# Activity Report 2022

31st Activity Report on Data Protection and Freedom of Information

BfDI

Federal Commissioner for Data Protection and Freedom of Information

# Table of content

# 1 Introduction

2022 was an extremely eventful year for my authority, in which it became clear that national and international cooperation between data protection authorities is inevitably becoming increasingly important.

In January, I assumed the chairmanship of the Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK). In the course of Germany's G7 Presidency, I invited the G7 data protection supervisory authorities to a meeting in Bonn. I attended the GPA conference in Istanbul as a member of the Executive Committee of the Global Privacy Assembly (GPA), the international association of national data protection supervisory authorities. I chaired two meetings of the International Working Group on Privacy in Technology in Tel Aviv and London. In addition, numerous meetings of the European Data Protection Board (EDPB) took place. But first things first.

As chair of the DSK, I had set myself two priority topics in addition to the organisational development of the Committee (see 3.2.1): employee data protection and the handling of patient data, especially in research. At three interim and two main conferences, DSK resolutions were drafted and adopted for both topics (see 3.2.4 and 4.1.4), providing guidance to legislators and stakeholders on possibilities and limitations in this area. In addition, we dealt, among other things, with the national implementation of the decisions of the EDPB.

In the reporting year, the EDPB adopted a number of important decisions on the uniform implementation and application of the GDPR in the EU (see 3.3). The focus here was on the transfer of data to third countries and the handling of fines and the right of access. In addition, things are finally moving forward with the lawsuits against Meta (Facebook, Instagram, WhatsApp) that have been on the table for far too long, all of which fall under the lead jurisdiction of the Irish Data Protection Commission (DPC). The DPC's resolution proposals, which were finally submitted in 2022, were in part considerably tightened up by the EDPB, in particular at Germany's suggestion.

Since 2021, the G7 data protection authorities have also met to discuss important international issues within the framework of the G7 consultations. While we still had to meet virtually in 2021, this year I was able to invite my G7 colleagues to join us in Bonn. One of the topics was the further development of the international Data Free Flow with Trust (DFFT) initiative, for which the G7 digital ministers had presented an action plan shortly before. It was good to see that data protection authorities beyond Europe have common ideas for the requirements of DFFT.

The GPA also dealt intensively with the consequences of globalisation and digitalisation at its conference in Istanbul. In a resolution on the future strategic direction of the GPA, international cooperation, knowledge transfer and the highest possible equivalent level of privacy and data protection were formulated as goals.

In addition, many other committee meetings took place at national and international level, which meant a lot of time and work not only for me, but above all for my staff, who are sought-after experts in these committees and often have lead reporting responsibilities. This work is necessary to further develop digitalisation in a positive, trusting way and to harmonise data protection requirements.

In addition to committee work, consultation and monitoring continued to be a focus of my office's work in 2022.

The EU's legislative plans on the European digital rights acts, the implementation of EU requirements in German law and the Federal Government's plans for further digitalisation in the health, administration and communication sectors are keeping me and my office very busy. I have complained and criticised time and again that data protection is only considered and integrated into many projects at a very late stage and, unfortunately, I have to do so again here. It is actually a simple recognition: those who think about and develop data protection from the start have significantly fewer problems and objections, and lower costs, than those who have to make costly

improvements later. We are also talking about unnecessary delays and costs in the range of years and millions of euros.

In particular, the monitoring and consultations of authorities and companies in the security sector are a significant part of my legal mandate. In 2022, numerous monitoring and counselling visits were again possible in person, which clearly improves the work for both sides. And, even though there were and still are individual complaints and criticisms in this respect, I would also like to state here that the persistence of my staff, but also the understanding of the inspected authorities, has led to some significant improvements (see Chapter 12).

The citizens' right to information about administrative actions also led to numerous enquiries and requests for support to my office in 2022. The right to freedom of information is still a troublesome nuisance for many public authorities. That is why we are working hard to create more understanding for civil rights and their implementation. The transparency law planned by the governing coalition could bring progress in this regard, which is why I will urgently participate in the consultation on the law and have already made several proposals for its content.

In 2023, I will also chair the Conference of Freedom of Information Commissioners in Germany (IFK). My aim is also to campaign from this position for more transparency in administrative action and for people's right to information.

This brief outline of some important topics in 2022 is only a part of the diverse work of my office. With the continuing digitalisation of all areas of life and work and the associated processing of data, some of which is highly sensitive, my authority will be faced with more and more work in the future. I can only do this work thanks to my extremely motivated and committed staff. I would like to take this opportunity to express my sincere thanks for their commitment, profound knowledge and willingness to help. The same goes for the dedicated official and company data protection officers with whom we are privileged to work, a committed civil society that cooperates with us and the citizens who exercise their rights and bring abuses to our attention. Last but not least, I would like to thank the German Bundestag, especially the budget rapporteurs for the BfDI (Federal Commissioner for Data Protection and Freedom of Information) budget, for always listening to us and for supporting our work.

Prof. Ulrich Kelber

# 2 Recommendations

## 2.1 Summary of recommendations for the 31st AR

I recommend that the federal government enact an Employee Data Protection Law that clearly regulates, for example, the use of AI in the employment context, the limits of behavioural and performance monitoring and typical data processing in the application and selection process (see 3.2.4).

In our opinion, it is still not poss ible to use Facebook fan pages in a way that complies with data protection laws. I therefore recommend switching off the fan pages. (s. 4.3.1)

I recommend the federal government to push for a substantial revision of the draft regulation on chat monitoring in conformity with fundamental rights and otherwise to reject the draft regulation altogether. (s. 4.4.1)

In order to legally secure the use of AI in the field of law enforcement and security, I recommend that the legislature conduct a comprehensive, empirical and interdisciplinary review by a commission of experts. (s. 4.4.2)

I recommend that the introduction of data fiduciaries on the basis of the TTDSG (Telecommunications Telemedia Data Protection Act) be fundamentally revised and implemented in conformity with the GDPR. (s. 5.5)

I recommend merging the Freedom of Information Act and the Environmental Information Act (and, if possible, also the Consumer Information Act) and further developing them into a Federal Transparency Act with proactive publication obligations. In a Federal Transparency Act, the Freedom of Information Commissioner needs ordering and enforcement powers in order to be able to act in case of conflict. (see. 6.3)

I recommend that the legislature use the upcoming evaluation of the Security Clearance Act (SÜG) to develop a coherent overall concept for personal screening at the federal level. Instead of a sprawling application of the opening clause to entire authorities, different clearance formats outside the SÜG as well as multiple reviews due to different activities, the scope of the law should be redefined. (see. 7.10)

In view of their established low utilisable value, I continue to recommend that the legislature abolish the Anti-Terrorism Filing System and the Right-Wing Extremism Filing System. (see. 9.2.4)

I recommend to the legislator that a legal clarification be made regarding the responsibility for reservists between the BAMAD (Federal Office for the Military Counter-Intelligence Service) and the BfV (Federal Office for the Protection of the Constitution). (see. 9.2.10)

