-called trusted lawyers in the asylum seekers' countries of origin. Within the framework of the asylum procedure, the Federal Office for Migration and Refugees (BAMF) has to clarify the facts presented by an asylum seeker ex officio. If the asylum seeker does not have knowledge of the specific facts in their country of origin and the Federal Foreign Office (AA) does not have any knowledge of this either, so-called trusted lawyers can be commissioned to carry out investigations. For this purpose, the BAMF sends the AA the specific facts of the case and the questions to be clarified on corresponding forms. Subsequently, the AA instructs a lawyer under contract with it in the country of origin. In this context, it must transmit the facts of the case and the questions to be clarified to the latter. Particular caution is required here in connection with the sexual orientation of asylum seekers. Data may only be transmitted to the AA and by the AA to the trusted lawyer to the extent necessary. Special care must also be taken in the selection and instruction of trusted lawyers in order to avoid endangering asylum seekers by (unintentionally) outing them or persons supporting them in the course of their investigations.

6.13 Analysis of mobile phone data by the Federal Office for Migration and Refugees unlawful?

On 2 June 2021, the Berlin Administrative Court (VG) ruled in the first instance on a complaint against the analysis of the mobile phone data of an asylum seeker and upheld it.

20 EDPB Opinion on the draft adequacy decision GDPR: https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf
EDPB opinion on the draft adequacy decision JHA-DIR: https://edpb.europa.eu/system/files/2021-04/edpb_opinion152021_ukadequacy_led_en.pdf

21 Adequacy Decision GDPR: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf

Adequacy Decision JI-RL: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf

Section 15a of the Asylum Act (AsylG) grants the Federal Office for Migration and Refugees (BAMF) the basic authority to evaluate the data carriers of foreigners. However, the prerequisite is that this must be necessary to establish the identity and nationality of the asylum seeker and that the objective cannot be achieved by less intrusive means.

The BAMF reads the mobile phone data of asylum seekers at a very early stage. Certain data are evaluated in a so-called result report. This is then stored in a data vault. Only after justification of necessity will this report be released for further use in the asylum procedure after appropriate examination by a fully qualified lawyer. This practice is questioned by the VG in its decision. In the case at hand, the BAMF could have used less intrusive means, such as the asylum seeker's documents submitted at an early stage, instead of analysing the mobile phone. The VG ruled that reading the data from the mobile phone and storing them for future reference was inadmissible. Since the collection of the data had been illegal, the VG was of the opinion that the results report should not have been used either. The opinion of the VG thus coincides with my position.

The BAMF has lodged an appeal with the Federal Administrative Court against the ruling of the Berlin Administrative Court. The decision of the higher court may have far-reaching consequences for the future practice of the BAMF and is therefore eagerly awaited, and not only in this context.

In a similar case, a data subject filed a data protection complaint with me against the analysis of his mobile phone. This has not yet been resolved.

6.14 P 20 - Police 20/20: The path to a common “data house”

There is still a long way to go before the federal and state police authorities have a common “data house” In order to achieve this goal, not only technical and structural hurdles must be overcome, but the guiding principles of data protection law must also be observed from the very beginning across the programme and in approximately 30 sub-projects.

In recent years, I have repeatedly reported on the project, which has now been renamed “P20 - Police 20/20” (see 29th AR No. 6.1), and I have made it clear to the Federal Ministry of the Interior, Construction and Community (BMI) how important my regular involvement is in the development of this large-scale IT project. In addition, I have asked several times for a list of all sub-projects

of P20 - Police 20/20 together with project descriptions in order to gain an overview of the scope of the project.

Involvement through the BMI in P20 - Police 20/20 and the sub-projects

My agency's information on the P20 - Police 20/20 project has improved. In April 2021, the BMI provided me with a list showing that the project currently includes about 30 sub-projects, some of which are already being piloted in different federal states and with different numbers of participants. In addition, I was involved in advance and at short notice in the award procedures for a uniform evidence management system (eAMS) and the electronic file in criminal cases (EAS). I have submitted initial comments on both procedures.

The BMI obviously recognised the need for consultation during the course of the year and has since informed me on a quarterly basis about the current status of the overall project. I was also invited to an appointment with the Competence Centre for Professionalism (CCF). In addition, meetings were held with the core data protection group, which is based in the BMI, and the INPOL working group (a working group of the DSK's Security Working Group) on selected topics. Workshops have already been held on “hypothetical data re-collection” and on the “data consolidation proof of concept (PoC)” sub-project. I have been promised further workshops on purpose limitation, AI applications, identity and access management and WiPras (repeat prediction assistant). I expressly welcome the fact that the BMI is now involving me more.

Data consolidation proof of concept (PoC) sub-project

With the Data consolidation PoC sub-project, another network system outside the police information network is to be created under the Federal Criminal Police Office Act (BKAG) (see 29th AR No. 6.1). In contrast to the police information network, the PoC is intended to allow data in the low-threshold area to be compared and researched with the involvement of the police authorities of the federal states. In fact, this is a second information network - in addition to the one provided for in Section 29 BKAG - which, however, falls below the storage thresholds provided for in the act. The Federal Criminal Police Office (BKA) is to act as a technical service provider and support the federal states as a “processor”.

At the end of the year, the BMI presented the software to me. Although the BMI did not consider itself responsible for this sub-project last year, it has since informed me that the PoC has been integrated into the overall P20 - Police 20/20 project. I have raised my data protection objections from the outset (since the beginning of 2019) and continue to uphold them. I consider the data proces-

sing proposed by the PoC to be inadmissible under data protection law and I formally issued a warning to the BKA in March 2021 pursuant to Section 16(2) sentence 4 BDSG. There is no legal basis for the supporting activity of the BKA as a commissioned data processor for the federal states as planned with the PoC. Moreover, the data processing envisaged by the PoC is in contradiction with the final regulations of the BKAG. The BKA is not legally allowed to act as a commissioned data processor, especially if the “commission” actually belongs in its own area of responsibility as a central body, namely in providing a nationwide network here. Setting up commissioned processing is specifically out of the question if the result is to undermine the legal limits of the activity as a central body. The BKA has commented on the warning, but does not share my legal opinion. I made my objections clear to the BMI once again in the workshop. Further developments remain to be seen. I will report on the progress.

Development of the overall project

One focus of development last year still clearly lay in the organisational and coordinating area of the various committees.

In terms of content, the BMI has made it clear that it will give priority to the standardisation of the case processing systems (FBS) and the procedural processing systems (VBS), interconnected systems (INPOL and PIAV) and an eAMSe. Appropriate interim solutions are currently being developed for this purpose. The amount of data held by the federal and state police forces is extremely extensive. With this in mind and due to the technical complexity, the IT systems can only be converted step by step before the data can be stored in the proposed data house. The conceptual design phase for the “common data house” is to be brought forward to the end of the year. The key to the data house will, in my view, comprise precise distribution of access rights so that the principle of purpose limitation is upheld and a distinction can be made between the individual police purposes (see No.11.5). The BMI has promised me early involvement in the data house sub-project.

In my last Activity Report (see 29th AR No. 6.1), I commented on the strategic component of the Police Information and Analysis Network (PIAV-S). PIAV-S is intended to expand the exchange of information and intelligence between the federal and state police forces. My data protection concerns about the project have not yet been dispelled. So far, it has not been possible to clarify conclusively whether the data processed by PIAV-S are anonymised or pseudonymised and are thus personal data. I am still in discussion with the BMI on this.

The overall programme manager made it clear that P20 - Police 20/20 was characterised by agile programming. In

a letter of principle coordinated with the INPOL working group, I recently commented on the form in which data protection requirements must be implemented within agile programming processes. In particular, data protection requirements must be fully defined and robustly documented before the start of agile development.

Cross-references:

6.25 Agile project development

6.15 GETZ: Inadequate evaluation

The Joint Counter-Extremism and Counter-Terrorism Centre (GETZ), founded in 2012, serves to combat politically motivated crime, terrorism, espionage and proliferation. However, a serious evaluation of this institution does not seem to be wanted.

All major federal and state authorities (40 in total) from the areas of the police, intelligence services and law enforcement meet regularly in the GETZ. There they informally exchange views on developments and trends in the various “phenomenon areas”. I am generally critical of the way the work in the GETZ is organised in terms of data protection law, as it affects the separation requirement between the police and intelligence services introduced in post-war Germany, and the exchange of information there is also far from transparent.

In spring 2020, the Federal Ministry of the Interior (BMI) sent me an evaluation report on the GETZ from 2017 in response to several requests. Due to its classification, I cannot go into the contents of the report here.

However, I can say that I consider the evaluation to be methodologically inadequate and incomplete and therefore not helpful overall. This starts with the fact that it was not an independent body, but one of the authorities involved, that was commissioned with the evaluation. The subject of the evaluation, the GETZ and its work processes, is not described in detail in the report. The topic of data protection was left out of the evaluation entirely - and this in a discussion group of police authorities and intelligence services the content of which remains unknown. How many crimes were prevented or solved through the practical exchange of information is also not an issue. Documentation of the evaluation is factually non-existent, so that it is not possible to make an independent assessment of the results of the report.

Overall, I got the impression that the main objective of the evaluation was to legitimise the political decision to establish the GETZ.

An independent and objective evaluation in the sense of a critical analysis of its success was obviously not

wanted. I communicated my criticism to the BMI in May 2020 and urgently suggested a new evaluation, without any response. I followed this up again in 2021, but have again received no answer. Only after I informed them that I would include this section in the Activity Report did the BMI inform me that I had apparently been provided with incomplete documents. I will now request these and report further if necessary.

6.16 Data processing at the BND

Establishing data protection-compliant conditions for the Federal Intelligence Service (BND) sometimes takes a lot of patience. Already in 2009, I had identified violations of data protection law in the context of the operation of a large central filing system at the BND. These have not been fully remedied to date.

In my 23rd Activity Report, I reported on violations of data protection law in a large filing system kept by the BND. Among other things, the BND had not implemented and carried out resubmission and erasure checks for this large file in accordance with the legal requirements. As a consequence, the file contained personal data the processing of which was no longer necessary and thus inadmissible. Nevertheless, these data have not been erased.

At the end of 2015, the BND implemented a system-based resubmission to check the necessity of further processing and, where necessary, arrange for erasure of personal data in the large filing system. As a result, the data set in the filing system was split into two types of data in particular. On the one hand, there are data for which a legally compliant erasure resubmission function has been implemented, and on the other hand, there are data that were contained in the filing system before the resubmission function was implemented. For the latter, the resubmission function was not put into operation, so that after ten years in the active file, they are transferred to the data protection archive area of the filing system without a check that they are necessary.

I continue to regard this approach as questionable under data protection law.

To date, the BND has rejected the non-technical solution of creating a legally compliant situation by reviewing the documents contained in the file for personal data subject to erasure, citing the unaffordable expense. For a long time, the BND and the Federal Chancellery (BKAm) has refused to erase the majority of the archived material, citing the need to keep the information for political purposes (e.g. committees of enquiry).

In 2018, there was a turnaround in the sense that the BKAm offered the prospect of erasing its archive holdings, but without naming a date. However, questions of archival law would first have to be clarified with the Federal Archives. I actively supported this clarification process and further pointed out that the unlawfully stored personal data must be erased. If it were possible to separate personal data from non-personal data, the latter could of course still be archived. However, if this is not possible, the entire archive would have to be erased.

A clarification of this issue with the BND, the BKAm and the Federal Archives could not be achieved by the editorial deadline for this Activity Report.

Although the data protection archive area is not actively used and is only accessible in narrowly defined exceptional cases, it is still growing steadily today.

I will observe further developments and continue to press for a data protection-compliant status for the filing system in the future.

6.17 Transfer of the Stasi files to the Federal Archives

Since 17 June 2021, the Stasi archives have belonged to the Federal Archives. For the time being, nothing will change in the legal regulations for dealing with the Stasi files.

With the entry into force of the Act Amending the Federal Archives Act, the Stasi Records Act (StUG), and establishment of an SED Victims' Commissioner, the Office of the Federal Commissioner for the Stasi Records was dissolved. Since 17 June 2021, this has become part of the Federal Archives as the Stasi Records Archive.

This does not entail a change in the legal basis with regard to the Stasi files. Thus, the previous regulations of the StUG continue to apply to the work with the documents, but also with regard to access to them.

I welcome this, as it is still not general archive property of the sort usually administered by the Federal Archives. The Stasi files contain highly personal data that were usually obtained by unlawful means or even invented and thus require special protection and special access regulations. I will therefore continue to ensure during future inspections that these standards are being met as before. Special attention will be required if the intended consolidation of the records of several previous local offices takes place.

6.18 Applications on the electronic health card

With the Digital Care and Nursing Modernisation Act (DVPMG), which came into force on 9 June 2021, some new applications of the telematics infrastructure (TI) were introduced, while other existing ones were newly regulated. In my advice on the technical implementation of the new requirements, I make sure that a separation of the data processing for the different applications is still guaranteed.

So far, the emergency data record and electronic medication plan applications have been set up for the electronic health card (eGK). The emergency data record is now being incorporated into the new electronic patient summary file (ePKA). The medication plan is being transferred to its own application in the TI, without storage on the eGK. Insured persons have a choice of which system to use for a transitional period.

Even though the ePKA has a similar name to the electronic patient file (ePA), it fulfils a different purpose. It should be possible to store clearly defined, structured emergency data here. These data are used, for example, to enable paramedics to obtain an overview of relevant pre-existing conditions and health status even without the technical approval of the insured person. They also form the basis for the exchange of data with doctors in other EU countries. In this context, insured persons must give their consent to participate in the European system in the first place, and they must specifically give their technical approval for the transfer at the time of treatment abroad by means of a clear confirmation.

In my advice to the Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) on the technical conception of ePKA and the electronic medication plan, I advocate that the data processing for the ePA, the ePKA and the electronic medication plan remain separate. Insured persons must be able to choose the three applications independently of each other and trust that data processed in the respective application will not be available in other applications at the same time and without their active participation. Mixing these processing operations, which could lead, for example, to emergency access to the ePKA also being possible with the ePA, must therefore be excluded.

Since the DVPMG does not provide for a clear set-up procedure for the ePKA, I also suggested using a procedure similar to the set-up of the ePA, which stipulates an application to the health insurance fund and then an initial set-up by the service provider.

The DVPMG also leads to changes in the e-prescription, the current test phase of which was extended in Decem-

ber 2021. For private prescriptions, it should be possible to store the invoice data in the central e-prescription store. One of the focal points of my advice to gematik is to restrict access to this billing data by third parties. The app for the e-prescription, which gematik not only specifies but also develops itself, offers push notifications as an additional function. Since this function is handled via the platforms of the mobile operating system providers, detailed consultation was necessary here. From a technical point of view, I was able to convince gematik to encrypt the content and also to disguise the meta data by sending blank messages. At the same time, I provided extensive advice on data protection law with regard to possible transfers of personal data to third countries, explained the consequences of the Schrems II ruling of the European Court of Justice (see No. 3.2.2.2) and asked for compliance.

The DVPMG is also commissioning gematik to develop an instant messaging service for the TI (TI Messenger). In this regard, I advised gematik on the design and specification for this service and paid particular attention to ensuring that the requirements published for hospital messengers by the Data Protection Conference (DSK) in a white paper were also taken into account for the TI Messenger. The end-to-end encrypted TI Messenger is based on the Matrix protocol and is initially only available to service providers. Later in 2022, those covered by the insurance will also be able to use it for communication with hospitals and medical practices. From the point of view of data protection, this would constitute a great advance and an acceleration in medical care at the same time.

6.19 Digital identities

In order to use digital administrative processes, citizens need a secure and straightforward way to identify themselves online. I advise the federal government on several projects related to digital identities and have been arguing for a solution that is based on secure technology and protects users with clear rules.

The federal government is running several sub-projects (e.g. Smart-eID, ID-Wallet) in the area of digital identities. The common goal of these sub-projects is to enable citizens to “identify” themselves online. The federal government has brought the sub-projects together in the Digital Identities project of the Federal Ministry of the Interior, Construction and Community (BMI).

Online identification function of the ID card

A technical infrastructure for digital identities already exists in Germany in the form of the eID system. This is the familiar online identification function of the ID card,

the electronic residence permit and the eID card for citizens of EU member states (statements about the ID card below always refer to all three, technically identical documents).

With a suitable smartphone or card reader, the ID cards equipped with a chip can be used to prove identities online in a legally secure way. The system is considered privacy-friendly and secure. Digital identity is physically separated from the internet in the chip of the ID card. Furthermore, the system does not use a single number for each ID card. Instead, the chip generates a different number each time the ID card is presented. This makes it more difficult to create unwanted profiles of users across several services.

Since the agencies that want to process data from the ID card online have to register and are issued with a certificate, citizens can be sure when using the ID card that they are only disclosing their identification data to reputable providers.

Smart-eID

The eID system has been criticised for its limited applications and for what are perceived to be significant barriers to its use because of the link to the physical ID card.

In order to simplify the use of the eID system, the Personal ID Card Act (PAuswG), the eID Card Act (eIDKG) and the Residence Act (AufenthG) were each extended as of 1 September 2021 so that the ID card data may also be transferred to a mobile device, e.g. a smartphone, by means of a secure procedure and then serve as electronic proof of identity without using the physical card. The procedure developed for this purpose as an extension of the eID system is called “Smart-eID”. The existing eID infrastructure separate from the smartphone is also used entirely for the online function of the ID card, so that the data protection-friendly elements of this infrastructure also apply here.

ID wallet

At the same time, the federal government is running another sub-project in cooperation with several companies in which an ID wallet (“electronic wallet”) is being developed. This is a smartphone app, the aim of which is to allow citizens to store all kinds of verification documents. In addition to data from identity cards and driving licences, qualification and membership certificates could also be kept there.

The technical background is an infrastructure based on blockchain technology. To this end, a pilot project in the non-public sector was launched in spring 2021 with the “Hotel Check-in” application. On the basis of a corresponding trial clause in Section 29 of the Federal Registra-

tion Act (BMG), the ID wallet was tested as an additional electronic procedure that meets the requirements of the Act.

The aim of the federal government is to open up the ID wallet to all areas of life and thus, together with the blockchain infrastructure, to create a so-called “ecosystem” for self-managed certifications of all kinds from the public and non-public sectors.

Given the supervisory responsibility of the data protection authorities of the federal states over the non-public sector (e.g. hotel operators), my advice with regard to this planned use of the ID wallet was exclusively related to the basic structure of the app designed by the federal government. In this context, I have already been able to address questions and comments on, among other things, the questionable appropriateness of the blockchain technology and the security of the ID wallet app, which will affect both the pilot project and subsequent broader use.

The use of blockchain technology in particular raises complex data protection issues that have not yet been adequately clarified. If personal data are processed in the blockchain, there must be a data controller to whom data subjects can turn. Among other things, this party must be able to exercise the right of erasure and rectification, which is a challenge in a structure designed for immutability such as blockchain technology.

Linking the Smart-eID to the ID wallet

Another goal of the federal government is to provide identification data derived from the electronic identity card in the ID wallet with the help of a so-called basic ID. In August 2021, a series of events was held involving experts from various disciplines with the aim of developing solutions for linking the Smart-eID and the ID wallet ecosystem.

Given a review and assessment period of only two weeks and in the absence of auditable documents, I have made my initial assessment based on the guaranteed objectives of the standard data protection model. I have developed a preference for the use of the (Smart) eID infrastructure for identification and permanent storage of identification data, where responsibilities are already established, the level of security is known and a legal basis exists.