I recommend reviewing the integration of videos on federal websites and implementing data protection-compliant alternatives to the widespread practice of integration using YouTube. (see. 12.2)

## 2.2 Recommendations of the 30th Activity Report

| | Recommendations of the 30th Activity Report | Status of implementation |
|---|---|---|
|  | 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. (30th AR No. 3.1.1, 5.7) | In the ongoing legislative process, my comments on the institutionalisation of the DSK and the improved cooperation of the German data protection supervisory authorities have been partially implemented to date. Within the current legislative period, however, I will continue to advocate in particular for the creation of both regulations for the binding nature of intra-German cooperation at the DSK level and the legal framework conditions for the establishment of a permanent DSK office in the BDSG (Federal Data Protection Act). |
|  | I recommend reviewing the methods and basic data for reporting vaccinations and vaccination rate monitoring. (30th AR No. 4.1.9) | No reference to testing and adjustment. |
|  | I recommend that the BMG (Federal Ministry of Health) provide for – and, if necessary, create – a suitable authority for the operation of the implant register, which can take over the register operation in the long term in a legally secure and data protection-compliant manner without conflicts of interest. (30th AR No. 5.10) | So far, no suitable authority, no plans known. |
|  | I recommend structuring the development of the “common data infrastructure” in a decentralised manner for the genome sequencing model project and providing for event-related data access in each case instead of double data storage. (30th AR No. 6.6) | No plans known on the structure to date. |
|  | 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 SÜG and the transfer of data in the so-called visit monitoring procedure be regulated by the SÜG. (30th AR No. 6.21) | There have been no corresponding amendments to the SÜG so far. However, an amendment is being planned. |
|  | In view of the fact that they have proven to be of little value, I continue to recommend that the legislature abolish the Anti-Terrorism Filing System and the Right-Wing Extremism Filing System. (30th AR No. 8.1.1) | So far, there is no indication that the two databases will be abolished. |

**Recommendations from older Activity Reports and their implementation status can be found at www.bfdi.bund.de/tb-empfehlungen.**

# 3 Committees

## 3.1 Overview of committee work

**Whether national, European or global: important decisions are now no longer made individually by individual supervisory authorities, but increasingly in committees. Accordingly, the work in these and the various associated (sub-)working groups also takes up a large and important part of my work. In doing so, I try – wherever it is possible and makes sense – to get actively involved in the committee work as chair or rapporteur.**

At the national level, the Data Protection Conference (Conference of Independent Federal and State Data Protection Supervisory Authorities) is probably the most important and largest part of my committee work. The work takes place not only in the two main and three interim conferences held annually at plenary level, but above all in the many working groups, sub-working groups and taskforces. In the reporting period, this included more than 50 groups in which my colleagues were represented; in twelve groups even as chair.

The European Data Protection Board and its many sub-working groups are another essential area of my committee work. In addition to the now 15 or so plenary meetings a year, my office is also represented in twelve sub-working groups and two taskforces. The BfDI takes on the role of chair/coordinator in a working group. In addition, my colleagues took on main reporting tasks in two cases and co-rapporteur tasks in three cases, as well as working in drafting teams in another two cases. In this way, we were able to exert considerable influence on the results of these committees.

The added value of networking and joint work is also becoming increasingly relevant at the international level. Here, of course, the international data protection conference known as the Global Privacy Assembly should be mentioned first and foremost. As a member of the Executive Committee, I play a key role in steering and guiding the conference and its goals.

The G7 Data Protection Roundtable, a new body introduced in 2021, is also increasingly important. Here, the chairmanship changes annually – analogous to the other G7 events – such that I was able to welcome my colleagues to the conference in Bonn this year. Besides this main event, however, there are many other preparatory meetings at working level.

In 2021, I assumed the chair of the International Working Group on Privacy in Technology, which is also called the "Berlin Group" after the place where it was founded and meets twice a year.

Together with participation in the Council of Europe's Data Protection Working Party T-PD and several other national and international roundtables, advisory boards and the like, this brings my office to a three-digit number of committee participations per year.

## 3.2 The Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK)

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

In 2022, I assumed the annually rotating chairmanship. The 103rd DSK took place in the Weltsaal of the Federal Foreign Office in Bonn and the 104th DSK took place in the former guest house of the federal government at Petersberg. The first interim conference was held as a video conference due to the pandemic. The two other interim conferences took place on the premises of the Federal Press Conference in Berlin.

Four resolutions were adopted on the topics of erasure moratoria in parliamentary investigation committees, data protection and scientific research, employee data protection as well as the Petersberg Declaration on

Group picture of the participants of the 104th DSK on the Petersberg

Research Data and five resolutions on various individual issues such as data protection-compliant online commerce, the commissioned processing agreement on Microsoft 365, processing of personal data in connection with the institution-based vaccination obligation and on the impact of the new consumer regulations on digital products in the BGB (German Civil Code) on data protection law.

In addition, the DSK revised its guidance on the processing of personal data for direct marketing purposes under the GDPR and for telemedia providers and adopted FAQs on Facebook's fan pages.

**Cross-references:**

3.2.4 New DSK resolution on the Employee Data Protection Law, 3.2.5 Moratorium on file destruction and data deletion, 3.2.6 Guidelines on Advertising 2.0, 4.1.4 Petersberg Declaration

## 3.2.1 DSK chairmanship and DSK 2.0

**The Data Protection Conference (DSK) performs an indispensable interface function in coordinating the supervision of federal and state data protection supervisory authorities. However, this role also brings with it particular challenges – especially in terms of internal organisation – if effective work is to be ensured. First steps for necessary adjustments were initiated in 2022 under my chairmanship.**

At the beginning of the year, I assumed the chairmanship of the Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK) for one year. In addition to the substantive focus of my chairmanship, which concerned the topic of research data (cf. 4.1.1. - 4.1.4), I was also concerned with the further development of the body via the general organisation of the work of the DSK and the orientation of its conferences.

As I explained in the last Activity Report, there is agreement within the DSK to reform the body and, based on the results of the DSK 2.0. Working Group, to submit its own proposals for this (cf. 30th AR 3.1.1). As the chair, I have actively tried to advance this process. In this context, it is my ongoing endeavour beyond the term of office as DSK chair to dispel any reservations about the federal structure and to develop viable joint solutions through pragmatic, goal-oriented offers.

An accusation heard again and again – sometimes, unfortunately, justifiably – is that the federal structure of data protection supervision in Germany leads to inconsistent interpretations and applications of the applicable law. However, for the acceptance of the work of the data protection supervisory authority and its weight in the

public eye, it is essential to act as uniformly as possible and thereby convey a high degree of legal certainty. Therefore, I consider it an important signal that the DSK introduced binding majority decisions this year with an amendment to its rules of procedure. In future, resolutions adopted by a two-thirds majority will be binding for all members of the DSK.