ID wallet app with driving licence verification

On 23 September 2021, the federal government surprisingly released the ID wallet app. However, the publication was not in the form of the pilot project linked to the Smart-eID (“Hotel Check-in”) on which I was consulted, but with driving licence verification as the first use case.

I was neither informed about this release date nor about the plans to integrate the driving licence in advance.

This app variant had to be withdrawn after only one week in order to avoid data misuse. Security researchers had identified ways to attack the system and deceive users about the true recipients of their data.

Summary assessment of the federal government's activities

As outlined above, the federal government's efforts to enable better usability of digital identities are distributed over several sub-projects that are running in parallel. In order to use digital administrative processes in the public and non-public sectors without media discontinuity, citizens need a secure and straightforward way to identify themselves online. The specifications for the implementation of such processes should primarily be designed by the state so that it does not have to submit to the rules of large technology corporations.

The basic prerequisites for an identification system are in place with the eID infrastructure, which is based on established technology. In my view, expansion of the hitherto rather limited possibilities for the use of electronic identities could also create a greater incentive to use them. Extensions and simplifications of the user interface also make sense if they ensure that the improvement in citizens' data sovereignty in the digital sphere that can be achieved with the eID also comes to fruition effectively.

In principle, I therefore welcome a digital usage system that keeps citizens' identification data and other attributes such as certificates under their own sovereignty, to use as they see fit. However, an approach in which data subjects themselves manage their data does not in itself lead to data sovereignty. It must also be ensured that they can make informed decisions about which data they disclose to whom, without any disadvantages. In addition, a clear set of rules is needed that identifies the controllers and their duties and systematically protects citizens. Technically, the solution must be sophisticated enough to be able to prevent fraud and data leakage. I will continue to advocate this in the consultation on the overall "Digital Identities" project.

6.20 The Security Clearance Act - A law with many question marks

The Security Clearance Act (SÜG) regulates a sub-area of national security and also contains special data protection regulations in this regard. In practice, it has become clear that there is still room for improvement in some areas. The current evaluation of the SÜG is a good opportunity for this.

Security clearance law is subject to the particular challenge of balancing the different interests of the state and the individual as far as possible. The security interests of the state are opposed by the right to informational self-determination of the individual, who must also disclose some highly personal data within the framework of the security check. In order to preserve confidential information and protect vital facilities for the state and its citizens from sabotage, government agencies screen everyone who is to be given access to such information and facilities in advance in a so-called security clearance check. In this process, various authorities collect and process extensive data from data subjects and their environment. Any data processing is an encroachment on the fundamental right to informational self-determination. Such interventions require clear limits and a legal basis. The SÜG therefore regulates the prerequisites and procedure for security clearance checks and contains special regulations on data protection.

In practice, however, it has been shown in the past that there are some regulatory gaps in the law, which sometimes pose major problems for the users of the law. In this section, I would therefore like to point out some gaps and inconsistencies in the SÜG by way of example.

The following questions must be answered by means of legal regulations:

1. Do data protection officers of a company have the right to inspect the security files kept there?

According to the current legal situation, data protection officers in public authorities have a right of inspection pursuant to Section 36 SÜG in conjunction with Sections 5 et seq. BDSG. At least according to its wording, this regulation does not directly apply to data protection officers in companies. In

my opinion, there is no reason to regulate the right of inspection differently here.

The ultimate responsibility for the content of the security files and the personal data stored and processed for this purpose lies with the management of the company concerned. In order to fulfil the data protection requirements in the area of the SÜG, the latter may (or must) appoint an in-house data protection officer. The legislation cannot have intended to make my authority the sole point of contact for companies and data subjects. The obligation to ensure proper data processing is made more difficult for companies if they cannot make use of a company data protection officer in the area of the SÜG.

I am therefore of the opinion that data protection officers must also have the right to inspect security files kept in companies. The legal situation here is not clear. A provision should therefore be included in the SÜG itself on the right of inspection of data protection officers in non-public bodies. In order to clarify the equal treatment of data protection officers in the public and non-public sectors, I recommend that the right of inspection of both types of data protection officers be regulated jointly in the SÜG.

2. Who is the correct addressee for a complaint in the non-public sector?

Section 36a(2) SÜG regulates my responsibility for data protection inspections of both public and non-public bodies, insofar as they carry out tasks under this Act. However, there is no clear regulation in the non-public area as to the addressee of my inspection results - especially in the case of complaints. An addition to Section 36a SÜG that regulates the addressee of the respective inspection results would be desirable here.

3. What measures are to be taken by the Federal Office for the Protection of the Constitution (BfV) in the case of a security check at the request of foreign agencies pursuant to Section 33 SÜG?

Section 12 SÜG regulates which measures are to be carried out for the different types of security clearance checks. What is not regulated, however, is what measures are to be taken if a review is carried out at the request of a foreign agency. In addition, further regulations on the handling of the personal data collected, such as provisions on destruction and erasure, are also required here.

4. On what basis can data be transferred in the context of the visit control procedure that frequently occurs in business?

Is consent to the transfer of data on the part of the data subject possible here?

According to the current legal situation, the transfer of personal data in the context of the so-called “visit control procedure” is not regulated by law. The visit control procedure is used when personnel with security clearance are to visit a place other than the employing company or government agency and access to classified information is required or possible.

Neither the SÜG nor the BDSG include regulations on conditions under which personal data may be transmitted to the organisation being visited or even which personal data are involved. Likewise, handling of the data by the receiving agency remains unregulated.

The data is currently passed on on the basis of consent given by the data subjects (Annex 19h to the Classified Information Manual of the Federal Ministry for Economic Affairs and Energy).

The problem here is that Section 36 of the SÜG declares Section 51(1) of the BDSG to be applicable *mutatis mutandis*. This regulates requirements for the quality of consent and its proof, insofar as data processing on the basis of consent is permitted by law. However, as mentioned above, there is no such regulation in the SÜG. The reference to Section 51 BDSG seems to fall short of the mark for the area of the SÜG. It seems more than questionable whether the requirement of consent authorised by law was actually the intention of the legislation. If reference should be made here solely to the requirements for consent and the obligation to provide evidence, this is certainly not clear.

Here, too, it would make sense to include a suitable provision in the SÜG itself for the visit control procedure. Alternatively, the reference to Section 51(1) BDSG could be limited to modalities and proof of consent, so that consent on the part of the data subjects would not be blocked because there is no provision in the SÜG.

I will explain the additions and changes to the SÜG that I believe are necessary to the new federal government and ask them to examine and possibly implement my suggestions.

It is then up to those in charge of the legislation!

I recommend that the company data protection officer's right to inspect the security files kept in the company, the addressee of a complaint in the non-public sector, the scope of the measures in security audits pursuant to Section 33 SÜG and the transmission of data as part of the so-called visit control procedure should be regulated in the SÜG.

6.21 Pilot project for “intelligent” video surveillance at Berlin Südkreuz station, 2nd part

The final report on the 2nd part of the project shows at best the initial steps towards the planned use; the software is far from meeting the requirements of use in the complex environment of a railway station. The project will continue until the end of 2021.

I already reported on the pilot project for intelligent video surveillance at Südkreuz station in Berlin in my 27th Activity Report (No. 9.3.3) and 28th Activity Report (No. 6.2). In the first part, Deutsche Bahn AG tested software for biometric facial recognition there, in conjunction with the federal police (see the Activity Reports mentioned above). In the second part, software from three different manufacturers was tested in autumn 2019 for the detection of various dangerous situations, tracking the positions of people or objects and retrograde evaluation of video data. In mid-May 2021, the test report (dated 23 November 2020) was brought to my attention. The result is that no software met the requirements, no more than promising approaches to solutions were found in several cases. As a reminder, the following situations were tested: “person lying on the ground”, e.g. a person who has fallen over and needs help; “entering defined areas”, e.g. people who are too close to the platform edge; “flows of people/crowds”, e.g. crowds forming in front of escalators; “counting people”, i.e. counting people in a defined area; and “objects left behind”, i.e. pieces of luggage that are left unattended for an extended period of time. These situations were tested with Deutsche Bahn AG taking the lead, while the federal police took the lead in testing the “tracking of positions” and “retrograde evaluation of video data”.

In the situations under the auspices of DB-AG, the false alarm rate was consistently too high, and in some cases situations were not recognised by the system. Only the visualisation of people flows and crowd formation worked well in all systems. “Tracking positions” could not be implemented at all by one manufacturer, the second

manufacturer could not track positions across cameras and the third manufacturer required extensive reconfiguration of the software to implement the requirements, which was found to be too extensive. As far as retrograde evaluation of the video data was concerned, none of the systems proved to be suitable for federal police use.

One of the basic conditions for the test was that it should not be possible to identify people on the basis of biometric features. The manufacturers therefore guaranteed that any biometric modules of the software were deactivated in advance. Some of the existing video cameras at Südkreuz station were used, the scenes were acted out by actors and each was recorded in a clearly marked area. This ensured that passers-by could avoid the areas and were not filmed involuntarily. The public was informed by means of signs and information in the press, and scientific support for this part of the project was provided by ITIS GmbH of the University of the Federal Armed Forces in Munich. The report ends with the recommendation to develop and test the video analysis technology further. The test is also to be extended to other software providers.

In my opinion, this poor test result should not be the basis for further, similarly elaborate tests, but should - at least at the present time - mean the end of such tests. Rather, the opportunity should be taken to increase station security through other measures.

However, the Minister of the Interior has already indicated in a press release from December 2020 that the tests will continue. According to the latest information, the tests for the second part of the project will continue until the end of 2021. I do not yet have any further details.

6.22 Eurojust, European Public Prosecutor's Office: New responsibilities

Criminal justice cooperation at the European level is becoming increasingly important. This is particularly true of recent legal acts relating to Eurojust and the European Public Prosecutor's Office. To ensure data protection in this area, I am involved in various committees at national and European level.

Eurojust

Eurojust is a body of the European Union that supports the judicial authorities of the Member States in cross-border cooperation. This concerns, for example, the areas of

combating terrorism, drugs and arms trafficking. As Eurojust itself is a European body, supervision lies with

the European Data Protection Supervisor (EDPS). My task, together with the data protection commissioners of the federal states, is to supervise the transfers of personal data by the German law enforcement authorities to Eurojust. I have checked, for example, whether there are secure channels of communication between Eurojust and the national agencies. I also held an information meeting with the German member of Eurojust, during which it was possible to clarify in particular questions about the specific functioning of Eurojust in the European multi-level system.

European Public Prosecutor's Office

The European Public Prosecutor's Office (EPPO) is a new institution at European level that started its work on 1 June 2021. The EPPO is responsible for offences against the financial interests of the Union and prosecutes offences against the EU budget. To this end, it may conduct investigations, take action for prosecution and exercise the functions of the public prosecutor's office before the competent courts of the Member States. Germany is one of the 22 Member States participating in the EPPO within the framework of greater cooperation. In its investigative work, the EPPO is authorised to make use of national law enforcement agencies, so that my supervisory activities primarily relate to compliance with data protection law by the federal law enforcement agencies concerned. Given the recent start of operations of the European body, I am also engaging with the data protection supervisory authorities of the participating Member States and the primary EDPS on the organisational design of the EPPO in the Member States and the clarification of open questions of competence. Overall, this is a new task within the scope of my supervisory responsibility.

Coordinated supervision of Eurojust and the European Public Prosecutor's Office (Coordinated Supervision Committee, CSC)

To ensure coordinated supervision of Eurojust and the EPPO in the EU, the members of the European supervisory authorities and the EDPS meet in the so-called Coordinated Supervision Committee (CSC). In this body, common approaches to cross-border supervisory issues are defined. I represent the German supervisory authorities together with two representatives of the data protection authorities of the federal states.

6.23 Cooperation with other supervisory bodies in the area of federal intelligence services

This year, I have intensified cooperation with the G10 Commission and the Parliamentary Control Panel in the

course of several talks at different levels and have set an important course for our future cooperation.

This year, I have continued the cooperation with the G10 Commission and the Parliamentary Control Panel (PKGr) that I started in recent years. To this end, a joint *jour fixe* with the G10 Commission took place at working level.

Cooperation with the PKGr was also further expanded after the inaugural visit of Mr Kiesewetter, the chair of the panel in the 19th legislative term, to my office in Bonn. The cooperative and encouraging discussion with Mr. Kiesewetter led to an exchange with the Permanent Representative, Mr. Schlattmann, and another meeting at working level. We want to continue this with the leaders of the 20th legislature. The intensification of these contacts is intended to set the course in advance for constructive future cooperation, which is of particular importance to me. In doing so, I would also like to take into account the amendments to the PKGr Act, which will come into force on 1 January 2022. In the future, the law provides for a closer exchange with the control bodies over the intelligence services at federal level (G10 Commission, BfDI and the newly created Independent Control Council), with the PKGr as the connecting element. I understand the amendment to the law not only as a legal mandate, but also as an opportunity to further expand and positively shape joint cooperation in order to take account of data protection with its continually increasing importance at this level, too.

6.24 Passenger name records (PNR) - Central questions remain unresolved

Proceedings are still pending before the European Court of Justice (ECJ) and the German courts to clarify the lawfulness of processing PNR data to combat terrorism and other serious crimes. In addition, the first figures on the use of abstract threat patterns in Germany are now available, which reinforce my doubts about their compatibility with fundamental rights.

I consider the extent of the processing of PNR data by police authorities to be disproportionate. I have already pointed this out repeatedly in previous reporting years (see 22nd AR No. 13.5.4; 26th AR No. 2.3.2; 27th AR No. 1.3; 28th AR No. 6.4; 29th AR No. 6.6).

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 and permanent basis for a period

of five years to allow for retrospective analysis. Germany has implemented the PNR Directive with the Passenger Name Record Act (FlugDaG).

In particular, the databases can be automatically compared with tracing databases, but also with previously created patterns. If a person meets the criteria of such a pattern (e.g. type of booking, chosen flight route, etc.), this is comparable to a hit when checking against a police database. The suspicion arises that the person concerned has committed - or will commit in the foreseeable future - one of the terrorist and other serious criminal offences mentioned in the FlugDaG. Individuals can thus become the focus of investigations by the Federal Criminal Police Office (BKA) and the state criminal police forces, customs, the federal police, the Federal and State Offices for the Protection of the Constitution, the Military Counter-Intelligence Service and the Federal Intelligence Service.

I, like my colleagues in Europe, doubt the positive conclusion of the EU Commission in its evaluation of the implementation of the PNR Directive, as I already made clear in the last reporting year (see 29th AR No. 6.6). The figures now available on the first two years of use of these patterns in Germany also cast considerable doubt on the proportionality of pattern matching.

During the first two years, moreover, the pattern-matching function was not able to further the legal aim of identifying individuals for whom there is factual evidence that they have committed a terrorism-related offence as defined by the FlugDaG or are likely to do so in the foreseeable future. In addition, the application of pattern matching on flights within the European Union (EU) is certainly not necessary for the implementation of the so-called PNR Directive ((EU) 2016/681). It will significantly increase the number of encroachments on fundamental rights, without any recognisable necessity.

At least since the **advisory opinion** of 26 July 2017 on the planned PNR agreement between Canada and the EU from the ECJ, it has become a matter of urgency to apply the ECJ's findings to the PNR Directive and the FlugDaG, too (see 28th AR No. 6.4). The ongoing applications for preliminary rulings before the ECJ by courts from various member states and lawsuits against airlines and the Passenger Information Unit at the BKA will provide further clarification on the compatibility of the PNR Directive and the FlugDaG with fundamental rights.

6.25 Agile project development

Large IT projects in the security service sector are becoming increasingly complex and dynamic, and development methods are constantly being adapted. The first projects are now being carried out with agile project management. The aim is to achieve flexibility, transparency and security for all parties involved. In order to arrive at executable software as early as possible in the development process, the design phase is reduced to a minimum and relies on agile project and software development. This does not have to be at odds with data protection.

Data protection guidelines must be observed in the development of IT systems. The goals and milestones must be defined and documented in such detail that sound data protection advice and control is possible. Otherwise, security authorities run the risk of having to revise or even reprogram parts of the IT system in a costly process due to complaints under Section 16 BDSG or orders under Section 69(2) BKAG.

The security authorities operate in the area of administration of state intervention that impinges on fundamental rights, with the corresponding legal reservations. Data protection requirements must be fully defined and robustly documented before the start of agile development. There is no room for negotiation with regard to this, as there is with the timing or budget, for example. For example, the project mandate must already clarify the concrete and detailed legal requirements within which the project can or must operate. Technical development goals must also be formulated and documented within the guidelines of data protection law.

Data protection requirements permeate the entire project development, from the objective of the project, through the development of a suitable data model and purpose-related data processing, to data storage, erasure and logging. In the development process, compliance with the development specifications and implementation of the technical requirements within the legal guidelines must be documented. This also includes proof that the traceability and comprehensibility of the software is guaranteed.

Times at which reports on the progress of development are prepared must be determined in advance. These can again be the subject of data protection advice.

Ultimately, there should be a technical description and documentation of the finished system which makes it possible to check the product for its admissibility under data protection law in full before it is used.

6.26 Personnel management system PVSplus: Data protection challenges that have not yet been solved

The introduction of the uniform personnel management system PVSplus into federal administration is associated with some as yet unresolved data protection challenges. I will be strengthening my advisory and monitoring activities in this area in the future.

For some years now, the federal administration has been tackling a major information technology project in the form of the “PVSplus personnel administration system”. The various personnel administration systems in the federal administration are to be consolidated on a large scale by means of a uniform information technology solution, which will be operated in future exclusively in the central computer centres of the Federal Information Technology Centre (ITZBund). The solution is based on the process of a large enterprise resource planning (ERP) provider.

So far, I have mainly offered advisory support within the scope of my supervisory activities, which has been actively requested in particular by the ITZBund, where PVSplus is being further developed for central deployment in the federal administration. Positive results of my consultations in the area of employee data protection included, for example, adjustments to pay slips. My advice has also enabled improvements to be made to the commissioned processing agreement.

At the same time, the data protection results achieved in this way over the years are still far from satisfactory. In particular, the software application used does not currently have sufficiently automated erasure routines to guarantee compliance with the legal erasure and retention requirements of the extremely sensitive personal data.

In addition to my advisory support for the project and product, I will also be focusing in future on targeted inspections of data processing via PVSplus at the federal authorities that use PVSplus for their personnel administration.

These “client authorities” should be aware: as long as PVSplus does not provide reliable automated erasure of personal data, compliance with the statutory erasure and retention requirements must be ensured by means of organisational measures.

7 Freedom of information

7.1 Committees

7.1.1 Conference of Freedom of Information Commissioners in Germany

In 2021, the Conference of Freedom of Information Commissioners of the Federal Government and the States (IFK) once again made some important contributions to current issues of transparency in government action.

The Conference aims to promote the right of access to official information and to campaign for further development of freedom of information. To this end, the IFK adopts resolutions which contain, for example, calls for changes in legal areas of freedom of information from governments at the federal and state levels. The IFK has a different chair every year and in 2021 it was the turn of the State Commissioner for Freedom of Information of Saxony-Anhalt. Due to the pandemic, the meetings took place as video conferences.

Three resolutions were adopted at the 40th Conference. The IFK demanded more transparency in the Office for the Protection of the Constitution, the introduction of official freedom of information officers in all public agencies and, as part of a position paper submitted to the newly elected Bundestag, the creation of a transparency law at the federal level.

The 41st conference also pursued the goal of giving freedom of information an even higher profile. Three resolutions were passed. The IFK called on the federal legislature to approve the Council of Europe's Tromsø Convention; this convention entered into force in 2009 and includes a general right of access to official documents of the public administration and minimum standards for processing access to information requests. In addition, there was a call for the advisory and supervisory powers under environmental information law in the federal states to be transferred to the State Freedom

of Information Commissioners. The IFK also called on the federal government to implement the EU Directive on the protection of whistle-blowers as soon as possible and to extend protection to whistle-blowers who report violations of national law.

Next year, Schleswig-Holstein will take over as chair of the IFK.

7.1.2 International Conference of Freedom of Information Commissioners

The International Conference of Freedom of Information Commissioners (ICIC) has elected a new executive committee for a three-year term.

Comisionada Presidente Blanca Lilia Ibarra from the National Institute for Transparency, Access to Information and Personal Data Protection of Mexico was elected as the first chair of the ICIC Executive Committee. In addition, candidates from Albania, Bermuda, Brazil, Chile, Kenya, South Africa and the United States were successfully appointed. The newly constituted executive committee took over business on 24 June 2021.

Following postponement of the 12th International Conference of Freedom of Information Commissioners, originally planned for Brazil in 2020, due to the pandemic, it was held in the form of various online events (webinars, workshops and meetings) from May 2021. This year's meeting of the commissioners took place on 23 and 24 June 2021 in the form of a video conference. In addition to reports on the state of freedom of information in the regions, the agenda included a resolution on the strategic priorities of the ICIC²² in the coming years and on the proactive publication of information in relation to the COVID-19 pandemic. The further development and orientation of the ICIC will be a task for the next few years according to the strategic plan.

²² More information about the ICIC's strategic plan:

<https://www.informationcommissioners.org/icic-signs-resolution-on-its-strategic-plan-for-the-next-three-years>

7.2 “Glyphosate” judgement - The publication of an opinion prepared by the authorities after access to information

Copyright does not preclude further dissemination of an officially prepared statement on the herbicide glyphosate if the authority has already published it as an official work. Further dissemination in the context of reporting on daily events was also permissible in the specific case.

The dispute over the publication of an opinion prepared by the Federal Institute for Risk Assessment (BfR) on the cancer risks of the herbicide glyphosate was resolved by Cologne Upper Regional Court (OLG Köln) on 12 May 2021 (ref: 6 U 146/20).

The Open Knowledge Foundation (OKF) had published the document without the BfR's consent in an editorial article on its website “Frag den Staat”. The BfR had taken legal action against this. However, Cologne Upper Regional Court rejected the authority's claim for injunctive relief in this regard. The court thereby confirmed the decision of the lower court (see 29th AR, No. 8.2.1).

The fact that the BfR's statement could in principle enjoy copyright protection was no longer in dispute before the OLG. According to the court, publication is nevertheless permissible for various reasons.

As an “official work” according to Section 5(2) of the Copyright Act (UrhG), the statement is exempt from copyright protection. The BfR had received more than 45,000 IFG applications and then decided itself, by means of a general decree published in the Federal Gazette, to make the document available to every applicant via the BfR website. The OLG assumed that the authority had thus published the work in the official interest for general consumption and had created an official work. Restrictive declarations and restrictions on access should not change this. The OLG also confirms a specific interest in dissemination - as is necessary according to the ruling of the Federal Court of Justice of 20 July 2006 (ref.: I ZR 185/03) - in the context of the high socio-political importance of the information, which concerns the effects of the plant protection product on the environment and health. On the other hand, the court leaves the question as to whether

the first time access granted to the information under the IFG is sufficient for the assumption that a public work was involved under Section 5(2) UrhG explicitly open.

The Foundation may also invoke Section 50 UrhG. According to this, public communication of works for “repor-

ting of daily events” is permitted to the extent required for that purpose. The court recognises that editorial reporting had taken place here. It concludes that the statement is not presented for its own sake, but appears editorially embedded in a larger context of critical reporting on the authority. The court does not consider the opinion as such or the non-issuance of the document to be the subject of the reporting, but ultimately the role of the BfR in connection with the (re-)authorisation of the plant protection product glyphosate. The defendant association is concerned both by the attempt to restrict access to information by means of copyright law, which it calls “censorship copyright”, and the danger posed by the weedkiller glyphosate. The content of the text enables the readers of the website to make their own assessment as to whether the accusations made in the report are justified - and if so, to what extent.

The court also considered the publication to be proportionate. In the underlying consideration, it had taken into account the fact that the report dealt with a topic that was of particular public interest and that an economic exploitation of the summary was out of the question.

The decision of the OLG Cologne is thus based on the circumstances of the specific case, in which the public authority itself made “official information” into an “official work” within the meaning of Section 5 UrhG by publishing it, and reporting on day-to-day events involving disclosure of the document was permissible. Beyond the individual case, the ruling of the OLG Cologne makes it clear that public authorities, at least, cannot invoke copyright law in a blanket and unrestricted manner to restrict the further publication and use of official information.

The appeal against the decision was not upheld. However, the decision is not yet legally binding, as an inadmissibility appeal has been filed with the Federal Supreme Court.

7.3 Open Government Partnership

Germany's 3rd National Action Plan as a member of the Open Government Partnership (OGP) was adopted. It contains numerous commitments to open government and administrative action, especially at the federal level.

The OGP is an international initiative to foster open government and administration. Among other things, the member states commit to promoting transparency, participation, cooperation and innovation in their respective countries. In order to fulfil this obligation, so-called “National Action Plans” (NAP) are described and laid down as projects involving “voluntary commitments”. In

addition to the federal and state governments, stakeholders in civil society are also involved in the development of the NAPs. The NAPs and the implementation of the commitments contained in them are evaluated by an independent body.

In the reporting year, the final report on the implementation of the 2nd NAP for the years 2019 to 2021 was adopted by the Federal Government. The 3rd NAP for the years 2021 to 2023 has already been adopted, which contains a total of fourteen voluntary commitments. In addition to the voluntary commitment to establish a web-based platform to make information on planning and approval procedures for major federal infrastructure projects in the transport sector publicly accessible, the intensification of the activities of the Competence Centre Open Data (CCOD) in the Federal Office of Administration is also included as a separate item, for example. The CCOD supports and advises the federal authorities on the provision of open data. The NAP envisages the long-term establishment of expert conferences and better knowledge transfer between the authorities, science, business, the federal states and civil society. The Federal Ministry of Justice and Consumer Protection is responsible for developing a concept for a federal legal information portal on which digital legal information is to be made available.

Three projects of the NAP are managed by federal states under their own responsibility. Hamburg has committed itself to the development of software products for the processing of digital participation procedures in the field of spatial planning and planning approval. North Rhine-Westphalia wants to create framework conditions for the provision of open data by public utilities and election data and - as a third state project - develop a state-wide participation portal together with Saxony. Two projects are being developed in cooperation between the federal government and individual federal states. The Federal Ministry of the Interior, Construction and Community (BMI) and the states of Baden-Württemberg and North Rhine-Westphalia are developing a platform on which open source projects can be listed and made available for public processing and further development. Together with the Hanseatic City of Bremen, the BMI also intends to set up a central national public procurement announcement service.

I expressly support the guiding principles and the goals of the OGP. In addition to further development of digitalisation, the aspects of transparency and open data should also be promoted in the future.

7.4 Format choice: Yes or No?

A right to choose the format of the provision of official information no longer exists if the information is already (fully) accessible in another format.

A petitioner asked me to mediate because he considered his right to access information to have been violated by the Federal Office for Information Security (BSI).

The subject of the information access request was the publication of the IT Basic Protection Compendium 2021 in a machine-readable format. During the conciliation procedure, the petitioner specified the subject matter of the application, namely that he wanted the document to be made available as an XML version. The BSI refused access to information with reference to Section 9(3) IFG, since a PDF version of the Basic Protection Compendium was available on the BSI website. The petitioner asked me to review whether an XML version should be made available to him.

The question of whether an applicant in an IFG procedure has a right to determine the (file) format in which the requested information is made available is repeatedly the subject of submissions.

The right to determine the “type of access to information” pursuant to Section 1(2) sentence 2 IFG also includes, in principle, the right to choose the file format (see 2nd AR on Freedom of Information, No. 4.14.3), according to which the petitioner would have had to be provided with the requested XML version.

In the present case, however, the BSI’s rejection of the application was nevertheless not a matter for objection, since the information in the XML version did not go beyond that in the PDF version. As far as my organisation was able to determine, there were only differences with regard to the additional metadata contained in the XML version.

There was therefore no (longer any) right to choose a format insofar as the requested information could already be obtained in another format in a reasonable manner from generally accessible sources. However, the decision would be different if the file formats had differences in content.

Regardless of this, I would welcome it if official information were provided in different formats, including from an open-data point of view.

7.5 Transparency in the legislative process

Increasing transparency in legislative procedures continues to be a declared goal of the federal government.

In November 2018, the agreement on increasing transparency in legislative procedures was adopted by the federal government. The Federal Chancellery surveyed all ministries on the status of implementation in autumn 2020. The result of this departmental survey shows some promising approaches. Many departments are already working actively and at an early stage with the stakeholders involved. The initiation of state and association participation in draft bills is increasingly (also) announced online.

The experience is usually positive.

On its website at www.bundesregierung.de, the federal government has set up pages on draft legislation and on participation. Links and references to planned “legal acts” of the federal ministries and the EU Commission are posted under “Legislative projects of the federal government”. Under “Participation at federal level”, ongoing and completed participation at federal level can be posted so that the public and expert groups have the opportunity to contribute their ideas, opinions or reactions on a case-by-case basis. The individual legislative and participation procedures can be found quickly and easily in this way. Legislative processes should become transparent and the participation of civil society be strengthened.

I welcome these efforts to strengthen transparency in the legislative process and strongly encourage further steps. Unfortunately, the legislative process suffers from completely unnecessary short deadlines for stakeholders outside the departmental circle, including the BfDI and in particular NGOs - as already mentioned - which thwart transparency because participation is only possible in theory. There must be a return to proper deadlines here.

7.6 Complaint against the BMVI for refusing access to information without reason

The Federal Ministry of Transport and Digital Infrastructure (BMVI) refused to release the email communication between Federal Minister Scheuer and the Head of Strategic Media Management without a viable legal justification. I formally objected to this position.

A petitioner asked the BMVI for access to information on the complete email correspondence between the Head

of Strategic Media Management of the BMVI and Federal Minister Scheuer regarding the publication of a press article on the so-called toll affair. The BMVI rejected the application with reference to the grounds for refusal under Section 3(1) point (g) IFG. In the BMVI's view, access to information was precluded by the ongoing proceedings of a parliamentary committee of enquiry. In its decision, the BMVI stated that the term “procedure” in the exception described above was comprehensive. The purpose of this norm is to protect the activities of the institutions that administer justice. According to Article 44 of the Basic Law, parliamentary investigation procedures fall under the third case group of Section 3(1) point (g) IFG. The committee of enquiry has a clear goal of clarification. According to the resolution of the Bundestag, the task of the committee is to investigate the events surrounding the infrastructure charge for passenger cars “from a contractual, legal and in particular a constitutional, budgetary and political point of view”. In doing so, it is required to take evidence that is deemed necessary for clarification of the facts and establishment of the truth. According to Section 17 of the Committee of Enquiry Act, the committee of enquiry comes to conclusions on the basis of its collection of evidence. In this respect, the requested emails were evidence of the ongoing committee of enquiry proceedings and had been sent to the committee in fulfilment of corresponding evidentiary resolutions.

The email history is only a small part of all the evidence. Publication without reference to the large amount of further evidence - a total of about one million pages of documents have reportedly been submitted to the investigative committee so far - could, it was argued, lead to a “distorted perception among the public and thus adversely affect or influence the investigators’ clarification of the facts and determination of the truth”.

In my opinion and contrary to the BMVI's view, there was no reason for refusing access to the information. In particular, there were no grounds for refusal under Section 3(1) point (g) IFG. This exclusion allows for the denial of access to information if the disclosure of the information may have an adverse effect on the conduct of ongoing judicial proceedings, a person's right to a fair trial or the conduct of criminal, misdemeanour or disciplinary investigations.

Contrary to the view of the BMVI, parliamentary enquiry procedures pursuant to Article 44 of the Basic Law are fundamentally not covered by Section 3(1) point (g) IFG.

Whereas in criminal proceedings the commission of a certain, clearly defined offence is examined by the court with regard to the individual guilt of a person, the proceedings of a committee of enquiry are about the cla-

riification of a factual situation for political purposes in the exercise of the control function of parliament. As an instrument and essential organ of parliamentary control, a committee of enquiry does not exercise judicial power, even if the procedural law of the committee borrows powers from criminal procedural law. Furthermore, a parliamentary committee of enquiry does not conduct any criminal, regulatory or disciplinary investigations and therefore does not fall under the third case group of Section 3(1) point (g) IFG.

The BMVI's reference to the fact that a committee, like a criminal court, has a mandate to clarify the facts of a case retrospectively and factually using means of criminal proceedings makes no difference. This line of argument also fails to recognise that a committee of enquiry is not an organ of criminal procedure, either in its constitutional organisation or in its constitutional role and monitoring function.

A justification for the denial of access to information was thus not ultimately apparent, and I objected to the refusal of access.

The BMVI emphatically rejected my complaint because, in its view, the prerequisite for a complaint - namely an objective legal violation of the Freedom of Information Act - had not been met. I still do not share the BMVI's repeated and unconvincing line of argument.

7.7 IFG - "Competition" for the book trade?

The rejection of an IFG application for electronic transmission of a book that was freely available from retail outlets was admissible.

The petitioner turned to the German National Library with his request for access to information. He requested electronic access to a book that was available at the time for purchase both directly from the publisher and freely in retail outlets. It was also possible to access it in the reading rooms of the German National Library.

The German National Library rejected the IFG application, citing Section 9(3) IFG. According to this regulation, access to information can be refused if the requested information can be obtained in a reasonable manner from generally accessible sources. Given the various options for buying the book or acquiring knowledge of its contents, I could understand the argument of the German National Library.

According to Section 4(2) of the German National Library Act (DNBG), the library's holdings are available to the general public in accordance with a user regulation.

However, according to Section 4(2) sentence 1 DNBG, use of the collections as well as the use of services of the library are generally subject to a fee. Whether this is a special and therefore overriding "regulation in other legal provisions on access to official information" within the meaning of Section 1(3) IFG could be left open in this case. This would also lead to a denial of the right of access to information under the IFG. The fact that the work in question was apparently protected by copyright - albeit already published - did not need to be considered in more detail either, as the rejection was already unobjectionable on the basis of Section 9(3) IFG.

The case exemplifies the fact that the book trade does not need to fear "competition" from the IFG as long as the works in question are not out of print.

7.8 Building Academy Foundation Board

The arguments for rejecting an application for access to documents on the establishment of the Federal Building Academy Foundation were not convincing.

Documents on the founding process for the Federal Building Academy Foundation were the subject of a mediation process. A petitioner requested from the Federal Ministry of the Interior, Construction and Community (BMI) access to documents relating to the drafting of the statutes of the Federal Building Academy Foundation. The petitioner also requested access to the expert opinion of an auditing company regarding the legal conception of the Foundation and to documents on the organisation and role of the office of the chair of the Foundation Board.

The BMI initially rejected the application with reference to Section 3(1) point (g) IFG because labour law proceedings in connection with the appointment procedure for the post of director had been concluded in the first instance, but an appeal on the merits of the case could still be filed. After I pointed this out in the conciliation procedure, this reason for exclusion was no longer cited, since Section 3(1) point (g) IFG only serves to protect ongoing court proceedings and not a (merely potential) legal remedy.

However, the refusal of access to information was also based on Section 4(1) IFG. The subject of protection under section 4(1) IFG is the official decision-making process. The BMI justified the rejection on the grounds of the decision-making process in the (new) appointment procedure for the founding director of the foundation, which had not yet been completed at that time, as all documents could have an impact on the appointment

procedure. Disclosure of the information would make objective staff selection more difficult or even prevent it.

In the blanket approach to all the information covered by the application, the reasons for the complete refusal of access to that information were not clear to me. In particular, the petitioner's IFG application focused on information about the preparation of the draft statutes and the legal conception of the foundation. I was not convinced that such discussions of legal issues could jeopardise the outcome of the staff selection process.

With regard to the report of the auditing firm, the BMI also refused access with reference to the grounds for exclusion under Section 4(1) IFG. Since the expert opinion was not preparatory work independent of the decision-making process, Section 4(1) sentence 2 IFG was not relevant. The justification is not valid in my view. Expert opinions are regularly incorporated into and precede the decision-making process. If, exceptionally, such a close link between the expert opinion and the decision-making process does exist, this requires a detailed justification, which the BMI was not able to provide clearly here. It was not adequately demonstrated that there was such a close link with the preparations for the decision that it could exclude the application of Section 4(1) sentence 2 IFG. It was therefore not apparent that the expert opinion had become part of the official decision-making process and directly served as preparation for the decision. This would have been the case in particular if the subject of the expert opinion, as submitted by the petitioner, had been (for the most part) assessments of the practical legal arrangements of the completed procedure for the establishment of the Building Academy Foundation.

The petitioner's application was also rejected in the opposition proceedings. Action is still pending in the matter, based (also) on a claim under press law. In any case, the expert opinion that is the subject of the application was made available to the petitioner after the conclusion of the renewed application procedure and the selection of a founding director.

7.9 Environmental Information Act

7.9.1 Ombudsperson function in environmental information law

My authority is now able to also exercise an oversight and ombudsperson role with regard to access to environmental information.

In March 2021, I was given responsibility for consultation and oversight for the Federal Environmental Information Act (UIG). In particular, my ombudsperson function, which previously existed only for the Freedom of Infor-

mation Act, was extended to the important area of environmental information law. Now anyone can appeal to the Federal Commissioner for Freedom of Information if they consider their right to access information under the Freedom of Information Act or the Federal Environmental Information Act has been violated. This is supported by extended oversight responsibilities for my organisation. The new responsibility results from an amendment to the UIG that came into force on 4 March 2021.

My long-standing request has been fulfilled with this advisory and supervisory responsibility for access to environmental information with regard to the federal public agencies. The importance of the Environmental Information Act as a basis for claims for access to information has grown not only against the background of climate change, which has become increasingly noticeable in recent years. Until now, if the authority receiving a request refused to make the information available, the only option open to applicants was to take time-consuming and costly legal action in the administrative courts.

7.9.2 UIG or IFG? A sometimes tricky question of demarcation

A public authority obliged to provide information must also consider and reinterpret a request made on the basis of the IFG from the perspective of the UIG if environmental information is the subject of the request.

A petitioner asked me to mediate in a request under the Freedom of Information Act (IFG) to the Physikalisch-Technische Bundesanstalt (PTB). A leak of the radioactive substance Krypton-85 had occurred on the premises of the PTB in Braunschweig. The incident constituted a significant occurrence within the meaning of the Radiation Protection Regulation (StrlSchV). An external expert organisation was commissioned to determine the cause of the incident. The petitioner's request was for the release of the report that had been prepared. The PTB refused access to the information. According to Section 109(3) StrlSchV, it was obliged to protect the results of the investigation of the incident from access by unauthorised persons. Section 109(3) StrlSchV constituted a confidentiality provision regulated by law within the meaning of Section 3 no. 4 IFG. Thus, there was no entitlement to access information on the report.