Other results of the DSK 2.0. Working Group include that the DSK must work less reactively and more actively. Fast, reliable answers and decisions on current and future data protection issues and participation in the data protection policy discourse in real time require efficient structures and processes.

I am therefore glad that the DSK has agreed on the formation of a presidium for its strategic-planning and content-related operational management, both internally and externally. From 2023 onwards, the DSK shall be chaired as a collegial body, initially on a trial basis, by a presidium consisting of the previous year's, the current year's and the next year's chair. This will be supplemented by the two representatives in the European Data Protection Board (EDPB), which also includes the BfDI. This ensures that all information flows quickly from the federal level, the federal states and directly from the EDPB as the central body of European data protection.

In my opinion, the success of the work of the presidium and the plenary meeting of the DSK also depends on the creation of a joint office to support the chair and the future presidium and to contribute to a further professionalisation and acceleration of the work of the DSK. I have offered to set up the office at the Single Contact Point (ZASt) affiliated to my office. Already today, the ZASt provides coordinating and supporting activities for the federal and state supervisory authorities in matters of cross-border cooperation with the European supervisory authorities and the EDPB. Due to this wealth of experience and the partly overlapping and/or complementary areas of responsibility for a future office, I see considerable synergy effects and efficiency gains for the work of the DSK. Due to the organisational separation from my office's tasks as supervisory authority, which is supported by law, the ZASt can continue to act as an independent administrator in the interests of all German data protection supervisory authorities, even in its new role as the office of the DSK.

Unfortunately, by the time of going to press, no agreement was reached on the introduction of an office. I assume, however, that the topic will continue to be advanced next year under the chairmanship of my colleague from Schleswig-Holstein. As the BfDI, I will continue to support all initiatives that contribute to a goal-oriented reform of the DSK.

**Cross-references:**

4.1 Research data

### 3.2.2 DSK Sovereign Cloud Taskforce

**Sovereign clouds are intended to strengthen the digital sovereignty of cloud users and reduce their dependence on individual cloud providers. Ultimately, however, this has so far been primarily a marketing term which – defined by the providers themselves – does not allow any binding conclusions to be drawn about the actual offer. On my initiative, the DSK has therefore founded the Sovereign Cloud Taskforce, which is to fill this term with life from a neutral position. At the 104th DSK in November 2022, it presented a position paper with requirements for sovereign clouds, which can support users in the future in the choice of cloud services used and providers in the design of their offers.**

Cloud computing has become an integral part of today's IT landscape. In outsourced operations, many users see the potential for savings and reduced effort. However, it also entails the risk of increasing dependencies, since data storage and processing are no longer under the direct control of the users. Against the background of a growing need for digital sovereignty, users are increasingly asking themselves to what extent such a relationship of dependency is acceptable, especially when it comes to processing personal data for which users are responsible under data protection law. Cloud providers are responding to this need by offering so-called sovereign clouds, although this term is not universally defined; the sovereignty of interpretation as to what constitutes a sovereign cloud has so far been left to the respective providers.

**Sovereign Cloud Taskforce**

On my initiative, the Sovereign Cloud Taskforce was established at the 103rd DSK in Berlin in March 2022. Its initial aim was to define the term "sovereign cloud" from a neutral position, to differentiate it from other cloud offerings and to set out requirements that a cloud must meet in order to be considered sovereign. In November of the same year, the taskforce I chaired submitted a position paper, which was approved by the 104th DSK and formulates requirements and expectations for sovereign clouds from a data protection perspective. The central premises are that the rights and freedoms of data subjects are central in the context of the processing of their personal data and that digital sovereignty requires compliance with applicable data protection law, with the re-

quirements themselves going beyond mere data protection compliance. From my point of view, it is particularly important to note that in a sovereign cloud, processing that is solely in the interest of the provider is excluded. This excludes financing models in which payment is ultimately made with personal data. A corresponding assurance must be effective at least far enough into the future that users have the option of switching to a cloud offering that preserves their sovereignty. In order to create this possibility of switching at all, I continue to see the use of open standards, or at least the availability of documented interfaces, as indispensable. Ideally, these interfaces also enable the exchange of individual components of the cloud service offered, so that users can choose the implementation that best suits them. This may even be one where they have the opportunity to do their own audit thanks to available source code.

A very important topic that I have again dealt with intensively in this reporting year is the influence of third countries (states outside the EU) on cloud providers. Here, the Taskforce asserts in its position paper that clouds can only be considered sovereign if third country influence can be completely excluded and effective enforcement of contractually agreed obligations is guaranteed. From the EU's perspective, this results, among other things, in the requirements that both the registered office and the server location of sovereign cloud providers and their commissioned processors must be located within the EU. To ensure that users do not end up relying on assurances, providers must offer them the opportunity to verify compliance with these requirements and actively participate in such verification. Furthermore, I consider verification through certification as an effective confidence-building measure. With such a cloud, data protection-compliant, sovereignty-preserving IT operations can succeed.

### 3.2.3 DSK Microsoft Working Group

**Hardly any software product is used as widely as Microsoft Office, increasingly also in its cloud-based variant MS 365. Those responsible are faced with the problem that MS 365 is repeatedly criticised because of data protection concerns. In order to provide greater clarity and to be able to give those responsible specific recommendations, the Conference of Federal and State Data Protection Supervisory Authorities (DSK) has conducted an intensive dialogue with Microsoft – with sobering results.**

The DSK started a dialogue series with Microsoft at the end of 2020 under the leadership of the supervisory authorities of Bavaria (State Office for Data Protection Supervision LDA) and Brandenburg (until the end of January 2022). In addition, the supervisory authorities of Berlin, Schleswig-Holstein, Saxony, Mecklenburg-Western Pomerania, Baden-Württemberg, Hesse, North Rhine-Westphalia and my office also contributed. The talks focused on the contractual bases for online services, which include the well-known Microsoft 365, as well as practical implications of the ECJ's case law on international data transfer (Case C-311/18 "Schrems II").

The DSK had already identified points of criticism of the contractual basis in the run-up. Within the framework of the dialogue with Microsoft, some points were able to be remedied from the DSK's point of view. However, the most serious problems remain.

The use of personal data from commissioned processing for Microsoft's own purposes is particularly critical. A viable legal basis is necessary for this type of use. The examination of such a legal basis requires knowledge of the nature of the data processed and the corresponding specific purpose of the processing. However, on the basis of the current "Data Protection Supplement of 15 September 2022" provided by Microsoft, this examination cannot be conclusively carried out.