I still see a need for clarification here. The term "unauthorised person" is not defined in radiation protection law. However, the term is found in various standards of radiation protection law. In Section 109 StrlSchV, it is used to distinguish persons who hold a licence or authorisation in the area of application of radiation protection law. This could therefore also be a (mere) regulation of the internal procedures and obligations of

the radiation protection supervisor to ensure organisationally in his own area of responsibility that unauthorised persons cannot access the records in question. The regulation would not then exclude a claim to access official information under the IFG. It would not impose any obligation of secrecy, but would merely limit the group of persons who are allowed access to the documents.

Furthermore, the PTB justified the rejection of the application on the grounds that the expert report contained company and business secrets according to Section 6 IFG. The third party concerned did not give their consent when asked.

In the present situation, however, it seems obvious that the petitioner's request should be interpreted as a request for access to environmental information. The PTB has disputed this, pointing out that the test report deals exclusively with technical aspects of a defective component that caused the leakage of Krypton-85. Environmental information is not present in these purely technical issues, it was argued. This reasoning contradicted the argumentation regarding Section 109 StrlSchV. Whereas there the report is associated with the incident

and is attributed a relevance under radiation protection law, which is based on the emission of radiation, the report is considered completely separately from the emission event with regard to its quality as environmental information. However, the broad scope of application of the UIG could lead to the report being regarded as environmental information.

If this view were followed, the grounds for exclusion under Section 6 IFG, i.e. the existence of a business or trade secret, would not be relevant to the application of the UIG. Pursuant to Section 9(1) sentence 2 UIG, access to environmental information on emissions cannot be denied because disclosure would make trade or business secrets accessible (Section 9(1) sentence 1 no. 3 UIG). The petitioner can still take legal action against the PTB's objection decision. I will be monitoring the progress of these proceedings.

8 Inspections and advice

8.1 Mandatory inspections

The pandemic has made it very difficult in some cases to carry out the inspections required by law in the security sector and has delayed processing. As a result of the often high degree of confidentiality of the controlled contents, inspection by means of a written procedure or even as a remote event was often not possible. Nevertheless, I was able to fulfil my inspection role.

8.1.1 Inspections and complaints in relation to the Anti-Terror Filing System (ATD) and the Right-Wing Extremism Filing System (RED)

Inspection of the Federal Intelligence Service

The use of the ATD in the Federal Intelligence Service (BND) was the subject of my inspection in the reporting year 2018 (see 27th AR, No. 9.3.11), which I was able to conclude in 2021. As a result, several objections were raised, which I cannot elaborate on here due to the level of secrecy of the subject matter of the inspection. Some of my complaints related to the way the data is automatically stored, which in my opinion makes it considerably more difficult, if not impossible in some cases, to check the data history. This criticism also plays a significant role in other complaints (e.g. in the controls of the Federal Office for the Protection of the Constitution). In the past, I had only refrained from making complaints in this context because the Federal Ministry of the Interior, Construction and Community (BMI) had promised to remedy the situation by redesigning the filing system. This has not happened to date.

At the end of 2020, I started the regular compulsory inspection of the ATD in the BND. This was done under the pandemic-related restrictions with an attempt to carry out the inspection of BND data records and the justification for their storage exclusively by means of a written procedure. The comparatively high classification of the subject of this control and the documentation justifying the storage, which has to be treated in strict confidence, make this considerably more difficult than an inspec-

tion in person on the premises of the BND. This leads to major delays in the process. I intend to carry out my ATD inspection at the BND again in 2022, if the pandemic situation permits.

Inspection of the Federal Office for the Protection of the Constitution

Both the Anti-Terrorism Filing System (ATD) and the Right-Wing Extremism Filing System (RED) were inspected by me at the Federal Office for the Protection of the Constitution (BfV) in 2019 and each will be assessed by me in 2021 with an inspection report. In terms of content, there were several points raised in both inspections, none of which has been accepted by the Federal Ministry of the Interior (BMI) in an initial response to the inspection reports. The BMI has different views on these issues and on the legal assessment. I can only agree with this opinion in the case of one specific complaint where a false impression was created during the on-site inspection. Of the original five points I raised in relation to the ATD and three in relation to the RED, I have therefore dropped one objection for each. These inspections are now complete. However, I have already started the next compulsory inspection of the ATD and the RED at the BfV for the end of 2021. Of course, I do not expect that it has been possible to resolve all the points from the assessment in 2019 or that there has been enough time to improve all aspects of the arrangements I criticised. From my point of view, the criticism that I have repeatedly voiced publicly, even before the 2019 inspection, remains valid for both filing systems: ultimately, they require fundamental reorganisation or abolition.

Inspection of the Federal Office for the Military Counter-Intelligence Service

Regular checks on the use of the RED by the Federal Office for the Military Counter-Intelligence Service (BAMAD) were due in the reporting year 2021. This oversight, which was carried out exclusively by means

of a written procedure, was concluded in the same year without any objections.

Inspection of the Federal Criminal Police Office

In November 2020, I checked the lawfulness of the processing of personal data in the RED by the Federal Criminal Police Office (BKA). For technical reasons, there was a duplicate set of data saved in the RED at the time of the inspection. In the follow-up to the inspection, the BKA informed that this duplication had been resolved in the meantime. I have therefore refrained from making a complaint (see Section 16(2) sentence 2 BDSG). In all other respects, the evaluation completed at the beginning of 2021 revealed no grounds for objection. The inspection of data saved to the ATD and its use by the BKA could not be completed by the editorial deadline.

Inspection of the Customs Criminal Investigation Office

I carried out the compulsory ATD inspection at the Customs Criminal Investigation Office (ZKA) in July 2021. The subject of the audit was the storage of personal data initiated by the ZKA. I am pleased to say that the ZKA has taken up my recommendations from the last two inspections. The storage requirements were fully documented in all audited cases. This year's inspection therefore gave no cause for complaint once again.

Inspection of the Federal Police

In 2021 it was possible to complete the inspection of the RED at a selected office of the Federal Police (BPol), which started at the end of 2019. Additional requests for essential documents explained the longer audit period. Due to the filing system's level of classification, the details cannot be reported.

One complaint and several recommendations were made to remedy shortcomings in the documentation. As in past audits, it is again apparent that notice of my inspection has led to a thorough review of the filing system by the responsible body. In the process, a not inconsiderable percentage of records ready for erasure were identified.

The ATD inspection with the BPol, which started at the end of 2019, was completed in the course of the 2020 reporting year. Recommendations were made to remedy existing shortcomings in the documentation here, too.

It was not possible to complete the regular compulsory inspections of the ATD and the RED at the BPol for 2021 by the editorial deadline.

I continue to recommend legislation to abolish the anti-terrorism filing system and the right-wing extremism filing system in view of the fact that they have proven to be of little value.

8.1.2 Eurodac

In the reporting year 2020, I initiated an inspection in the area of police use of the European Dactyloscopy (Eurodac) database by the Federal Criminal Police Office (BKA). This was carried out exclusively in writing because of the pandemic. The inspection was concluded in 2021.

In my last Activity Reports, I have already provided information about previous compulsory checks on data processing in the Schengen Information System (SIS), the European Visa Information System (VIS) and the Eurodac European asylum system (see 27th AR No. 9.3.5 and 28th AR No. 6.7.1).

Information from the Eurodac asylum filing system used for the purpose of security and law enforcement may only be accessed by certain law enforcement authorities. The searches must also be necessary in the specific case for detection, prevention or prosecution of terrorist offences or other serious criminal offences. Strict conditions apply here. Accordingly, a Eurodac search may only be carried out if previous searches in the national fingerprint systems and in the VIS have not led to identification of the person concerned (so-called search cascade).

In one of the cases examined, Article 20(1) of the Eurodac Regulation was violated because the VIS search to be carried out beforehand was omitted. The explicit provision of the Eurodac Regulation does not currently allow this.

The investigative approach chosen may have been perfectly understandable from the point of view of the law enforcement authorities. However, it did not comply with the strict requirements of a Eurodac search under the legislation, by which I am bound as the supervisory authority. I have therefore issued a complaint to the Federal Criminal Police Office (BKA) pursuant to Section 16(2) sentence 1 BDSG.

In connection with this failure to carry out the VIS search, the Federal Criminal Police Office promised to raise the awareness of the corresponding department.

Since I also found in the course of my audit that documentation of the VIS searches had not been carried out adequately, I also drew attention to my previous recommendation on this subject (see 28th AR No. 6.7.1).

8.1.3 VIS

In the reporting year 2020, I initiated an inspection of police use of the Visa Information System (VIS) in the Financial Intelligence Unit (FIU). This was carried out exclusively in writing because of the pandemic. The inspection was concluded in 2021.

I have already provided information about previous mandatory checks on data processing in the European VIS in my recent activity reports (see 27th AR No. 9.3.5 and 28th AR No. 6.7.1).

Police authorities and intelligence services may consult data from the VIS if this is necessary in specific individual cases in order to prevent, detect or prosecute certain terrorist offences or other serious criminal offences.

Up to 31 March 2021, the FIU was part of the Customs Criminal Investigation Office and was thus designated as an authorised body in accordance with the notification. However, the FIU was not identified on the national list as an authorised organisational unit within the body with authorised access, as stipulated by Article 3(5) of the VIS Resolution in conjunction with Section 2(3) of the VISZG.

Since 1 April 2021, the FIU has been a separate directorate alongside the Customs Criminal Investigation Office due to a change in the law that came into force on that date. Since this change in status means that it is nominally no longer covered by the notification that is nevertheless required, I have issued a reminder for a subsequent notification, but have refrained from making any further objection, since it could be assumed that the FIU was authorised to retrieve this data.

My inspection of the FIU resulted in two complaints.

VIS searches were carried out even though the individuals concerned did not need a Schengen visa. There was insufficient verification and documentation of why it was assumed that the requirements of the VIS access decision had been met.

VIS data were also transmitted to third countries without the requirements of the VIS access decision being met. In addition, not all national transmission requirements were checked, identified and documented.

In its response, the Federal Ministry of Finance (BMF), as the legal and technical supervisor of the FIU, promised to address the points to which I objected and to

review the corresponding instructions. Arrangements are also to be made for inclusion on the list of bodies authorised to retrieve the data.

8.1.4 Inspection of the data retrievals in the INZOLL customs investigation information system

Police databases allow a great deal of insight into sensitive personal data with little effort. It is therefore all the more important that searches of these systems only take place within the scope of official necessity. This was the subject of my recent inspection of the Customs Investigation Service.

When the new Customs Investigation Service Act (ZFdG) came into force in April 2021, I was commissioned to carry out extensive compulsory checks on data processing in the Customs Investigation Service as part of my activities. I completed this assignment in August with an inspection at the Customs Criminal Investigation Office (ZKA) in Cologne. The subject of my inspection was the access to data in the information system of the Customs Investigation Service (INZOLL) by employees of the ZKA. I focused on the personal data accessed via a search screen.

With a carefully selected sample, it was possible for me to obtain an interdepartmental and cross-working group insight into the searches completed with the reasons given for them and to establish the necessary connection between the respective processing procedure and the search in the database.

Overall, I was satisfied with the results of the ZKA inspection and I could not detect any unauthorised searches. Only for one search was the file reference missing, which meant that I could not complete the audit of this process. Despite the good results of the inspection, I have made recommendations to the ZKA to improve both the workflow of employees during searches and the INZOLL user management. There should be more restrictions on access to the system in future, for example, and an optimal process should be established to regulate workflows in relation to INZOLL access in the event of personnel changes. Furthermore, I consider it essential to provide the employees of the Customs Investigation Service with more intensive training in handling searches, including detailed instructions and training to eliminate uncertainties relating to justifications for search requests and to documentation and file management.

I should mention here that the successful inspection process, despite the pandemic-related restrictions, is also due to the good preparation and cooperation of the ZKA.

8.1.5 Schengen Information System

In the reporting year 2020, I initiated an inspection in the area of police use of the Schengen Information System (SIS) in the Customs Criminal Investigation Office (ZKA). Due to the pandemic situation, this inspection was carried out as a purely written process and was concluded in 2021.

I have already provided information on previous mandatory checks on data processing in the SIS in my last three activity reports (see 27th AR No. 9.3.5, 28th AR No. 6.7.1, 29th AR No. 9.5.1). The police and judicial authorities of the Member States of the Schengen area record searches for individuals and objects and entry and residence bans in the SIS (for further checks and information on SIS II, see also No. 8.2.7).

My inspection of the ZKA did not reveal any significant data protection shortcomings, and I did not have to issue any objections. However, my inspection report contains two recommendations concerning matters related to tendering procedures (documentation and necessity of certain measures).

Cross-references:

8.2.7 Data protection supervision and advice in respect of the Federal Office for the Protection of the Constitution (BfV)

8.2 Other inspections

8.2.1 Questionnaire survey of data protection officers in job centres

I conducted a questionnaire survey at 22 job centres on the organisational position of data protection officers.

According to Art. 37(1) GDPR, job centres as public bodies are obliged to appoint a data protection officer. The data protection officer has a crucial position within the organisation in ensuring compliance with data protection regulations. The position and tasks are regulated in the GDPR and the Federal Data Protection Act (BDSG).

The aim was to review the organisation of job centres with regard to the position and fulfilment of the role of data protection officer. Of particular interest was the extent to which data protection officers are free to fulfil their tasks properly, whether they can act independently of instructions, whether there are any conflicts of interest and how cooperation and support is provided by the organisation. With regard to the fulfilment of their role, there were questions about whether data protection officers carry out structured audits of the various areas

of activity and the other ways in which monitoring is carried out and the advisory role is fulfilled.

My inspection revealed that in many cases data protection officers have not been released from other duties to a sufficient extent. In twenty cases, I therefore recommended freeing up more of their time. I consider a complete exemption from other work to be necessary when the number of employees reaches 500, otherwise it is not possible to fulfil the tasks properly.

There were also shortcomings in the area of deputisation during absences. In my opinion, it is part of the proper performance of the role and a duty of support for the centre to ensure there is a deputy in place in the event of absence. How the centre arranges this, however, is basically up to the organisation itself. I recommend appointing a permanent deputy who has at least a basic knowledge of data protection law, as this is the only way to ensure uninterrupted completion of the work even in the case of longer absences. In order to ensure continuous representation, eight of the job centres inspected were recommended to change their regulations on the deputisation for the data protection officer.

There were further complaints in the area of the data protection officers' monitoring activities. They are obliged to monitor compliance with data protection regulations. Only through comprehensive, structured monitoring activities which cover every business area of the job centre at regular intervals is it possible to maintain a high level of data protection. In eight cases, I recommended that an annual monitoring plan and corresponding monitoring reports be prepared. This is to ensure that regular checks are actually carried out within the job centre and that the results of the checks are accessible to the data controller. In this way, complaints can be rectified promptly by the controller.

In the follow-up to the written inspection, I became aware of several cases in which differences arose between the management of job centres and the data protection officers regarding their position and the performance of their tasks. I will therefore continue to monitor these points.

8.2.2 Case processing system of the Federal Criminal Police Office

The Federal Criminal Police Office (BKA) processes a great deal of personal data in its case processing system (VBS) every day. This information system still does not comply with data protection law. Elimination of the data protection problems I have identified is slow.

In the reporting year 2019, I objected to the VBS of the BKA because of several serious data protection violations

(see 28th AR No. 6.7.3). I criticised the lengthy process involved in eliminating the data protection violations I had identified in my last Activity Report (see 29th AR No. 9.5.3). On several occasions I have asked the Federal Ministry of the Interior, Construction and Community (BMI) to send me a schedule and action plan indicating how and when the BKA intends to eliminate the data protection violations I have identified. My request has not been met so far. The BMI points out that the announced reorganisation of documentation and file management in the BKA is a very complex project due to the overlaps and compatibility requirements with the electronic files under the E-Government Act (EGovG) and the electronic files in criminal cases. The future system of documentation and file management would have to meet the legal provisions and the various professional requirements in the BKA. Until the necessary measures are implemented, the skills of BKA employees are reportedly being further strengthened in the area of documentation and file management, and procedural processes, with regard to the segregation check for example, are being further optimised. A concept for the further development of the VBS is being developed.

I certainly recognise the complexity of the project. In view of this, I offered to advise the BKA on addressing problematic situations under data protection law in connection with the VBS in the form of a joint workshop. Given the considerable data protection problems, however, I expect the reorientation of the VBS to be a priority in the BKA. I found the first joint workshop, which took place at the beginning of December 2021, to be constructive and purposeful.

8.2.3 First order issued to the BKA

I made first use of my authority to issue orders under Section 69 (2) of the Federal Criminal Police Office Act (BKAG) in connection with a case of excessively long storage of data. The BKA has appealed against it.

The petitioner had already contacted me several years ago because a security check on him had not been successful. The Federal Criminal Police Office (BKA) did not provide him with any information. My review had shown that he had been on file with the police for several decades and with the BKA since 1998 as a so-called contact and associate. The legal basis for storage of the data is Section 483(1) sentence 1 of the Code of Criminal Procedure (StPO). According to this, the law enforcement agency may keep personal data in a criminal proceedings file “insofar as this is necessary for the purposes of the criminal proceedings”. Unfortunately, interpretation of this wording is extremely broad. In this regard, the Federal Constitutional Court has ruled that the storage of data about third parties in criminal proceedings requires

a specific individual proximity of the person concerned to the danger or criminal offence under investigation (see BVerfG, judgement of 20 April 2016, BVerfGE 141, 220 (274 f. marginal no. 116)). Since 2018, this has been formulated in a very similar way in the BKAG (Section 19(1) no. 3). Such limitations must also be taken into account for files covered by the StPO for reasons of proportionality in a constitutional interpretation, especially when such a long period of time is involved. Such proximity or similar involvement could not be documented by the BKA over an extended period, so that storage of the data about the contact and associate concerned is, in my opinion, disproportionate.

The petitioner’s request for information from the BKA was rejected with reference to the grounds for refusing information pursuant to Section 57(4) in conjunction with Section 56(2) BDSG. However, in my review I came to the conclusion that the petitioner was entitled to the information. The BKA had not given me any viable reasons according to which the fulfilment of its role and the safety of the public would be endangered by the provision of the information.

Against this background, I objected to the storage of information indicating that the petitioner was a contact and associate and pointing out the failure to provide information pursuant to Section 16(2) BDSG. The petitioner himself had already taken action against the BKA for release of information and erasure of his data. My complaint was rejected by the Federal Ministry of the Interior, Construction and Community (BMI) as the supervisory authority of the BKA. Pursuant to Section 69(2) BKAG, I have therefore now instructed the BKA to block the petitioner’s data record, to provide him with the information and to erase the data on conclusion of his legal action. The BMI disputes my competence to order erasure of the data and in this respect refers to the legal justification for the BKAG. In my view, however, the BKAG must comply with European law on this point. The JHA Directive explicitly provides for these powers for national supervisory authorities in Art. 47(2) point (b) (“in particular by ordering the rectification or erasure of personal data”). The BKA has filed a complaint against my order. A decision has not yet been made.

8.2.4 Radio cell database of the Federal Criminal Police Office

According to established case law of the Federal Constitutional Court (BVerfG), certain intensive encroachments on fundamental rights are admissible only for the protection of certain legal interests or only above certain levels of suspicion or danger. Corresponding intervention thresholds are to be guaranteed by statutory regulation (BVerfGE 120, 274 [326 f.]). This consti-

tutional postulate has been repeatedly undermined by the Federal Criminal Police Office (BKA). There is no appropriate legal basis for the operation of a database for the comparison of radio cell data.

In the reporting period of the 27th Activity Report, I objected to a filing system in which the BKA stored data from radio cell searches from a large number of proceedings in various federal states (see 27th

AR No. 9.3.6.2). In this filing system, the BKA matched personal data that the law enforcement agencies at the federal and state levels had collected through radio cell searches. The filing system was based on the general clause in Section 7 BKAG (old version) (Role of the central office). However, particularly intrusive data processing requires a specific legal basis. The Federal Constitutional Court demands clear and proportionate regulations for measures involving intensive intervention. The greater the encroachment on fundamental rights, the more precisely the legislation must regulate the preconditions and thresholds of encroachment. The constitutional requirements to be placed on the factual limitation of the respective power of intervention depend above all on the type and severity of the encroachment on fundamental rights. In particular, the intensity and scope of the encroachment are determining factors and must be linked to certain thresholds for intervention. Crucial here is whether the data subjects themselves have given cause for the intervention (cf. BVerfGE 100, 313, 376; 115, 320, 347; 109, 279, 353).

In this respect, the general clause of Section 7 BKAG (old version) only has the function of linking and coordinating information. The provision cannot justify more serious encroachments on fundamental rights because it is too broad and too sweeping (see also Bäckert, *Terrorismusabwehr durch das Bundeskriminalamt*, 2009, p. 22). I now see this view confirmed in the decision of the Federal Constitutional Court of 27 May 2020 (BVerfGE 155, 119). Here the court stated that the Federal Criminal Police Office, as a central agency, is essentially limited to performing coordination tasks (marginal 209).

There is no recourse to Section 16(1) and (4) BKAG here either. Section 16(1) BKAG authorises the BKA to process data that it has collected in connection with the fulfilment of a specific statutory task or for the fulfilment of another task. In the present case, however, the (initial) collection of the radio cell data by the BKA itself has no legal basis. Above all, however, Section 16(1) BKAG is a basic provision that is intended to enable the BKA to process personal data in order to complete its work. In this respect, the provision is subject to the same objections in the present context as Section 7(1) BKAG (old version).

I was therefore very surprised to learn that the BKA has already been operating a database for the storage and comparison of radio cell data since 2019; information which, incidentally, I was given only after repeated enquiries. I took this as an opportunity to carry out an inspection. As of 6 September 2021, the database contained 99,880,125 records. In line with the court ruling cited above, such intensive encroachments on the fundamental rights of data subjects cannot be based on Section 7(1) in conjunction with Section 2(1) and (2) BKAG (old version) nor on section 483(1) of the Code of Criminal Procedure. In the absence of an adequate legal basis, the data storage and comparison in the database violate the legal reservation and are thus unlawful. I objected to them as such. The Federal Ministry of the Interior and Community and the Federal Criminal Police Office have opposed my view.

8.2.5 Processing of identification data by the Federal Criminal Police Office in INPOL-Z

In 2011, I inspected the storage of identification data by the Federal Criminal Police Office (BKA) in the nationwide central police information system (INPOL-Z) and recommended improvements (see 24th AR No. 7.4.3). I reviewed the current status of the cleansing process in a consultation and monitoring visit.

The BKA operates the nationwide INPOL-Z central police information system. Identification data, such as fingerprints, are stored in its so-called “E-Group”. The responsibility for this data under data protection law lies with the police authorities of the federal states, which store them in the system.

Originally, the BKA had continued to store these data from the state police forces even after the state in question had erased them. This procedure was subsequently changed by the BKA and storage of identification data continued if it had its own findings that justified further storage. During my review of this continued storage in 2011, I came to the conclusion that it is lawful only if it is based on a written, documented forecast decision on further storage (so-called negative forecast) (see 24th AR No. 7.4.3).

Negative forecasts

In a recent review of the implementation of my requirements in this regard, I found that in some cases the necessary negative forecasts were not in place. For this purpose, I examined samples of selected cases in which the BKA had continued to store data that had been discontinued by a state authority and had not been needed in the meantime.

Even before the inspection, the BKA informed me that a written, documented forecast decision had not been made specifically for the identification data in any of the cases, even though the BKA Act (BKAG) requires a specific negative forecast for identification data (Section 16(5) no. 2 point (a)). On site, I therefore checked for a general negative forecast in accordance with Sections 18, 19 BKAG, which corresponds almost word-for-word to the special regulation according to Section 16(5) no. 2 point (a). From a data protection point of view, I agree that for a forecast decision on the identification data, reference is made to the general documentation for Sections 18, 19 BKAG. In some cases, however, the negative forecast was limited simply to a repetition of the wording of the law. In fact, there is therefore a lack of documented forecast decisions, and I have objected to these cases.



I have already commented on the requirements for a so-called negative forecast in previous activity reports (see 26th AR No. 10.3.2). In the forecast decision, the expectation of criminal proceedings against a data subject must be documented in writing so that it can be reviewed in full in court. If this documentation is missing, storage of the data is illegal.

Current status of the identification data erasure and cleansing process

The function of “erasure with transfer of ownership” has been implemented in INPOL-Z. This allows an E-Group to be offered to another state for continued storage under its own responsibility. In my view, it is now technically impossible for a transfer to take place “against the will” of a potential new owner.

As a consequence of my inspection in 2011, the function “identification by means of FastID” was also introduced in INPOL. I had suggested a function of this sort at the time on the basis of my inspection. In this way, an INPOL participant can “take ownership” of the data stored in the E-Group resulting from an identification procedure by simply scanning four fingers and matching them against the AFIS fingerprint database. In the case of a hit, only a restricted data set is saved, to which the E-Group of the other state “surrendering ownership” is later appended. With this new function, further identification procedures can be dispensed with and the principle of data economy can be taken into account. In addition, an automated erasure procedure came into operation at the end of 2020.

I have no fundamental data protection concerns about the erasure and cleansing process. On a positive note, I would like to mention that more than 4.5 million E-Groups have already been erased, for which the BKA had assumed ownership from the federal states without a negative forecast (see 24th AR No. 7.4.3). The 70,000 E-Groups still remaining in the BKA are currently under review. I have asked the BKA to cleanse the existing database by 31 December 2022.

Structural testing of INPOL applications

In INPOL-Z, first and last names are stored in a separate area, the so-called P-Group. Aliases are also stored separately, namely in the so-called A-Group. Third parties have expressed to me the fear that these two areas (or groups) could possibly be linked in such a way that an individual would be falsely attributed with the “criminal career” of another person. I have therefore taken this information as an opportunity to examine these areas in INPOL-Z in the BKA from a structural point of view. My inspection revealed that this fear is unfounded.

I also checked other areas, namely the E-Groups and D-Groups, in INPOL-Z. Again, I could not find any incorrect links between these groups.

Identification data storage in relation to administrative offences

At the request of one of the state data protection authorities, I also examined cases in which identification procedures were carried out in relation to an administrative offence and the data were then stored in INPOL-Z. Inspection of the state data records does not fall within my area of responsibility, but the examination of structural issues in INPOL does.

I do not see any legal basis for the storage of identification data in INPOL-Z that has been collected in relation to administrative offences. The law only allows data to be stored in relation to persons accused and suspects of a criminal offence for whom negative forecasts are set out in addition.

I have therefore recommended to the BKA, as the agency responsible for compliance with the INPOL regulations according to Section 31(1) BKAG, to ensure in future that storage of these data is no longer technically possible.

Overall, the inspection visit was extremely cooperative and positive. I particularly welcome the fact that the BKA has asked me to organise a joint workshop on the forecast decisions required by law so that pressing questions in this area can be discussed and clarified in more depth.

I asked the BMI to comment on my report on the consultation and inspection visit shortly before the editorial deadline, which is why no statement has yet been made.

8.2.6 Data protection supervision and advice in respect of the Federal Office for the Military Counter-Intelligence Service (BAMAD)

At the BAMAD, I carried out the mandatory inspection of data processing in connection with alerts in the second generation Schengen Information System (SIS II) in the reporting year. Furthermore, I have started my inspection of data processing in the area of observation.

Inspection of discreet alerts in the SIS II at BAMAD

In the third quarter of 2021, I carried out checks on discreet alerts in the SIS II at BAMAD (for further checks and information about SIS II, see No. 8.1.5 above). BAMAD may initiate alerts in the SIS II if the information to be obtained in this way is necessary to avert a significant threat posed by the person concerned or other significant threats to the security of the state. During my consultation and inspection visit, I did not find any matters of concern. Nevertheless, I have made practical recommendations which concern in particular the implementation or adaptation of process flows and specifications for erasure of alerts. Furthermore, I have pointed out to BAMAD that effective data protection control must also be ensured in the coronavirus pandemic and in ongoing cases with a special need for secrecy. Preparing for the inspection had been difficult for me, as BAMAD had refused for reasons of secrecy to send documentation for a purely written inspection, which I had favoured. But I am confident that such frictions can be avoided in the future. A positive aspect is BAMAD's prompt response to my inspection report and the assurance that my suggestions for improvement will be implemented in the short term.

Inspection of data processing in the field of observation

In autumn 2021, I carried out an inspection in the area of observation at BAMAD and found that a further inspection date was necessary due to the volume of data to be checked. The technological possibilities of secretly observing individuals and objects are constantly developing and the acquisition and use of data by means of observation are a serious encroachment on the fundamental rights of data subjects. For this reason, I felt compelled to carry out a detailed examination of compliance with data protection regulations at BAMAD and the Federal Office for the Protection of the Constitution (see No. 8.2.7 below). My focus in this type of inspection is on checking that the collection of data in the context of the observation carried out is actually appropriate and

proportionate in the individual case, that storage periods are being complied with and, where appropriate, that duplicate file-keeping is avoided. For reasons of secrecy and the continuation of my oversight, I cannot go into further detail here. I will report on the results of my inspection.

Cross-references:

8.1.5 Schengen Information System; 8.2.7 Data protection supervision and advice in respect of the Federal Office for the Protection of the Constitution (BfV)

8.2.7 Data protection supervision and advice in respect of the Federal Office for the Protection of the Constitution (BfV)

At the BfV, I checked data processing in the area of observation in the reporting year and continued with the follow-up of the mandatory checks already carried out in 2020 regarding data processing in connection with alerts in the Schengen Information System of the 2nd generation (SIS II) and searches in the Visa Information System (VIS). I have acted in an advisory capacity for some planned projects and will continue the interaction that has begun in the coming year. I was also able to achieve pleasing results in consultations on the future responses of the BfV to requests for information.

Interfaces between the Financial Intelligence Unit (FIU) and BfV

If there is suspicion of money laundering in connection with the financing of terrorism or extremism, the cases are reported to the BfV via the FIU. The establishment of partially automated interfaces is intended to improve the transmission paths. The legal foundations are already in place in the Money Laundering Act. Due to the number of suspicious activity reports and in order to speed up processing and clarification, an improvement of the transmission channels also seems to make sense from my point of view. However, some questions have arisen about the exact arrangements, which the BfV has not yet been able to answer conclusively. It is still unclear exactly how processing by the BfV will take place, how long certain types of reports will be stored and which access options the BfV will be given for the FIU's database. I will continue to monitor this inter-agency project.

Inspection of searches in the VIS

The inspection of the BfV's searches in the VIS, which began at the beginning of 2020 (see 29th AR No. 9.5.1), has not yet been completed. In this context, I have called for some improvements and adjustments to the processes and documentation, some of which have already been made. With regard to the other shortcomings identified and the erasure of data requested, a statement

from the BfV was received shortly before the editorial deadline and is now being examined.

Inspection of data processing in the field of observation

In autumn 2021, my authority carried out an inspection in the area of observation by the BfV. This area was last inspected in 2006 (see 21st AR No. 5.5.2). Particularly in view of the constantly changing technological possibilities, I considered another inspection to be appropriate. New thematic areas were highlighted for the first time. In the course of my consultation and inspection visit, I was pleased to find that the announcement of my inspection had already brought about a fundamental revision of some essential processes in the area of observation, thereby making them more data protection-friendly. Other weaknesses relating to data protection law were also identified during the inspection which the BfV had already agreed to remedy or improve in the final meeting. For reasons of confidentiality, it is not possible to give a more detailed account of this. The inspection report is being finalised at the time of going to press.

Integrated Document Management System

In future, a uniform document management system (integrated DMS) is to be introduced for the Federal Office for the Protection of the Constitution (BfV and all state offices for the protection of the constitution) and the Federal Office for the Military Counter-Intelligence Service (BAMAD), which will ensure largely consistent case processing and interface connection for all participating authorities. The way in which documents are processed still varies greatly from one authority to the next, and significant improvements in cooperation are expected with the integrated DMS.

In this context, I acted in an advisory capacity to the BfV in 2021, while also maintaining close contact with colleagues from the data protection authorities of the federal states. The data protection classification of the integrated DMS was of particular importance here and will continue to be crucial in the future. Joint consultation on this major BfV project will also be necessary in the coming year.

Inspection of discreet alerts in the SIS II at the BfV

In the reporting year 2020, I checked discreet alerts in the SIS II at the BfV (see 29th AR No. 9.5.1; for further checks and information on SIS II, see No. 8.1.5 above). Due to the pandemic-related restrictions, I did not receive the BfV's response to my inspection report until spring 2021. Some data protection shortcomings were remedied and suggestions for improvement were implemented, but there is still a disagreement about the scope of data exchanged between the participating authorities

that is permissible under the SIS regulations in European law. A reply to my revised statement was not received before going to press. I expect further constructive interaction, which will result in necessary adjustments to the data processing.

Exercise of discretion by the BfV in the context of a claim for information under Section 15(1) of the Federal Protection of the Constitution Act (BVerfSchG)

The right to information about personal data stored by the BfV, which is regulated by Section 15(1) BVerfSchG, is a fundamental right of inspection of the data subject vis-à-vis the BfV. It is a prerequisite for the effective exercise of other rights, in particular rectification, restriction of processing and erasure of personal data.

Pursuant to Section 15(1) sentence 2 BVerfSchG, the right to information applies not only to data specifically assigned to the applicant in a so-called personal file, but also to data in files that are not exclusively personal, i.e. administration files. According to the wording of the law, however, the duty to provide information is limited to "data that can be found via storage pursuant to Section 10(1)", i.e. by means of a stored record of locations in the Intelligence Information System (NADIS), the central filing system of the Office for the Protection of the Constitution.

The Upper Administrative Court (OVG) of North Rhine-Westphalia (NRW) (judgement of 31 July 2019, ref. 16 A-1009/14) and most recently the BVerwG (decision of 28 July 2020, ref. 6 B-61/19) have ruled on the question of whether the BfV must take account of discretionary considerations in cases under section 15(1) sentence 2 BVerfSchG and if so, how.

According to the BVerwG, it is not sufficient when exercising discretion merely to take as the basis the search options in the electronic file system and the individual steps leading up to the provision of information. Rather, the administrative effort required in the individual case must be estimated, i.e. as a minimum, it must be determined how many file items will be found in a search for the name of the person filing the application. Only from this hit rate can a conclusion be drawn about the actual administrative effort.

On the basis of these two decisions, the BfV informed all persons submitting applications that fall within the scope of its exercise of discretion how many file items were found in a search for their names in administrative files. There was no further explanation of how this information should be interpreted, however. The BfV merely pointed out in a general way that its electronic file system cannot determine whether the search term is actually a

person's name and whether the information found really concerns the person making the application.

The technical circumstances mean that each hit has to be viewed individually and an identity check has to be carried out, with the result that the BfV regularly refused to provide further information in view of the large number of hits and the resulting disproportionate administrative effort. This blanket statement has understandably led to irritation among applicants. In order to get an idea of the technical conditions myself, I made a consultation and inspection visit to the BfV in the third quarter of this year. This confirmed the administrative burden described by the BfV. Subsequently, I submitted to the BfV proposed wording for an information notice, which sets out the technical requirements for searching the electronic filing system and the associated administrative burden in a more transparent way and is thus altogether more citizen-friendly.

I am therefore pleased that the BfV has essentially promised to adopt my proposed wording in the future. In addition, I am in discussion with the BfV about other procedural changes that might reduce the administrative burden in order to be able to provide material feedback to data subjects in individual cases.

Cross-references:

8.1.5 Schengen Information System

8.2.8 Inspections relating to the Security Clearance Act - A lot of bad practice and a bit of best practice

In mid-2020, I established a stand-alone unit for data protection oversight of security clearance procedures. So in 2021, despite COVID-19, I was able to carry out more checks than in the past. The results show that certain errors are found in almost all the checks, but there are also some bright spots.

During the reporting period, I inspected four commercial enterprises and eight public authorities to ensure that they complied with the data protection provisions of the Security Clearance Act (SÜG).



Under this law, all persons who have access to classified federal information (information requiring secrecy) or vital or defence information at their place of work in the public service or a private company are subject to clearance checks. A whole range of personal data is collected and processed in this connection.

The authorities inspected were

- the Federal Financial Supervisory Authority
- the Directorate-General for Waterways and Shipping
- the Sankt Augustin Federal Police Headquarters
- the German Patent and Trade Mark Office
- the Institute for Federal Real Estate
- the Federal Cartel Office
- the Federal Office of Civil Protection and Disaster Assistance
- the Federal Office for the Military Counter-Intelligence Service.

Of the businesses inspected, two are active in the field of security and one in the field of building cleaning. The fourth business is a critical infrastructure operator.

One of these inspections was a follow-up check. The deficiencies that I had already identified in the company in question in 2017 (see 27th AR No. 9.3.13) had unfortunately not been completely remedied. I have once again identified several significant violations of data protection law and have therefore submitted a complaint to the Federal Ministry of

Economic Affairs and Energy, which supervises the company with regard to confidentiality.

There was also cause for complaint among the authorities inspected. These were addressed to the Federal Ministry of the Interior, Construction and Community (BMI), among others. The background to this was the discovery of data protection violations in the Federal Office of Civil Protection and Disaster Assistance. Another complaint against the Federal Ministry of the Interior was made following a submission by a member of the public and concerned data protection violations in the security division of the Central Office for Information Technology. Furthermore, I have issued a complaint against the Federal Ministry of Transport and Digital Infrastructure due to violations of data protection law by the Directorate-General for Waterways and Shipping.

In other respects, my findings are essentially comparable to the violations I have already uncovered in previous reporting periods (see 28th AR No. 6.7.4 and 29th AR No. 9.5.5). Among the most frequent deficiencies was an inadequate flow of information between Security and Sabotage Protection Officers on the one hand and the Human Resources Department on the other. Likewise, deficiencies in follow-ups repeatedly led to disregard of destruction and erasure deadlines. I also repeatedly found inadmissible content in security files, such as copies of federal identity cards, passports and residence

permits and documents with personal data of uninvolved third parties that were improperly redacted, if at all.

Seven of the inspections had not yet been finalised at the time of going to press. Although all inspections revealed data protection violations or deficiencies in the area of the security clearance procedure, I was able to refrain from making complaints in some cases because shortcomings were corrected immediately or they were one-off cases without serious consequences. It was noticeable that the area of security and sabotage protection often does not receive adequate attention from the responsible agencies. Causes include ignorance, lack of time and staff shortages. My advice was often sought to support security and sabotage protection officers and to raise their awareness of and reinforce the need for a data protection-compliant approach to security clearance procedures. I am very pleased that this service was used by the bodies inspected.

Best practice / Positives

In some inspections, data protection violations were found in the vast majority of the files examined. However, I welcome the fact that the bodies inspected have consistently shown a willingness to cooperate and have already corrected some of the shortcomings identified. In individual cases, it was possible to remedy the situation on the spot and immediately restore the protection of the informational self-determination of the data subject concerned.