Responsible parties who want to use Microsoft 365 have the obligation to prove that their use complies with data protection requirements. As long as Microsoft does not create the necessary transparency, users will remain in the dark about what is happening with their data. The DSK has therefore come to the conclusion that data protection-compliant use of Microsoft 365 is not possible on the basis of the current data protection supplement. Further information can be found in the summary of the report of the DSK's "Microsoft Online Services" working group.[1]

Under European law, the lead competent data protection supervisory authority for Microsoft and the data processing associated with MS 365 is the Irish data protection supervisory authority DPC, as Ireland is Microsoft's main location in Europe. However, the BfDI and the German state data protection authorities are responsible under data protection law for the use of MS 365 (and other software) by the bodies they control, hence the focus of the working group.

1 https://datenschutzkonferenz-online.de/beschluesse-dsk.html

### 3.2.4 New DSK resolution on the Employee Data Protection Law

**The increasingly rapid digitalisation of the world of work is a reality. Unfortunately, the current legal framework for employee data protection does not do justice to this. The general clause of Section 26 of the Federal Data Protection Law (BDSG) is not sufficient to provide employees with adequate protection of their personal rights. The uncertainty that exists among all parties involved regarding the question of which data processing in the employment relationship is legally permissible and which is not, requires a clear and differentiated solution. In its resolution of April 2022, the DSK calls on the legislator to present an Employee Data Protection Law in a timely manner.**

The DSK had already called for the creation of an Employee Data Protection Law in 2014 (cf. 25th AR No. 9.3.1 and Annex 9). In the meantime, new regulations on employee data protection have become more urgent than ever, because the current provision of Section 26 of the BDSG is not sufficient against the background of current technical developments. It is too vague, leaves too much room for interpretation, is not sufficiently practicable, normatively clear and appropriate. As a result, it leads to ambiguities about the permissibility of processing personal data in the employment context for employers, employees, applicants, staff representatives and courts. Moreover, practices that violate workers' need for protection remain possible. More far-reaching regulations are necessary and overdue. The federal government has also recognised this and committed itself in the coalition agreement to creating regulations on employee data protection in order to achieve legal clarity for employers as well as employees and to effectively protect personal rights. According to the federal government, a draft bill is to be prepared under the joint leadership of the Federal Ministry of Labour and Social Affairs (BMAS) and the Federal Ministry of the Interior (BMI), with the BMAS having the technical lead. Cornerstones will be developed in the run-up to this. The independent advisory board on employee data protection set up by the BMAS, of which I was a member, also comes to the conclusion that the creation of an independent employee data protection law is necessary.

In its resolution "The Time for an Employee Data Protection Law is 'Now'!" of 29 April 202222, the DSK calls for the creation of regulations under employment data protection law within the framework of an independent law, at least in the following areas:

**Use of algorithmic systems including artificial intelligence (AI)**

The limits and framework conditions of the use of algorithmic systems in the employment and application context should be regulated by law. Due to the existing relationship of dependency, employees and applicants are particularly in need of protection in this respect. In addition to the Hambach Declaration of the DSK and the "Criticality Pyramid" developed by the Data Ethics Commission (see 28th AR, Nos. 4.4. and 4.6), the current developments on the creation of an EU legal framework for AI should also be taken into account. Anti-discrimination or transparency requirements as well as improved possibilities of law enforcement also require legal standardisation.

**Limits of behavioural and performance monitoring**

The limits of behavioural and performance monitoring should be regulated by law, for example for access to and evaluation of emails and other IT data of employees by employers, for the use of geo-information systems (GPS tracking) and biometric procedures in the employment relationship or regulations on the use of video surveillance. Secret surveillance in the employment relationship or continuous monitoring of workers' behaviour should be prohibited.

**Supplements to the framework of consent**

Standard examples of the inadmissibility of the use of consent for the processing of employee data are, for example, important.

**Rules on data processing on the basis of collective agreements**

The legislator should clarify whether collective agreements can form additional legal bases for data processing in the employment relationship.

**Regulations on the relationship between Sections 22 and 26 of the BDSG and on Articles 6 and 9 of the GDPR**

The DSK recommends the creation of clear, specific regulations for the processing of special categories of personal data in the employment relationship, such as health data.

**Prohibitions on the use of evidence**

The DSK is in favour of a legal standardisation of a prohibition on the use of evidence for unlawfully processed employee data.

**Data processing in application and selection procedures**

2 The resolution of 29 April 2022 can be found at: https://www.bfdi.bund.de/entschliessungen

The typical data processing situations in application and selection procedures should also be regulated.

Against the background of this resolution, the Advisory Council Report and the current plans of the federal government, I am optimistic that the Employee Data Protection Law is now on the right track right. Within the framework of the upcoming legislative process, I will continue to advocate for a fair balance between the constitutionally protected interests of employers and the equally protected right to informational self-determination of employees.

**I recommend that the federal government enact an Employee Data Protection Law that clearly regulates, for example, the use of AI in the employment context, the limits of behavioural and performance monitoring and typical data processing in the application and selection process.**

### 3.2.5 Document destruction and data erasure moratorium

**At the end of 2012, it became known that the Federal Office for the Protection of the Constitution had destroyed files on the so-called NSU (National Socialist Underground terror group). Subsequently, the chairman of the NSU investigation committee of the Bundestag therefore asked that no files related to right-wing extremism be destroyed. A comprehensive file destruction and erasure moratorium was declared at the federal level. Contrary to the original intention to lift the moratorium, it is now to be extended again.**

Parliamentary investigation committees want to ensure a sufficient data basis for their investigative work. For this purpose, they are issuing so-called erasure moratoriums, among other things. These prohibit police authorities and intelligence services from deleting such data that relates to the subject of the investigation. Especially for the investigative committees looking into right-wing extremist terrorism by groups such as the so-called NSU, the interest of the parliamentary investigative committees in receiving personal data is particularly understandable and weighty.

Nevertheless, there is criticism of the erasure moratoria. This is because they do not name specific files or records, but describe a subject area in general. Therefore, the scope and the circle of further stored data are difficult to delimit. As a result, the authorities continue to store personal data on a large scale that should actually be deleted. Erasure moratoriums thus encroach on the fundamental rights of data subjects. These interventions are particularly intensive if the persons actually have no relation to the subject matter of the investigation or the data would even have to be deleted. Normally, it is precisely the data that the authorities no longer need for their tasks, e.g., because a suspicion against data subjects has not been substantiated, that is to be deleted. Therefore, a moratorium on erasure, which is aimed precisely at preserving such data that should actually be deleted, is a particularly sensitive intervention. Despite this particular sensitivity, there are no legal foundations to date that regulate the processing of personal data by the authorities for the purpose of conducting a parliamentary investigative committee.

Together with the data protection supervisory authorities of the federal states, I therefore adopted a resolution in March 2022 calling for data protection through clear guidelines and processing restrictions for public authorities.3

In it, the DSK appeals to the federal and state legislators to provide the security authorities with clear legal guidelines on how to deal with data to be deleted in the event of an erasure moratorium. These must secure access to the data for the investigative committees. At the same time, it must be ensured that the data is completely withdrawn from the administrative execution of the authority. [3]

Some state legislatures have already acted accordingly. The Federal Ministry of the Interior and Home Affairs (BMI) recently informed me that it welcomes legal bases for a processing restriction for the parliamentary preservation of evidence. However, the initiative must come from the Bundestag itself. This had been pointed out in a letter to the Committee on the Interior and Home Affairs. However, the BMI considers a moratorium on deletions to be legally compliant and necessary even without a clear legal basis. It therefore remains to be seen whether the federal legislature will act.