One business stood out in a particularly positive light. 99.39 percent of the files were kept in an exemplary manner here. By marking the data subject in the personnel management system, the business ensures reliable and data protection-friendly processing of the information that must be included in the security file. The system reminds the security officer after five years that an update or repeat check must be carried out or the corresponding file must be destroyed. This ensures that resubmissions are carried out correctly. I have not found any violations here. This actually underlines that a technically and organisationally well thought-out system is conducive to keeping security files and controlling the associated work processes.

Another positive I noted at the Sankt Augustin Federal Police Office was that the security officer prepares an annual security report, which informs the management of the authority about his activities and developments in the field of security clearance law. The security report ensures a certain flow of information and is also a very good example of how this particular area can make itself heard in an agency.

Cross-references:

6.20 The Security Clearance Act - A law with many question marks

8.2.9 Inspection and advice in respect of the Financial Intelligence Unit (FIU)

Since its transfer from the Federal Criminal Police Office (BKA) to the General Customs Directorate (GZD) in 2017, the FIU has not erased any data from its database. In addition, I have had to identify further deficiencies in data protection law, which have led to several complaints. I also advised the FIU on the use of real data in software testing.

In my 29th Activity Report (No. 6.8), I already reported on the FIU and its working methods. The focus was on the redesign of its IT landscape and the development of the FIU 2.0 information network. In the current reporting period, I have now carried out an inspection at the FIU in relation to erasure of personal data for the first time.

With effect from 26 June 2017, the FIU began operating as an independent administrative authority under the umbrella of the GZD. It is responsible for receiving, collecting and analysing reports on suspicious financial transactions that may be related to money laundering or terrorist financing. In this context, it processes a huge number of reports of suspected money laundering containing sensitive personal data.

In June 2020, following the transfer of the FIU from the BKA to the GZD, the erasure periods provided for in the Establishment Order (EAO) for the current FIU Information Network expired for the first time. I took this as an opportunity to inquire both with the FIU and the responsible technical and legal supervisory authority in the Federal Ministry of Finance (BMF) about the implementation status of the erasure requirements. In several statements, I was informed that at that time it was impossible either to implement the necessary erasure mechanism in the system or to arrange for manual erasure of personal data by the case handlers. I took these statements as an opportunity to initiate a formal inspection procedure at the FIU.

The inspection revealed several data protection shortcomings, each of which I raised as a complaint with the BMF. For example, the legal regulations stipulate that both technical and manual precautions must be taken before a system is put into operation in order to implement data protection principles effectively and protect the rights of data subjects. The FIU has failed to do this. The FIU Information Network was even operated for se-

veral years without complying with the erasure requirements of the Money Laundering Act and the aforementioned EAO, which govern its work. At the same time, the FIU has failed to provide its employees with appropriate rights for manual erasure. My individual case reviews have confirmed this. In my sample inspection, I was able to establish the existence of erasure requirements in more than one third of the individual cases. Erasure had not been carried out in any of these cases. The FIU and the BMF refer to the introduction of restricted processing as compensation for the failure to erase the data. This does not, however, mitigate the violations of data protection law. In this context, I have informed the BMF that even the legal prerequisites for applicability of an exemption have not been met.

The FIU and the BMF have initiated the implementation of technical erasure requirements in the system and assured me of the fastest possible implementation. However, the BMF rejects manual erasure by case handlers in many cases. Manual deletions are, among other things, not compatible with the core role of the FIU. The largest possible data pool must be available for analysis purposes, as supposedly harmless facts could later become valuable reports.

This leads to my next point of criticism: the blanket, unchecked transfer of money laundering suspicious activity reports into the FIU's data pool for the purpose of data retention and use of the data for analysis and research purposes violates the principle of data minimisation. The Federal Constitutional Court has already rejected data retention in other contexts on several occasions. Moreover, such an approach contradicts the explicit requirements of the Money Laundering Act, which, in addition to regular segregation checks, also explicitly provides for checks during individual case processing. The same applies to the EAO mentioned above. If data are no longer required for the FIU to perform its tasks, they must be erased.

During my inspection, I also found a lack of documentation and record keeping at the FIU, which made my review considerably more difficult. This includes, for example, incomplete, inconsistent or contradictory information in the case processing system, the absence of deadline entries and a lack of justifications and decisions for further storage. Against this background, I consider a larger-scale data protection inspection and self-inspection by the authority to be difficult to implement.

Overall, there is a need for improvement at the FIU. In future, the implementation of the legal requirements must be reflected in the workflow of case processing and in the erasure concept for the new FIU Information

Network 2.0. I will therefore continue to push for the FIU to perform its tasks in accordance with the requirements of data protection and monitor the implementation process.

Advising the FIU on testing using real data

The processing of personal data at the FIU is subject to purposes laid down by law. Test purposes are not included. Since it is also in the interest of data protection to ensure that the software used is of high quality, I advised the FIU on alternatives that protect fundamental rights.

The FIU approached me to tell me that they wanted to use real data for various test and development projects. A copy of their entire operational database was to be used for this purpose. Specifically, this involved updating existing software, introducing the erasure mechanism already mentioned and a search interface. Unmodified real data is also absolutely essential for (continuous) training of the artificial intelligence models used by FIU Analytics. The FIU stated that it considered this to be legally permissible on the basis of real operation.

However, I have expressed my concerns regarding the use of real data for testing purposes. It is true that software testing is also essential from a data protection perspective to ensure the integrity of data processing. However, personal data is subject to the principle of purpose limitation. The Money Laundering Act (GwG), which is relevant for the FIU, seems not to include a sufficiently specific and clear legal basis for testing IT applications with real data. Tests with a copy of the entire productive database would also contradict the data protection principle of data minimisation. Before testing with real data can even be considered, it must always be verified that there are no less intrusive options available to achieve the purpose pursued by the software test.

I subsequently entered into dialogue with the FIU in order to highlight a variety of alternatives to testing with real data. Above all, I have encouraged the systematic creation of test cases that cover specific requirements, and also of marginal cases and negative tests. Another alternative would be to generate artificial test data. Techniques such as fuzzing could also be used to detect unforeseen errors. I also pointed out the importance of ensuring data quality in avoiding errors. Finally, prior anonymisation or pseudonymisation of real data before use for test purposes would be conceivable, too.

Apart from the problem of the absence of a legal basis, these options for testing should be explored as a matter of priority before any real personal data is considered for use in the context of a pilot operation. I will continue to monitor the processing of data by the FIU.

8.2.10 Inspection of unlicensed postal service providers

In the year under review, I inspected the large area of unlicensed postal service providers for the first time. Due to the pandemic, it was only possible to carry out the inspection in writing. Even though I was able to gain a good insight into the data processing of the inspected companies in this way, in future I will again prioritise on on-site consultation and spot checks.

Companies that intend to transport letters weighing up to 1,000 grams in Germany require a licence from the Federal Network Agency as a postal service provider. If only heavier letters and parcels are carried or courier services are provided, a postal service provider does not need a licence, but notification is required that it is operating as a postal service provider. Several tens of thousands of companies are registered with the Federal Network Agency as non-licensed postal service providers, ranging from sole traders, through bicycle courier services, to large forwarding companies.

Data protection inspection must therefore be limited to spot checks. During the year under review, I sent a questionnaire to a random selection of non-licensed postal service providers with general questions about data protection and processing of personal data in the provision of the postal service.

The result was that I did not find any serious data protection deficiencies in the postal service providers inspected. The inspected companies often processed personal data only to a very small extent in the context of their services, such as sorting and delivery of mail on site. They regularly worked for licensed postal service providers as subcontractors and used their infrastructure.

However, it became apparent that there is little awareness of data protection issues in these companies and that there is a widespread need for information and education, which cannot be covered by inspections alone. I will therefore also be expanding my information services for these companies, supplemented by direct advice in the context of on-site inspection visits.

8.2.11 Questionnaire on rights of data subjects

The rights of data subjects under the General Data Protection Regulation (GDPR) are often the subject of enquiries, both directly to companies and authorities and in the form of submissions and complaints addressed to me as the supervisory authority. In the postal

services sector, I therefore inspected more than a dozen companies in writing on the implementation of data subjects' rights.

Data subjects whose personal data are or have been processed have a number of data subject rights under Chapter 3 of the GDPR. On the one hand, the controller must inform data subjects about any processing of personal data, and on the other hand, the GDPR then gives those persons active rights: they can request information, rectification, erasure or restriction of processing, if applicable, receive and transfer their data in a common format or object to the processing. More detailed information on the rights of data subjects and instructions on how to exercise them can be found on my website (www.bfdi.bund.de).

Following a large number of individual case reviews in the context of submissions and complaints about data subjects' rights, I inspected a double-digit number of postal service providers this year with regard to implementation of these rights. Controllers should provide detailed information on the implementation of the legal requirements and give me an insight into their processes in this connection.

The positive result shows a solid level of data protection across the board. All companies have addressed data subjects' rights and how they should be granted. In many cases, there are written processes with clear responsibilities - after all, the one-month deadline for responding to the applications of data subjects usually has to be met.

However, I have also noticed some weak points in the responses. The central right to information in particular still needs to be adapted to the latest developments in case law by one or two controllers. Isolated indications of a different understanding of the legal requirements were communicated to the organisations inspected and are also being enforced accordingly where necessary.

As expected, larger companies receive significantly more enquiries about data subjects' rights than regional postal service providers. However, as a result of the inspection, the employees involved in all the companies contacted have become more aware of the rights of data subjects. I am therefore confident that data subjects will be able to exercise their rights in respect of these companies even more effectively in the future.

Cross-references:

3.2.5 Guidelines on right of access Art. 15 GDPR

9 BfDI internally

9.1 Organisational review

The results of an organisational review show, among other things, that additional staff are needed for optimal fulfilment of my statutory remit, given the increased - and still increasing - volume of work.

A full organisational review, including a staffing needs assessment, was conducted in my agency from August 2020 to October 2021. The aim was to clarify the potential for optimising the organisational structure and processes. Especially with a view to the future performance of tasks and the associated allocation of resources, the staffing needs assessment in particular should provide a valid basis for future budget preparations. This also corresponded to the requirements of the Audit Committee of the German Bundestag and the Federal Audit Office.

My organisational unit was in charge, with external support from a consultancy firm selected by the Federal Office of Administration. All organisational units including the management staff and the Single Contact Point (ZAST) were involved in the organisational review. The study was based on the methodological recommendations of the organisational manual of the Federal Ministry of the Interior, Construction and Community (BMI).

Based on these recommendations, an initial catalogue of tasks was first drawn up and validated for the staffing assessment in all organisational units, which was then coordinated with the organisational units so that a retrospective estimate of the volume of work was possible based on the personnel capacities available as of 30 November 2020. With this data, it was possible to carry out both a task-critical examination (purpose and implementation) of the as-is analysis and a process and interface analysis. This revealed potential for optimisation. The in-depth analysis was carried out in the thematic areas “Central Knowledge Management”, “Controls” and “Processing of Inputs from the Public”, which I considered to be strategic priorities.

The subsequent resource requirement forecast for the specialised tasks, taking into account the results of the

task-critical survey and statutory task definitions, has shown that I still lack resources to fulfil my statutory mandate to a high quality standard.

The realisation that I need more IT specialists to fulfil my - ever expanding - statutory role, which must be carried out with increasing use of technology, is an important finding of this organisational review.

It should also be noted that, along with the allocation of further statutory tasks, the intensity of the work has also increased significantly, especially due to an increasing number of procedures and technologies involving digital data collection and processing. Both can only be tackled with sufficient additional human resources, as the personnel can no longer be found internally.

9.2 Personnel development in 2021

My authority had a total of 346.4 posts available in 2021. Despite the coronavirus pandemic, which significantly limited personal contact in 2021, and a number of new posts in the 2021 federal budget, I was able to fill about 75% of the available posts. I have been able to use the in-house videoconferencing technology for this and have recruited many junior staff and experienced employees. I see myself well on the way to being able to fill the posts made available by the budgetary legislation.

For the reporting year 2021, I have been given a total of 346.4 posts in the budget to perform my duties properly. These are divided into 328.9 posts for civil servants and 17.5 posts for pay-scale employees. Even in the age of the pandemic, I have succeeded in recruiting numerous junior staff and experienced employees for my organisation. By contrast, I recorded only six staff departures in 2021, some of which were unforeseen. In total, my organisation has a staff of 275 people as of 31 December 2021.

As in the 2020 reporting year, staff recruitment procedures were affected significantly by the pandemic situa-

tion. Due to contact restrictions, I was not able to start the application selection process until the 2nd quarter, contrary to my original plans. I have not yet reached the desired number of new colleagues. In 2021, I received a total of 432 applications and was able to conduct 29 application processes with the help of modern in-house video conferencing technology. 153 people attended for interview, from whom I was able to recruit over 44 new colleagues. Of these, 26 colleagues have already started their employment with me, and another 18 people will follow in 2022. I remain confident that, as an attractive employer, I will be able to fill the remaining vacancies in my organisation in the coming months.

In order to promote my agency as an employer, I have again invited eight students and ten trainees to spend training days in my office in recent months. In addition, I have started to offer internships for school students in Bonn, beyond the usual Girls and Boys Day. The first of these ran successfully in November 2021 and there was lively interest. The overall staff development concept I am planning is currently being drawn up according to thematic modules and coordinated with interest groups. Treating each other with respect is also important to me, which is why I have also put a conflict management policy into effect. I was also able to present a comprehensive promotion policy and coordinate it with the interest groups.

9.3 Press and public relations

My agency's press work in 2021 was again largely dominated by issues related to the coronavirus pandemic. The electronic patient file also remains a perennial topic, especially in the specialist press. We are reaching more and more citizens with our public relations work. The official account of my agency on the decentralised messaging service Mastodon now has over 3,000 subscribers. For the first time, the public was able to participate live in two BfDI events through digital formats. And: demand is very high for our children's books on data protection.

Public relations

Most of the enquiries to my press office in 2021 were also related to the coronavirus pandemic: the coronavirus warning app, digital vaccination certificates and 3G in the workplace are just a few of the main topics. As last year, I was frequently confronted with the mistaken view that data protection would prevent an effective fight against the pandemic, or at least delay it or make it unnecessarily bureaucratic. I will not give up on my attempts to persuade the public that a contradiction is

being invented here that does not exist in reality. The same applies to the listing of alleged "data protection breaches" or „pranks“, which lead to allegations of excessive data protection in Germany. For example, it was repeatedly claimed that distribution of vaccination invitations in Lower Saxony had failed because of data protection. The same applies to the public complaints by the German Society for Orthopaedics and Trauma Surgery that data protection makes it more difficult to get people to join the trauma register. Where my agency was consulted, we were able to refute such myths very quickly with the facts.

The short-term phenomenon of the social network "Clubhouse", which has been discussed at length in the media, must also be seen in the context of the pandemic. Only verbal discussions should take place in digital spaces. I have forwarded corresponding enquiries to my colleagues in the federal states, as I have not inspected the app since my powers do not extend to it.

Conversely, my announcement of a review of the use of Facebook pages by federal ministries from January 2022 had no impact on their use by state authorities or municipalities. I answered many enquiries in this connection by pointing out the federal organisation of data protection in Germany and published my letter to the federal authorities in the transparency section of my website.

There was also a very high level of interest in certain specific topics. These include my prohibition of the use of the study Child Welfare and Custody, legislation on the modernisation of registers, my investigation of journalistic enquiries submitted to the Federal Commissioner for Stasi Records and the developments on electronic patient records. While the first topics only attracted significant media interest temporarily, the electronic patient file is becoming more and more of an "ongoing issue".

In connection with the flood disaster, there was significant media interest in the topic of "cell broadcasting" (see 11.2 Data protection-friendly disaster warning). In addition to questions about data protection, I had to explain repeatedly how cell broadcasting works. Unfortunately, I still saw the erroneous term "warning SMS" in the reporting. I can therefore only urge media professionals to continue to contact my press office in confidence with enquiries in order to prevent the dissemination of data protection myths.

I issued 16 press releases in the reporting period and was invited to the Federal Press Conference once. I have also written seven guest articles and essays for various media. My press office answered 526 enquiries by mail and 511 by telephone.

Website and social media

In 2020, I launched my own instance of the decentralised messaging service Mastodon. The official account of my authority (social.bund.de/@bfdi) now has over 3,000 subscribers. In addition to publishing press releases and new documents on my website, I also answer questions from users. I would like to increase this interaction in future and thus provide even more insights into the work of my authority.

I have also opened up my instance to all federal ministries and supreme federal authorities as well as the German Bundestag, the state parliaments and the state data protection commissioners. However, I have only received a few positive responses to my official invitation so far. I will repeat my offer to the new government and continue to promote privacy-friendly social media services.

In addition, I would like to improve the opportunities for the public to share their experiences in the areas of data protection and freedom of information. To this end, I revived the “Data Protection Forum” (<https://forum.bfdi.bund.de>) in spring 2021. The lively participation in the forum and the positive feedback are encouraging me to continue to seek interaction with the data protection community in the future.

In summer 2021, I also revised my website (<https://bfdi.bund.de>). The new structure and design are intended to make content easier to find. The new site is based more closely on the types of information that users are searching for. Thus, there are specific sections for the general public, experts and media professionals. Contact details and forms are now also easier to find. However, during the redesign of the website, there was a brief data glitch during which no complaints were forwarded to my authority via the new online forms over a period of several days due to a configuration error. The error was quickly rectified.

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. However, I was able to offer digital events for the first time, in the form of the Freedom of Information Symposium 2021 and the Police Information Systems Symposium. Through data protection-compliant streams, I even reached more people than would have been possible with a face-to-face event.

As part of the series of “Bonn Days of Democracy”, I took part in the virtual discussion on the topic “How

many fundamental rights am I prepared to give up to use Instagram?”.

I hope that the situation next year will allow us not only to offer more of these events, but also to hold them again either face-to-face or as hybrid events.

Visitor groups

Unfortunately, no visitor group support took place this year because of the coronavirus pandemic.

Information material

As part of my advisory and educational work, I was able to publish my children's books on data protection, which have been developed with CARLSEN Verlag, in December 2021. The Pixi book “Die Daten-Füchse - Das ist privat!” (The Data Foxes - That's private!) was designed for children of kindergarten age, their parents and all Pixi lovers. The book from the Pixi Wissen series “Die Daten-Füchse - Was ist Datenschutz?” (The Data Foxes - What is data protection?) has been created for children in primary and secondary schools and for any other interested readers.

In order to find out what young readers think of my new Pixi books, I visited one primary school and one comprehensive school in Bonn. I was impressed by how quickly and openly we got into conversation, how many questions were asked and also how critical the students are towards requests for personal data when downloading apps or games.

The demand for information material suitable for children and young people was and remains high. In less than a week, I received more than 9,000 orders for my Pixi books. This again suggests to me that we are on the right track. There will therefore be a second edition of the “Data Foxes” in 2022.

At the same time, the two current Pixi books will be turned into videos. In doing so, I am hoping to open up another source of information and ensure that our important messages are accessible all the time.

Our other publications have also been in demand again this year. Among the brochures for a professional audience and the general public, “Info 1” with its texts and explanations on the General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG) remains the perennial favourite. But the newly published “Info 6” with information about the GDPR in the federal administration also met with considerable interest. Among my flyers, “Remote and Mobile Working - A Data Protection Guide” was particularly important and popular information material for citizens in the age of the coronavirus pandemic and working from home.