#### 3.2.6 Guidelines on Advertising 2.0

**What is advertising? What is direct marketing? What does the GDPR regulate? The DSK has published guidance on the main principles of the GDPR with regard to direct marketing.**

3 Resolution "Parliamentary Investigative Committees and Erasure Moratoria: Data Protection through Clear Guidelines and Processing Restrictions for Public Authorities" Resolution of 23 March 2022 available at www.bfdi.bund.de/entschliessungen

The Data Protection Conference published new guidance on the most important data protection principles for direct marketing in February 2022. The guidance builds on the application notes of the DSK from 2018 on the processing of personal data for advertising purposes, taking into account the GDPR regulations and the regulations of the Unfair Competition Act (UWG). The GDPR itself does not contain any relevant rules for direct marketing. In the guidance, the DSK has now defined the terms "advertising" and "direct marketing", for example. Essentially, it covers five thematic areas:

- Weighing of interests in direct marketing,
- Information requirements,
- Consent to data processing for direct marketing,
- Practical case studies,
- Advertising contradiction.

The "Guidance of the Supervisory Authorities on the Processing of Personal Data for Direct Marketing Purposes under the General Data Protection Regulation (GDPR)" is available on the website of the DSK.[4]

## 3.3 European Data Protection Board

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 data protection authorities, the BfDI is a member of the Board. More details can be found on my website.[5]

**More Information about EDPB can be found here:**

(Scan QR-Code or click)

### 3.3.1 General report

**In the reporting year, the European Data Protection Board (EDPB) further intensified its work on a uniform application of the General Data Protection Regulation (GDPR) throughout Europe. Guidelines were adopted and statements were made. Cross-border cooperation was also further intensified, especially by way of coordinated enforcement action by several supervisory authorities. In addition, five dispute resolution proceedings were decided and others are pending.**

In 2022, the EDPB further consolidated its high density of plenary meetings and held a total of 15 conferences, alternating between video conferences and face-to-face meetings in Brussels. In addition, there were numerous meetings of the EDPB working groups (expert subgroups). Furthermore, a high-level meeting of EDPB members took place in April with the aim of improving cooperation in data protection enforcement at the European level.

One focus of the work in this reporting year was again on the development of guidelines and recommendations pursuant to Art. 70 of the GDPR for the uniform implementation of the GDPR in Europe. In addition, the Board adopted numerous statements in the consistency procedure under Art. 64 of the GDPR and issued statements in legislative procedures together with the European Data Protection Supervisor (EDPS). In my last two Activity Reports (30th AR No. 3.2.1, 29. AR No. 3.2), I referred to initial decisions against world-leading tech companies. There have also been further developments here.

The EDPB has also continued to implement its strategy for the years 2021 to 2023 (cf. No. 3.3.2 below). One focus was on coordinated mechanisms for enforcing data protection at European level in cross-border situations.

**Guidelines, recommendations and statements/coherence procedures**

The EDPB adopted numerous guidelines and statements in the reporting year[6], on which I regularly worked as rapporteur or co-rapporteur. As a rule, these were subject to public consultation in order to maintain transparency.

- **Guidelines 01/2022 on data subject rights** – Right of access aim to analyse the different aspects of the right of access under Art. 15 of the GDPR and to further specify how the right of access is to be implemented in practice. Among other things, the

4 https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf
5 https://www.bfdi.bund.de/edsa
6 Guidelines and statements of the EDPB: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

guidelines include clarifications on the scope of the right of access, the information that controllers must provide to the data subject and the main modalities for granting access. In addition, the concept of manifestly unfounded or excessive application is explained.

- **Guidelines 02/2022 on the application of Article 60 GDPR** are intended to further harmonise the application of the legal provisions on the cooperation procedure between the lead supervisory authority and other supervisory authorities concerned ("one-stop shop mechanism"). The guidelines are intended to help supervisory authorities interpret and apply their own national procedures in a way that is consistent with and interlocks with this cooperation procedure (see also No. 3.3.7).
- **Guidelines 03/2022 on dark patterns in social media platform interfaces:** how to recognise and avoid them provide practical recommendations for the development and use of such platforms and on how to assess and avoid "dark design patterns" on user interfaces that violate the GDPR. Dark patterns (henceforth: "deceptive design patterns") influence users' behaviour and their ability to effectively protect their personal data.
- **Guidelines 04/2022 on the calculation of administrative fines** under the GDPR harmonise the existing practices of data protection authorities and also provide uniform "starting points" for the calculation of a fine. Three aspects are taken into account here: the nature (category) of the infringement, its seriousness and the turnover of the company concerned.
- **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement** provide guidance to legislators at EU and national level, as well as law enforcement agencies, on the introduction and use of such technologies. In it, the EDPB reiterates, among other things, its call for a ban on the use of facial recognition technologies in certain cases, e.g., the remote biometric identification of natural persons in publicly accessible spaces.
- **Guidelines 06/2022 on the practical implementation of amicable settlements** are intended to help eliminate differences in the treatment of data subjects and enforcement measures at national level in the event of termination of proceedings by amicable settlement. These differences have so far resulted from the fact that amicable settlements in the Member States partly do not exist at all or are regulated and handled very differently.
- **Guidelines 07/2022 on certification as a tool for transfers** explain the practical application of transfers of personal data to third countries or international organisations on the basis of certification. In addition to the general guidelines for certification and accreditation under the GDPR, these guidelines focus on the specific aspects of certification as a tool for third country transfers (cf. No. 3.3.10 below).
- **Guidelines 08/2022 on identifying a controller or processor's competent supervisory authority** have been adapted with regard to the identification of a "principal establishment" for the joint responsibility situation within the meaning of Article 26 of the GDPR.
- **Guidelines 09/2022 on personal data breach notification under GDPR** have been adapted for cases where controllers do not have their own establishment in a Member State. The existence of a representative in a Member State is not sufficient to benefit from the one-stop shop mechanism. Therefore, such a controller must contact the supervisory authority of each member state in which it operates.
- **Recommendations 1/2022 on the application for approval and on the elements and principles to be found in controller-binding corporate rules (Art. 47 of the GDPR)** contain an update of the existing "BCR-C-Referential", which contains criteria for the approval of controller-binding internal data protection rules, and merge it with the related standard application form. The new recommendations build on the agreements that data protection authorities have reached in the course of authorisation procedures for specific BCR applications since the GDPR came into force and incorporate the requirements of the ECJ's Schrems II ruling.