Focus group test

An important part of my statutory remit is to raise public awareness about data protection. Specific measures for children given special attention. In order to appeal to the right target audience when creating services for children and young people, I arranged for a focus group test to be carried out. In this way, we have established the following for our target audience:

- how children and young people are aware of the issue of data protection and how they feel about it;
- where children and young people come into contact with the topic in their everyday lives;
- what children and young people find exciting about the topic and what interests them less;
- how children and young people could be inspired by the topic.

With the results from the focus group, we will now create further specific services and materials for children and young people.

Cross-references:

11.2 Data protection-friendly disaster warning

9.4 At the scene of the action: The Capital Team of the BfDI

My authority has long maintained a small liaison office in the federal capital with colleagues from various specialist departments. I have now also formed a Capital Team there, linked to management, which acts as a central contact on the ground for all political events.

A very important part of my statutory remit is to advise the Bundestag, the Bundesrat, the federal government and other institutions and bodies. This applies in particular with regard to legislative and administrative measures that protect the rights and freedoms of natural persons with regard to the processing of personal data.

Berlin is the hub of national political events and the accompanying social, economic and academic interaction. This means that my Bonn-based authority needs local representation on the Spree, while European networking can be better ensured from the Rhine. For structured networking in the political sphere, I have formed a Capital Team in the liaison office as a first step in bringing together channels of information and interaction and in easing the burden on my specialist departments as a result. It is located in the management divisions and is intended to bring together specific political information

and communications in the context of Berlin's political scene and to process them for my agency. In view of my statutory remit, I also see myself in particular as a service provider for parliament and government and attach particular importance to this interface.

With the new Capital Team, it is now possible for me to expand my information services for the parliamentary sector. For example, special information for MPs and their staff is published regularly in the form of the Parliamentary Newsletter. This is available on my homepage and is also distributed publicly thereafter ([www.bfdi.bund.de/ parlamentsbrief](http://www.bfdi.bund.de/parlamentsbrief)). In addition, I offer workshops on the basics of data protection and selected individual topics for this target audience. As well as providing information, this is intended to sharpen understanding of and empathy for data protection issues. We also make this service available to German MEPs.

Contact and interaction with all the other business, academic and social stakeholders in the capital is also one of the key tasks of the Capital Team. Ultimately, I am required to follow relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technology and business practices. Behind both tasks is the idea that the protection of citizens' data is best served if I, as the custodian, work towards solutions that protect fundamental rights from an early stage and help to avoid undesirable developments.

9.5 BfDI facts and figures

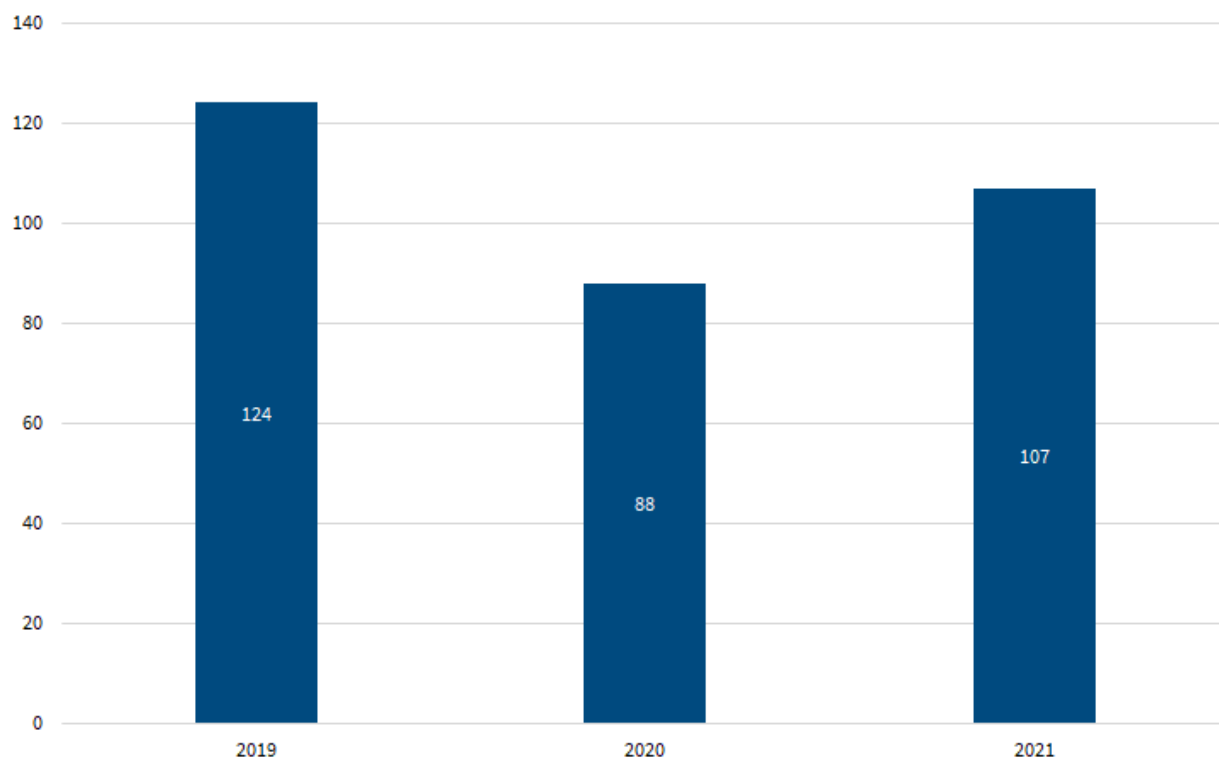
In the previous sections, I have reported on selected individual points of the data protection year 2021. However, this reflects the day-to-day work of my office only in part. The following figures and statistics provide a better overview of what I was involved with last year.

Consultation and inspection

One of the most important activities of my authority is advising and monitoring the bodies under my supervision. Unfortunately, I am still only able to carry out limited inspection visits because of the pandemic. Nevertheless, as can be seen from the graph, I was able to increase my inspection activities beyond the 2019 level. The figure of 107 inspections in the reporting year includes 82 written checks, however.

In addition to my inspection activities, I engaged with the bodies under my supervision in a total of 37 - partly virtual - consultation and information meetings in order to remain in discussion about the concrete implementation of data protection.

Consultations and inspections at supervised entities



Committee work

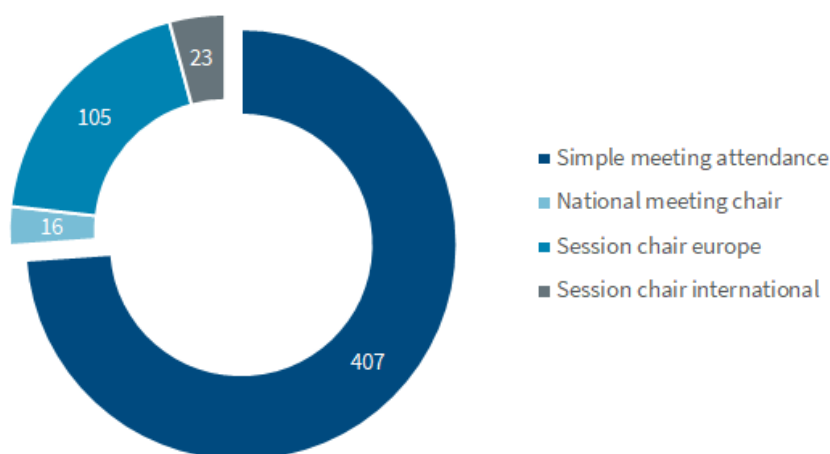
Data protection supervision requires constant coordination not only at the national but also at the European level in order to work towards uniform implementation and enforcement of the General Data Protection Regulation (GDPR). In addition, the wider international networking of data protection authorities is taking on an increasingly important role.

I am actively involved in this process with the aim of further development of data protection and freedom of

information. In the year under review, I took over the leadership of the Berlin Group and actively participated in the Executive Committee of the Global Privacy Assembly.

This represents considerable work for me and my staff. Taking all meetings of main bodies, working groups and subgroups together, my authority was represented at 551 meetings in the year under review. It is particularly noteworthy that in a good quarter of these meetings, the chair (or deputy chair) came from my authority.

Meetings in national and international committees





Complaints and enquiries

In the year under review, citizens addressed a total of 6,829 complaints and enquiries to me. I was also able to advise 7,124 people by telephone. This roughly corresponds to the figures of the two previous years. After the great wave of enquiries at the start of the GDPR, the need for advice on the part of the public seems to have settled at the current level.

A submission is considered a complaint if the data subject believes that their rights have been violated in the collection, processing or use of their personal data. Otherwise, it is to be considered a general consultation enquiry. The difference between the types of submission lies in their legal consequence, as complaints are in principle resolved formally. The right of complaint is regulated in the GDPR and under specific laws.

| Complaints and enquiries | 2019 | 2020 | 2021 |
|---------------------------------------|-------|-------|-------|
| General enquiry | 4.280 | 4.897 | 4.329 |
| Complaint Art. 77 GDPR | 3.118 | 2.861 | 2.383 |
| Complaint Art. 80 GDPR | 3 | 25 | 19 |
| Complaint § 60 BDSG | 44 | 56 | 54 |
| Enquiry against intelligence services | 44 | 39 | 44 |

Reports of data protection breaches

All public and non-public bodies must report data protection breaches to the competent supervisory authority. I received 10,157 corresponding reports in the reporting period. The reports to my authority come in particular

from tax offices, job centres and telecommunications providers.

The excessive reporting beyond the mandatory level that was sometimes observed when the GDPR was first introduced is now a thing of the past. The annual number of reports is around 10,000.

| Complaints and enquiries | 2019 | 2020 | 2021 |
|--------------------------|-------|-------|-------|
| General enquiry | 4.280 | 4.897 | 4.329 |
| Complaint Art. 77 GDPR | 3.118 | 2.861 | 2.383 |

Reports of data protection breaches

All public and non-public bodies must report data protection breaches to the competent supervisory authority. I received 10,157 corresponding reports in the reporting period. The reports to my authority come in particular from tax offices, job centres and telecommunications providers.

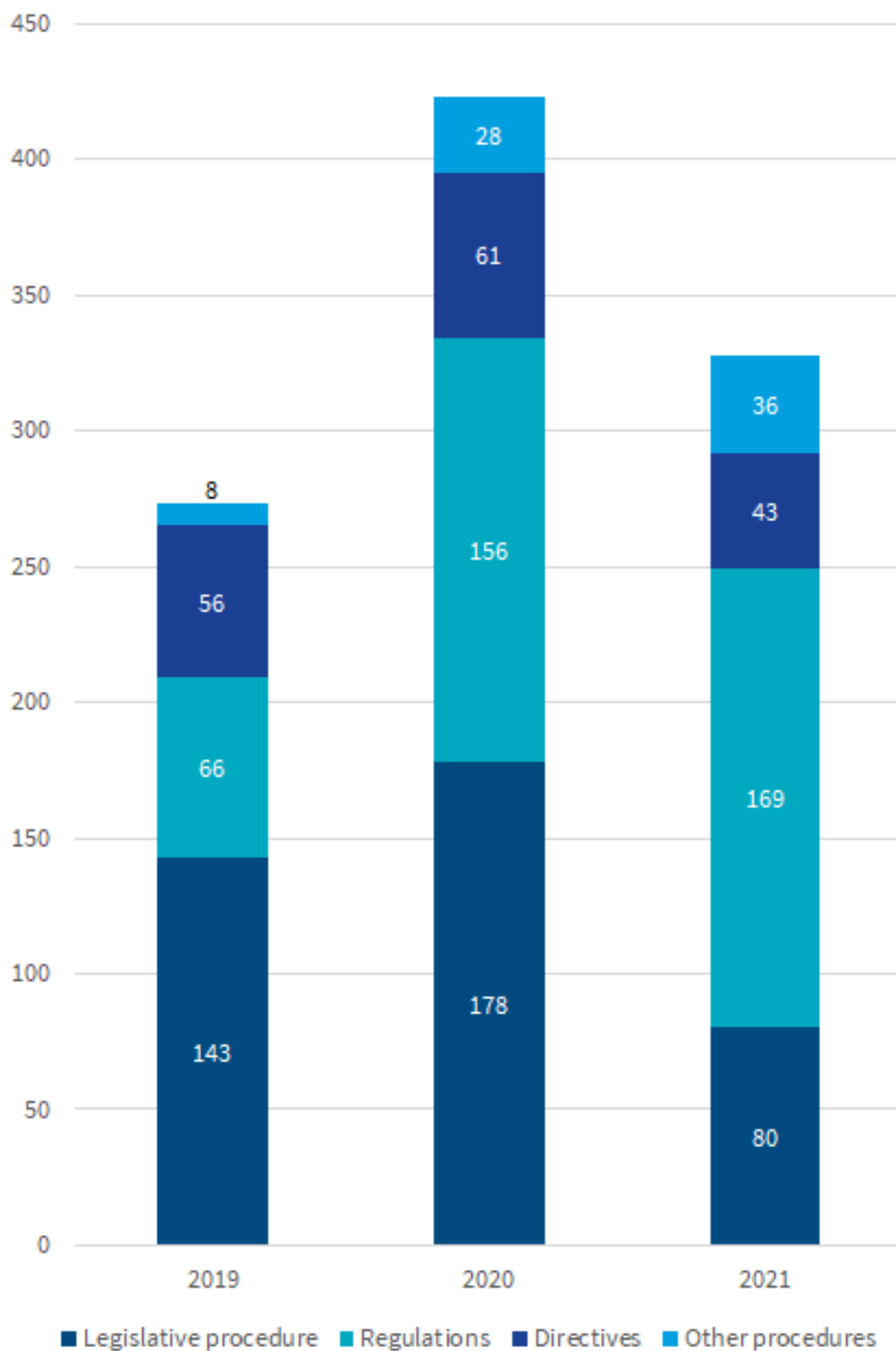
The excessive reporting beyond the mandatory level that was sometimes observed when the GDPR was first introduced is now a thing of the past. The annual number of reports is around 10,000. Formal monitoring of legislative projects

Pursuant to Section 21 of the Joint Rules of Procedure of the Federal Ministries (GGO), the lead ministry must involve me at an early stage in the preparation of

draft legislation, insofar as it impinges on my remit. As explained in several places in this report, unfortunately this does not always work smoothly. In the year under review, despite the federal elections, there were a few instances of my involvement and it was greater than in comparable years without elections, with the exception of 2020, which was marked by the COVID pandemic. My involvement in legislative procedures took place in particular in the first half of the year.

In addition to the 328 instances of involvement under Section 21 GGO shown in the chart, I commented on 43 file orders, 18 EU legal acts and one Federal Constitutional Court case. I was also able to contribute as an expert to twelve hearings of committees of the German Bundestag.

Participations according to § 21 GGO



Submissions with reference to freedom of information law

I received a total of 622 submissions during the reporting period. After an outlier last year, the number of submissions has thus returned to the level of previous years.

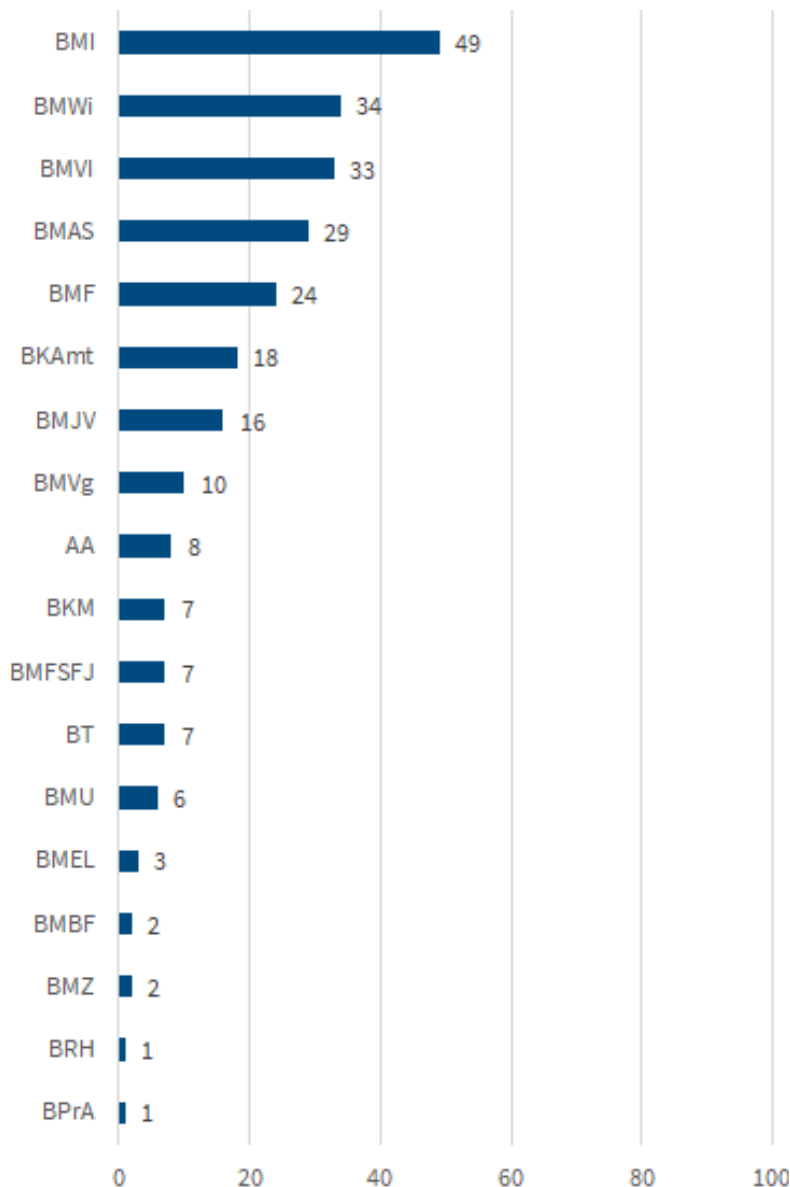
My ombudsperson function in the area of the Freedom of Information Act (IFG) was also extended to matters covered by environmental information law as a result of an amendment to the Environmental Information Act (UIG) in March 2021. Since then, I have received a total of 10 requests for mediation in applications under the UIG during the reporting period. The majority of the applications on which the submissions were based related to emissions, such as those caused by radiation or in connection with the so-called “diesel scandal”. I

expect the numbers to increase as awareness of my new role grows.

In 276 cases, the submissions on questions and topics from the area of the Freedom of Information Act were general freedom of information requests.

In 336 cases, petitioners consulted me in my function as ombudsperson according to Section 12(1) IFG and complained about a violation of their right to access information. The majority of the submissions concerned the Federal Ministry of Health and its area of activity, which - as in the previous year - is due to applicants' strong interest in information relating to the coronavirus pandemic. The content of the applications included risk management for coronavirus conditions, enquiries related to vaccines and the procurement of FFP2 masks.

Statistics on appeals pursuant to Section 12 (1) IFG

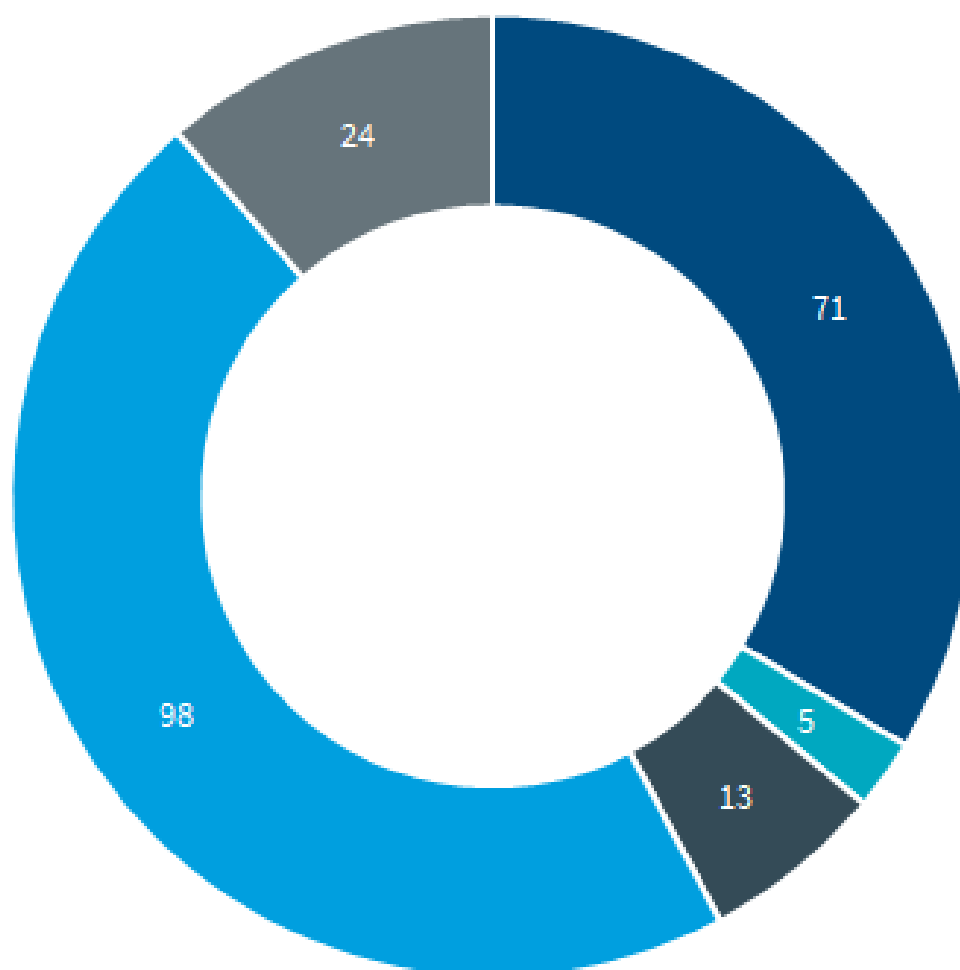


IFG applications to my authority

During the reporting period, I received a total of 211 applications for access to information. These applications related both to access to file contents concerning

submissions made to my authority itself and to my comments on draft legislation. Compared to previous years, the number is stable.

IFG requests to my authority



- Access to information granted
- Access to information partially granted
- Access to information refused
- Other settlement
- Not settled in the reporting year

10 Single Contact Point

10.1 Review

The Single Contact Point (ZSt) coordinates cross-border cooperation between the data protection supervisory authorities of the Federation and the Länder with the other Member States of the European Union, the European Data Protection Board (EDPB) and the European Commission. From the perspective of the ZSt, the year 2021 was marked by the first landmark decisions against leading technology companies. In addition, cooperation of the German supervisory authorities with Europe intensified, supported by the election of a deputy to the joint representative by the German Bundesrat.

The year 2021 marks a turning point in the work of the EDPB. The first important, in some cases long-awaited, decisions were taken on major technology companies. This will set the course for enforcement of the data protection rights of millions of data subjects. The decision of the Luxembourg data protection authority on the online mail order company Amazon involving a fine of EUR 746 million has demonstrated the force of the GDPR. It will have a considerable effect in signalling the need for more data protection-compliant action. The struggle facing the national and European data protection supervisory authorities is particularly evident from the decisions on the social network Facebook and the messenger service WhatsApp.

First emergency procedure in Facebook case: Irish regulator obliged to investigate

The announced changes to the privacy policy and terms of use of the messenger service WhatsApp gave rise to fears that personal data from WhatsApp would be passed on to Facebook. In view of the considerable risks to the data protection rights of WhatsApp users in Germany, the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) prohibited Facebook's European headquarters in Ireland from processing personal data of WhatsApp users residing in Germany for its own purposes for three months by means of an interim measure introduced on 10 May 2021.

In order to take definitive action against Facebook, the HmbBfDI requested a binding decision from the EDPB under the emergency procedure within a period of two weeks. This was not an easy task for this body, which comprises the supervisory authorities of the 27 EU and the three EEA states and the European Data Protection Supervisor. Moreover, it was the first ever procedure of its kind and a number of difficult procedural and data protection questions had to be answered within a short deadline. Procedurally, the question was which requirements are made to determine an emergency and whether a situation exists in which an emergency is presumed to exist legally. The EDPB addressed the different purposes for which personal data is exchanged between WhatsApp and Facebook in the procedure. In the EDPB's view, some of the data exchanges are highly likely to be unlawful, even if a final assessment is not possible on the basis of the information available in the emergency procedure.

The ZSt was faced with the challenge of organising coordination between the German supervisory authorities of the 16 federal states and the federal government within a tight timeframe, ahead of coordination at the European level. The fact that this national coordination succeeded is due to a special effort and consistent implementation of the established processes of the German supervisory authorities. However, the German position arrived at in this way was not able to win over the majority in the EDPB, despite gaining some support. Contrary to the HmbBfDI's request, the EDPB did not immediately order the imposition of definitive measures against Facebook. It confined itself to ordering the Irish regulator to investigate the allegations further.

Dispute resolution proceedings in the WhatsApp case: higher fine imposed

Proceedings compelling the messenger service WhatsApp to comply with transparency obligations under data protection law were somewhat more successful from a German perspective. On Christmas Eve 2020 and after lengthy investigations, the Irish supervisory authori-

ty, which is in charge throughout Europe in this area, presented a draft decision which, among other things, stipulated the imposition of a fine. In addition to Germany, numerous other European supervisory authorities had objected to the draft decision. As a result, the Irish regulator initiated - for the first time in this form - a dispute resolution procedure before the EDPB. Even though some guidance on the dispute resolution procedure was already available because of an earlier case in a more straightforward situation and in the guidelines drawn up shortly beforehand (see No. 3.2.6), numerous difficult questions arose, including some of a procedural nature. Thus, it was first necessary to decide on the admissibility of each objection and each point of those objections. The EDPB used this opportunity to develop the requirements for a proper statement of objection. This is a prerequisite for further referral of the matter. The content related to the transparency of data processing by WhatsApp. As a preliminary question, the operations in which personal data are processed had to be clarified. Here, the EDPB also tested WhatsApp's address book upload function. It came to the conclusion that the telephone numbers transferred in the specific case are personal data, even though they undergo a "hashing" procedure.

Due to the complexity in this area, the EDPB chair extended the procedural deadline to two months. The EDPB draft decision partially upheld the objections. The failure to accept some of the German objections met with concerns from individual German supervisory authorities.

By not upholding these objections, the EDPB missed the opportunity to look not only at transparency but also at the lawfulness of the underlying data processing by WhatsApp, which the lead supervisory authority considered not to be within the scope of the investigation. In view of the otherwise positive results, the decision was nevertheless approved by all the German supervisory authorities. On 28 July 2021, the EDPB adopted its decision, which, among other things, resulted in a significantly higher fine of €225 million being imposed on WhatsApp. In the meantime, WhatsApp has appealed, so the decision is not yet legally binding.

Increasingly visible results in cross-border casework

The conclusion of cross-border cases by final decisions under Art. 60 GDPR was increased significantly in 2021 (2018: 2, 2019: 77, 2020: 89, 2021: 139²³). This form of conclusion to a procedure is regulated in most detail in the GDPR and at the same time, it is the one in which the public has the strongest interest. These decisions have previously gone through the cooperation procedure, which serves to standardise application of the law across

Europe. This is done by the lead supervisory authorities throughout Europe and the specific supervisory authorities involved in each case exchanging and coordinating information. Decisions made in this way are not individual opinions, but the result of the cooperation of the supervisory authorities involved. Where statements are made about the assessment of processing operations under data protection law, this is of particular importance. The decisions taken in this way are published on the EDPB website.²⁴

The following is an evaluation of the decisions in cross-border cases submitted by supervisory authorities in 2021 as final decisions under Art. 60 GDPR:

As the month-by-month view shows, there was a significant increase in final decisions in the months of April and June.

The increase in April is due to the fact that the Irish supervisory authority had submitted 198 case closures in one fell swoop. In legal terms, however, these closures are not final decisions under Article 60 GDPR, but amicable settlements between complainants and data controllers, without an official decision on the merits of the case. This includes cases where controllers made concessions but the complainants did not respond to them in subsequent proceedings. In determining the total number of final decisions in 2021 for this Activity Report, the 198 case closures reached by the Irish supervisory authority through amicable settlement were not included.

The increase in June is due to the fact that the supervisory authorities had previously agreed also to submit a decision in simple cross-border cases where no data protection breach was found. In order to implement this, Luxembourg again issued declaratory decisions concluding proceedings in a number of cases that had already been closed.

Germany was very active in handling cross-border cases and was able to take the top spot here in 2021 alongside France: of the final decisions under Art. 60 GDPR, 22 out of 139 decisions originate from Germany. This does not include the amicable settlements reached by the Irish regulator.

There are also 22 decisions from France. Luxembourg comes next with 13 decisions and Sweden with 12.

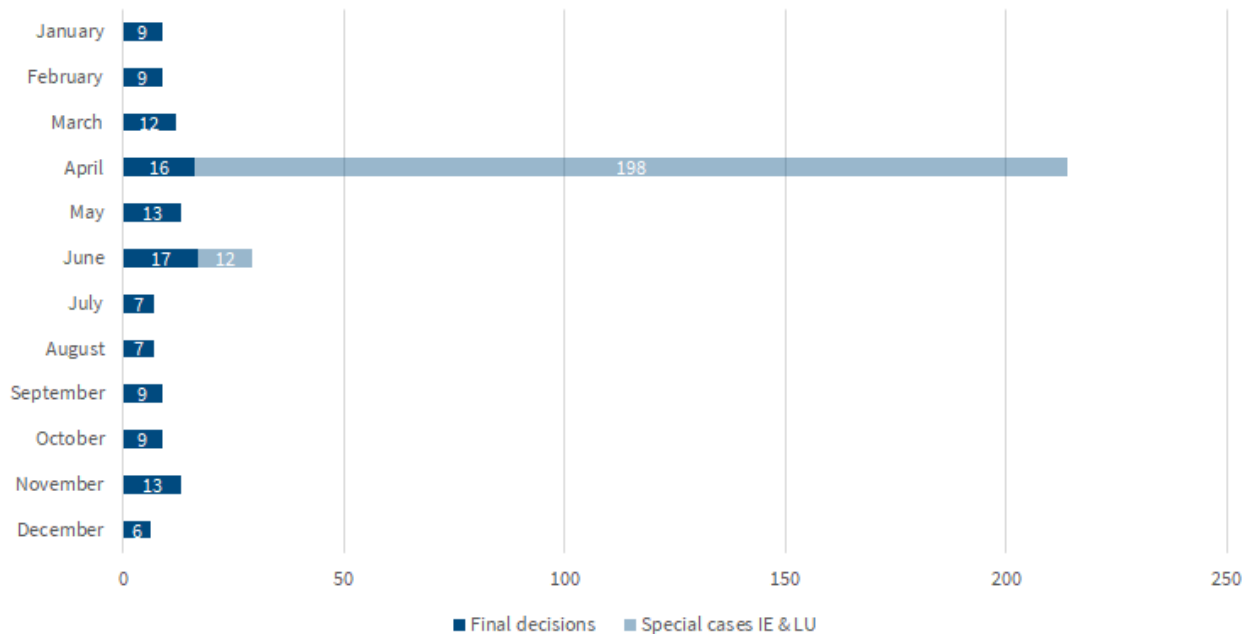
Cooperation between the Joint Representative and the ZAST with the newly elected deputy

More than three years after the provision in the Federal Data Protection Act (BDSG) came into force, the Federal

²³ In determining the total number of final decisions in 2021 for this Activity Report, 198 case closures reached by the Irish regulator through amicable settlement were not included.

²⁴ https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en

Final decisions under Art. 60 GDPR in 2021



Council elected the Bavarian State Commissioner for Data Protection - Prof. Petri - as my deputy on the EDPB on 25 June 2021. One of the tasks of the deputy is to propose common positions for conducting negotiations on the EDPB together with me, if possible by consensus. In addition, he joins me in representing the positions of the German supervisory authorities in the plenary meetings. The deputy also has the right to vote on the EDPB in certain country-specific matters. After the election, organisational measures were agreed with my deputy to ensure efficient cooperation between the BfDI as its joint representative, the supervisory authorities of the federal states and the ZAST based in the BfDI.

Optimising the voting process for establishing common positions in the context of written procedures

As preparation for the voting procedure on the EDPB, it is the task of the ZAST in the case of written procedures to coordinate the establishment of a common position for the federal supervisory authorities and those of the federal states, pursuant to Section 18 BDSG. Written EDPB procedures have been particularly common since the beginning of the pandemic (2018: 6, 2019: 4, 2020: 47, 2021:

52) and votes are carried out via the European Internal Market Information System (IMI). In parallel, the ZAST organises the national vote on the common position, which has so far been held outside the IMI by email. In order to optimise this internal coordination process, which is unique in Europe, a new module was launched in the IMI in 2020 at the suggestion of the ZAST (see 29th

AR No. 11.2). This module was tailored to the needs of the German supervisory authorities. After a trial of the new IMI module with the federal and state supervisory authorities, the changeover to the new optimised voting process was completed in mid-2021. This facilitates the casting and evaluation of votes, which is now no longer done by email, but directly in the IMI with no media discontinuity, in a labour-saving and secure manner.

Cross-references:

3.2.6 Guidelines for dispute resolution procedures before the EDPB

11

Where is the positive?

Unfortunately, the contributions in the previous sections must, by their very nature, often focus on critical monitoring of legislation, inadequate implementation of data protection regulations and identification of flaws in controls. In these sections, however, I always attempt to show how many things are resolved for the better within the framework of consultations and inspections.

To make it even clearer that interaction between the supervisory authority and the bodies under its supervision can lead to really positive results on the basis of effective cooperation, we have also collated some additional examples of this. Our aim: let's see more of it.

11.1 Successful cooperation with the BMU

Unfortunately, many ambitious legislative procedures over the past year did not comply with the Joint Rules of Procedure of the Federal Ministries - especially because the schedules were too tight. The BMU shows that there is another way!

I would like to highlight the pleasing example of successful cooperation between the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) and myself. In the context of the consultations over the legislative process for the Third Regulation Amending the Radiation Protection Regulation, which dealt, among other things, with the transmission of measurement-related data, my participation took place at an early stage and in compliance with appropriate deadlines.

Thanks to my early involvement, constructive consultations were possible. My suggestions regarding data protection law, in particular in terms of clarification and data minimisation, were taken up and the amendment requests discussed were implemented as agreed in the further legislative process.

Together with the BMU, we succeeded in introducing a data protection-friendly version of the regulation.

Long may such close and effective cooperation continue - especially with other federal ministries and federal authorities!

11.2 Privacy-friendly disaster warning

Since the flood disaster in 2021, the plan has been to use a technology already established in other countries for alerting the population to the risk.

Sirens and FM or DAB radios are extremely privacy-friendly media for alerting the population. No data of the recipient is processed here, as the message is sent without a return channel. The situation is different for warning apps, where data traces can be left with the provider, operating system manufacturer and possibly even service providers. These apps are also not ideal for raising the alarm, especially as only a limited section of the population has them installed or is able to install them. Nevertheless, the federal government has put its faith in these apps, which were also supposed to fulfil the requirements of Article 110 of the Directive on the European Electronic Communications Code. This stipulates that Member States are to establish a technical warning system by 21 June 2022, with which mobile phone users can (more) easily receive public warnings.

After the flood disasters in North Rhine-Westphalia and Rhineland-Palatinate in July 2021, the intention is now to use a technology for alerting the population that has already been tried and tested in other countries. Even before the revised Telecommunications Act (TKG) came into force, Section 164 a TKG was inserted, which regulates the introduction of public warnings via cell broadcast. As with sirens and radios, no return channel is required and thus no data is created by the receiving parties. The new system will make it possible to send out alerts at lightning speed to mobile devices that are

able to receive them and that are located in the geographical area designated by the initiating authority. Even though the original impetus for the introduction of cell broadcast alerts had nothing to do with data protection, I strongly welcome the introduction of this privacy-friendly technology.

Cross-references:

5.1 Telecommunications legislation TKG/TTDSG

11.3 Deactivation of access on secondment

In customs investigations, improvements in the handling of access rights to police databases were achieved through the joint consideration of a report of a data protection breach.

The customs investigation office reported the unauthorised retrieval of personal data via an official user ID to me as a data protection violation. The background was that an employee was briefly seconded to an external authority and used his existing access to automated retrieval of data from an official directory to perform his duties there in violation of instructions. In dealing with this matter, I examined, among other things, whether the customs investigation office had taken sufficient technical and organisational measures to prevent unauthorised retrievals from its databases.

As part of the joint consideration of the case, reporting channels and business processes were established to deactivate all access to databases used by the police for the duration of a longer-term secondment to an external agency by technical means. Provided these are adhered to, similar data protection breaches should not recur.

11.4 Raise awareness, create transparency, promote data protection!

Data protection includes raising public awareness, creating transparency and promoting professional discourse. Uncertainties in dealing with personal data or difficulties in assessing data protection issues can be avoided by discussing them and staying in dialogue.

In the reporting period, I succeeded in bringing some important data protection issues out of the shadows and into a broad public debate.

→ With the publication of my position paper on the principle of purpose limitation in police information systems, I have made known my position regarding

the implementation of this central data protection principle in police information systems, including in the interest of transparency in my supervisory activities. In police practice, compliance with purpose limitation is unfortunately not a matter of course (see e.g. No. 8.2.2; 28th AR No. 6.7.3). The position paper contains explanations, in particular, of the necessity for defining and separating purposes, granting access rights, search options and marking and logging obligations in police information systems.

→ In October, I held a symposium on “Police Information Systems in the Age of AI and Big Data - Essential for Police Work or Multifunctional Data Storage on Call?” High-profile representatives from academia, politics, data protection supervision and police practice discussed the current data protection challenges in the design of police information systems. This was a public event in hybrid format, with 350 people participating virtually. In the midst of this event, it once again became clear that different points of view are sometimes not as far apart as they first seem. In my view, further discussions are necessary to reconcile police concerns with the interests of civil society and data protection supervision on a solid legal foundation.

The video recording of the event is available on my website (www.bfdi.bund.de/mediathek). Everyone had the opportunity to ask questions of the participants in the discussion. Many members of the public have made use of this opportunity.

→ Finally, with the consultation process on Artificial Intelligence (AI) in law enforcement and security, I put forward seven theses for public discussion. Everyone was invited to participate in the consultation with their comments and opinions (see below No. 4.2.2). The comments received help to consolidate the constitutional requirements for the use of AI in the area of law enforcement and security and to facilitate the positioning of the Federal Commissioner for Data Protection and Freedom of Information (BfDI) in international bodies. A position cannot be developed soon enough, especially in view of the current advances of the EU Commission in the field of AI (see No. 4.2. below).

Cross-references:

4.2 Artificial intelligence - regulation as a task for society as a whole, 8.2.2 Transaction processing system of the Federal Criminal Police Office