In **the coherence procedure**, the EDPB has drafted numerous statements. These largely concern:

- binding internal data protection rules submitted by Member States (Art. 47 GDPR),
- the accreditation of certification bodies (Art. 43(3) GDPR) and
- bodies to monitor compliance with codes of conduct (Art. 41 GDPR).

For the first time, the EDPB also issued a statement on approved criteria of a German company for the pan-European certification of processors (Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors).[7]

In the context of the **consultation in the legislative procedure,** two joint state ments of the EDPB and the EDPS are particularly noteworthy:

- In the **Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse**, the EDPB and the EDPS made it clear that the proposal may pose more risks of interference with fundamental rights of individuals, and thus for society as a whole, than ensuring a successful fight against child sexual abuse. While fully supporting the objectives and intentions of the proposal, the EDPS and the EDPS are concerned that it could be used as a basis for a general and indiscriminate screening of the content of virtually all types of electronic communications (see also No. 4.4.1).
- In **Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space**, the EDPB and the EDPS endorsed the idea of strengthening individuals' control over their personal health data as enshrined in the proposal. At the same time, however, the EDPB and the EDPS see a risk that the protection of privacy and data protection rights could be weakened. This danger exists above all with regard to the categories of personal data and the purposes associated with the so-called secondary use of data (cf. No. 5.1 below).

**Decisions in dispute settlement proceedings**

In July, the EDPB issued a decision in the dispute resolution procedure on the Irish Supervisory Authority's (DPC) proceedings against Meta Ireland (Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR)[8]. The EDPB therein obliged the DPC to establish an additional breach of Art. 6(1) GDPR because Instagram cannot rely on the necessity of the performance of the contract (Art. 6(1)(b) GDPR) or legitimate interests (Art. 6(1)(f) GDPR) as a legal basis for the processing of personal data related to children's user accounts. Consequently, the DPC was directed to reassess its planned remedies in line with the EDPB's conclusions to take account of the additional breach and to ensure that Instagram fully implements the commitments. With regard to the calculation of the amount of the fine, the EDPB instructed the DPC to ensure that the final amounts of the fines imposed were effective, proportionate and dissuasive. Accordingly, the fine had to be increased significantly. As a result of this EDPB decision, the DPC has imposed a fine of €405 million on Instagram. The EDPB's decision was based on so-called "authoritative and substantiated" appeals, which were also filed by several German supervisory authorities, including my authority, under the auspices of the Hamburg Commissioner for Data Protection and Freedom of Information.

Already in June 2022, the EDPB issued a decision in the dispute resolution procedure on the proceedings of the French supervisory authority (CNIL) against Accor SA (Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR).[9] This obliges the CNIL to recalculate the fine to be imposed on Accor SA. The fine was imposed because Accor had unlawfully embedded cookies on its website.

The EDPB issued three further dispute resolution decisions regarding Meta Platforms Ireland Limited (Meta IE) in December 2022. The binding decisions address important legal issues arising from the draft decisions of the Irish DPC as lead regulator in relation to Meta IE platforms Facebook, Instagram and WhatsApp. I consider these decisions to be incompatible with the requirements of the GDPR and had accordingly appealed against the decision on WhatsApp as the supervisory authority concerned. In the two decisions against Meta IE, the EDPB disagreed with the DPC's proposed conclusion that Meta IE was not legally obliged to rely on consent to carry out the processing activities related to the provision of its Facebook and Instagram services. This could not be categorically ruled out without further investigation.

Therefore, the EDPB decided that the DPC must conduct a new investigation. In addition, the EDPB directed the DPC to establish a violation of the principle of fairness in both final decisions and to take appropriate corrective action. The EDPB also found serious breaches of transparency obligations and that Meta IE had presented its services to users in a misleading manner. In terms of fines, the EDPB instructed the DPC to impose a signifi-

7 EDPB statement: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-252022-regarding-european-privacy-seal_en
8 Decision in the dispute resolution procedure: https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf
9 https://edpb.europa.eu/system/files/2022-08/edpb_binding_decision_01_2022_accor_en_redacted_en.pdf

cantly higher fine for the identified transparency violations due to the additional violations of Art. 6(1) GDPR (lack of legal basis for the processing of personal data). This is because the proposed fines did not meet the requirement of an effective, proportionate and dissuasive effect. The further implementation of the decisions will take place in the coming reporting year.

**Cross-references:**

3.3.2 Implementation EDPB Strategy, 3.3.7 Guidelines on Art. 60 GDPR, 3.3.10 Guidelines on approved certifications and codes of conduct as tools for third country transfers, 4.4.1 CSAM Regulation, 5.1 European Health Data Space,

### 3.3.2 Implementation of the EDPB strategy 2021-2023

**In addition to its annual work programmes, the EDPB has established an overarching strategy for the period 2021 to 2023. Coordinated data protection enforcement mechanisms at the European level are a focal point in the second year of joint implementation.**

The four pillars of the EDPB strategy[10] for the period 2021-2023

1. promoting harmonisation and facilitating legal conformity (compliance),
2. supporting effective enforcement and efficient cooperation between national supervisory authorities,
3. a fundamental rights approach to new technologies and
4. the global dimension

and their implementation in the first year, which I described in my last Activity Reports (30th AR No. 3.2.1, 29. AR No. 3.2). In this reporting year, I have again been involved in the implementation of the strategy at both national and European level.

In order to implement the first pillar, the EDPB adopted the designation and position of data protection officers (in companies and public authorities, among others) in terms of Articles 37-39 GDPR as a topic for its second coordinated enforcement action in 2023. For the past year, the EDPB had selected the use of cloud-based services by the public sector as the first coordinated action, which I am implementing in the area of federal administration. The two coordinated measures follow the EDPB's decision in October 2020 to establish a Coordinated Enforcement Framework (CEF)[11] (see No. 3.3.3). Together with the Support Pool of Experts[12], the CEF is a key measure of the EDPB's strategy. The two initiatives aim to strengthen enforcement and cooperation between data protection authorities. The latter objective is part of the agreement reached in Vienna in April 2022 to improve cooperation on data protection enforcement at the European level, especially in cross-border cases. [13]

In the second pillar, in accordance with this agreement, the EDPB defined criteria for cross-border cases of strategic importance, in addition to the coordinated enforcement framework (CEF)[14] and selected three initial strategic cases for deepened and accelerated cooperation. As a further result of the meeting in Vienna, the EDPB adopted a list of partly obstructive aspects of national procedural laws that should be harmonised at European level to improve enforcement of the GDPR. The list addresses, among other things, the status and rights of parties in national administrative procedures, procedural deadlines in the cooperation procedure, requirements for the admissibility or rejection of complaints, the investigative powers of data protection authorities and the practical implementation of the cooperation procedure. This so-called "wish-list"[15] was sent to the European Commission for consideration of possible improvements.

### 3.3.3 Coordinated Enforcement Action 2021/2022

**European data protection supervisory authorities coordinate their action in the first Coordinated Enforcement Action (CEF) and investigate the use of cloud-based services by the public sector**

The Coordinated Enforcement Action is a planned annual coordinated action of the European supervisory authorities within the framework of the CEF. It is an initiative of the EDPB to promote cooperation and enforcement among supervisors and is a key measure of the EDPB Strategy 2021-2023 (cf. 3.3.2). Here, a previously defined topic is worked on together according to a pre-agreed methodology. The topic of the current

10 EDPB strategy for the period 2021-2023: https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2021-2023_en
11 Information from the EDPB on the CEF: https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en
12 Information from the EDPB on the Pool of Experts: https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-terms-reference-edpb-support-pool-experts_en
13 https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf
14 https://edpb.europa.eu/system/files/2022-07/edpb_document_20220712_selectionofstrategiccases_en.pdf
15 To the wish-list: https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf

and first Coordinated Enforcement Action is the use of cloud-based services by the public sector. My authority is participating in this as part of my responsibility for data protection supervision of the federal administration, along with 21 other supervisory authorities, and has conducted investigations into the use of cloud services in the area of labour and health administration and the ITZBund (Federal Information Technology Centre) as the central service provider for cloud services of the federal authorities.

The investigation started by the working group concerns about 75 supervisory items from different subject areas. The focus here is on, among other things, data transfers to third countries and regulations in connection with commissioned processing. Following the evaluation, a joint report will be prepared and adopted by the EDPB. After that, supervisors will decide on coordinated national supervisory and enforcement measures.

**Cross-references:**

3.3.8 Implementation of the Controller-Binding Corporate Rules

### 3.3.4 EU systems: Central coordination of supervision in the CSC

**The responsibility for coordinating the supervision of EU systems and institutions is already concentrated in the Coordinated Supervision Committee of the EDPB, and will be even more so in the future. Europol was added this year, and other EU systems will follow in the coming years.**

In the Coordinated Supervision Committee (CSC) based at the EDPB, the national supervisory authorities and the European Data Protection Supervisor (EDPS) coordinate their supervisory activities and support each other as far as certain EU information systems and EU institutions are concerned. The CSC is currently responsible for four major areas. These are, first of all, the Internal Market Information System (IMI), Eurojust and the European Public Prosecutor's Office. With the amendment of the Europol Regulation (Ordinance) by Regulation (EU) 2022/991 in June 2022, the Advisory Board for Cooperation (cf. 27th AR No. 9.2.3) was also dissolved and Europol was transferred to the area of responsibility of the CSC.

In the coming years, the CSC's remit will be expanded to include numerous EU systems. The already existing systems Schengen Information System (SIS), Customs Information System (CIS), Eurodac and Visa Information System (VIS) are to be located at the CSC. At present, separate Supervision Coordination Groups have been set up for each of these. In future, the CSC is also to be responsible for the planned EU systems European Criminal Records Information System for Third-Country Nationals and Stateless Persons (ECRIS-TCN), Entry/Exit System (EES) and European Travel Information and Authorisation System (ETIAS) as well as the EU Interoperability Framework.

Together with the respective country representation, I actively participate in the regular meetings of the CSC and the drafting of joint documents such as the preparation of a uniform information leaflet for data subjects on the EU-wide use of IMI. In addition, I assumed the vice-chairmanship in December 2021.

The CSC work programme for the period 2022-2024 is available on the CSC section of the EDPB website.[16] The work in the committee focuses on the exercise of data subjects' rights and the promotion of the exchange of information between the members as well as the implementation of joint controls. In addition, there is the preparation of the upcoming expansion of the CSC's area of responsibility.

**Cross-references:**

3.5.3 New ETIAS Advisory Board on Fundamental Rights; 3.5.4 Report from the SCGs; 9.2.8 Coordinated checks on alerts for covert/targeted checks in the Schengen Information System

### 3.3.5 EDPB publishes guidelines on the right of access to information

**With the right of access, data subjects can find out what data companies and authorities process and store about them. With new guidelines, the EDPB provides more clarity and consistency.**

The right of access is very important in practice. However, the corresponding Art. 15 of the GDPR leaves a great deal of room for interpretation, which has led to different opinions in the legal literature, among supervisory authorities and to divergent court decisions. After more than two years of work, the EDPB adopted guidelines on the right of access[17] in January 2022, on which I worked as co-rapporteur.

Particularly important points identified in the guidelines:

16 https://edpb.europa.eu/csc/about-csc/work-programme-coordinated-supervision-committee_en

17 Guidelines 01/2022 on data subject rights - Right of access, available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

- The scope of the right of access is essentially based on the definition of personal data (Art. 4(1) GDPR). A restrictive interpretation does not take place. Internal documents and email correspondence can also be included.
- The right to obtain a copy (Art. 15(3) GDPR) is not an independent right, but a modality for fulfilling the right of access. As a rule, however, a copy must be given to data subjects.
- The controller has an obligation to take reasonable steps to identify the data subject in order to prevent personal data from being disclosed to unauthorised third parties through the right of access. On the other hand, however, no higher hurdles may be set up than for the provision of the data itself.
- If large amounts of data are processed, the controller can transmit the information in several separate layers, especially in the online context (so-called layered approach).
- A request for information cannot be refused by the controller solely on the grounds of the burden of responding or other considerations of proportionality. The motivation behind a request for information is basically irrelevant.
- The guidelines also provide information and concrete examples of the intervals at which data subjects can assert their right of access. When is there frequent repetition? At what point is the right of access abused? For credit agencies, for example, an interval of once a year is not excessive. In the case of abusive requests, a request for access may exceptionally be refused as excessive.

I welcome the common guidelines. During the negotiations, I, together with my colleague from North Rhine-Westphalia, introduced the German interpretation of the right of access according to Art. 15 GDPR into the process. The guidelines represent a successful common position of the European supervisory authorities and make an important contribution to strengthening the right of access in the EU. The EDPB has conducted a public consultation on the guidelines and is currently evaluating the comments received. The final text of the guidelines is expected to be adopted by the EDPB in early 2023.

### 3.3.6 EDPB presents guidelines on fines

**The EDPB has adopted new guidelines on the calculation of fines under the GDPR. They serve to harmonise the practice of fining across Europe and provide points of reference for calculating fines while leaving room for discretion in individual cases.**

In the case of breaches of the GDPR, national data protection supervisory authorities have so far used different methods to calculate fines as a result of different legal traditions and cultures. Through the guidelines adopted in May 2022[18], the practice of fining is now carried out with the help of a uniform European methodology. The guidelines are an important building block in an overall development of data protection authorities towards greater convergence and a more strategic orientation of their law enforcement.

The guidelines now issued by the EDPB on the calculation of fines under the GDPR neither specify mandatory lump sums (so-called price tags) nor do they provide for a purely mathematical calculation formula. Both would be legally dubious and the latter, in my view, even illegal. Instead, the guidelines provide guidance on starting amounts and how these can be increased or decreased by other discretionary factors. On the one hand, they therefore lead to an approximation of the amounts of the fines, but at the same time they also allow the necessary scope for discretion in individual cases.

The guidelines ensure greater transparency for the exact scope of application of the economic entity and also confirmed the Union law principle of direct association liability (see also 29th AR No. 10.2). It is also to be welcomed that, on the one hand, the deterrent high fines foreseen by the European legislator are still possible, especially against large corporations, while, on the other hand, the particularities of micro, small and medium-sized enterprises (SMEs) are sufficiently taken into account in the exercise of discretion and the sensitivity to punishment is not overstimulated.

It is now up to the national data protection authorities, the EDPB and the national and European courts to fill the new guidelines with life in their respective decision-making practice and to achieve real harmonisation across Europe. It is also a litmus test of whether harmonisation of data protection enforcement can succeed with a national supervisory structure.

### 3.3.7 Guidelines on Art. 60 GDPR

**The EDPB adopted the final version of the guidelines on Art. 60 of the General Data Protection Regulation (GDPR) in March 2022. The guidelines are part of the EDPB's strategy and work programme for 2021-2023. They are intended to support efficient cooperation and**

18 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

**rapid consensus-building between national supervisory authorities in the cooperation procedure and thus contribute to more effective enforcement of the requirements of the GDPR. I acted as lead rapporteur in the development of these guidelines.**

One of the most important innovations introduced by the GDPR is the so-called one-stop shop mechanism. This mechanism states that in cases involving cross-border data processing, the supervisory authority of the Member State where the main establishment of the controller or processor is located shall be the lead authority for the enforcement of the GDPR. At the same time, the GDPR provides that data subjects can always also submit their complaints to a supervisory authority at their habitual place of residence. This supervisory authority is also the contact for the complainants in the further course of the complaint procedure. In order to meet these parallel requirements, Art. 60 GDPR regulates the cooperation procedure between the lead supervisory authority and the other supervisory authorities concerned.

The Guidelines on Art. 60 GDPR refer, among other things, to the interactions of the supervisory authorities in this one-stop shop mechanism with each other and to the cooperation with the EDPB itself. To this end, the guidelines make the following key statements:

- The cooperation procedure applies in principle to any case of cross-border processing.
- The lead supervisory authority is primarily responsible for handling such cases, but is ultimately not empowered to decide on its own.
- The cooperation procedure does not affect the independence of the supervisory authorities. Rather, they retain their own discretionary powers within the framework of cooperation.
- The supervisory authorities involved exchange all relevant information with each other at an early stage in order to reach a consensus (see No. 3.3.2)[19].

A brief guide annexed to the guidelines is intended to give staff in the supervisory authorities an overview of the procedure and to illustrate the complex process.

**Cross-references:**

3.3.2 Implementation of the EDPB strategy 2021-2023

## 3.3.8 Binding internal data protection rules - news from the Binding Corporate Rules

**Binding corporate rules (BCRs) are an appropriate guarantee of Chapter V of the General Data Protection Regulation (Art. 47 GDPR) for the transfer of personal data from the EU to third countries within a group of companies (cf. 30th AR No. 3.2.2.2). Last year, the EDPB issued statements on a large number of BCRs, on the basis of which these BCRs were approved by the national supervisory authorities. In addition, the EDPB Expert Subgroup International Transfers (ITS ESG) dealt with the further development of the EDPB's BCR acceptance procedure with regard to its efficiency (quality assurance, acceleration, simplification).**

In the IT S ESG, which deals with the BCR procedure with regard to specific and general issues, I am represented together with representatives of the supervisory authorities of the federal states. In the reporting year, the work on Recommendations 1/2022 on the application for approval and on the elements and principles to be found in Controller-Binding Corporate Rules (Art. 47 of the GDPR)[20] – hereinafter: BCR-C Referentials – revising the EDPB's Working Paper WP 256 rev.01[21] and the associated application form WP 264[22] should be highlighted.

In terms of content, the BCR-C Referentials were adapted[23] to the requirements of the Schrems II ruling of the ECJ[24] on the basis of the new standard contractual clauses of the European Commission for the transfer of personal data to third countries. In addition, results or agreements that have become apparent in the course of the review of specific BCR applications since the entry into force of the GDPR were taken into account. The description of the required BCR elements was clarified accordingly in order to facilitate both the application

19 Improving informal cooperation is also part of the agreement reached in Vienna in April 2022 to improve cooperation on data protection enforcement at the European level: https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf

20 BCR-C Recommendations, 1/2022, available at: https://edpb.europa.eu/system/files/2022-11/edpb_recommendations_20221_bcr-c_referentialapplication-form_en.pdf

21 WP 256 rev.01, available at: https://ec.europa.eu/newsroom/article29/items/614109/en

22 Standard application form (WP 264), available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendation-standard-application-form-approval-controller-binding_en https://edpb.europa.eu/sites/default/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf

23 Standard contractual clauses for the transfer of personal data to third countries, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de https://ec.europa.eu/info/sites/default/files/1_de_annexe_acte_autonome_cp_part1_v3.pdf

24 "Schrems II" ECJ judgment of 16/07/2020, Case C-311/18, available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=40595668

and the work of the inspecting supervisory authorities. The results were adopted by the 71st EDPB plenary meeting in November 2022. The revision of the so-called "BCR-P Referentials" for processors (WP 257 rev.01[25] and the associated application form WP 265[26]) will follow.

In addition, the templates for the EDPB statement and the national supervisory approval decision were adapted to take into account the consequences of the Schrems II ruling as well as to explain the scope of a BCR approval, also with regard to the aforementioned changes in the "BCR-C Referentials".

### 3.3.9 EU-U.S. data privacy framework (Privacy Shield successor)

**The ECJ had declared the US adequacy decision, the so-called "Privacy Shield", invalid in the Schrems II ruling (Case C-311/18[27]). The European Commission and the US government then negotiated a successor regulation based on the requirements resulting from the ECJ ruling. After the announcement of the agreement in principle by both sides in March 2022, Executive Order 14086 on 'Enhancing Safeguards for United States Signals Intelligence Activities'[28], published on 7 October 2022, there followed a further step towards the successor to the Privacy Shield, the EU-U.S. Data Privacy Framework (EU-U.S. DPF). And finally, with the publication of the draft adequacy decision on the EU-U.S. DPF, the launch of the adoption procedure and the invitation to EDPB to submit comments followed. I will be intensively involved in this.**

**Background – Schrems II ruling of the ECJ:**

With the Schrems II ruling, the ECJ (op. cit.) had again clarified and specified the requirements for the transfer of personal data to the USA. As the ruling invalidated the EU's adequacy decision for the US, personal data could no longer be transferred to the US on this basis. The ruling also states that standard data protection clauses must be supplemented with additional measures (supplementary measures), if necessary, so that the data enjoys an equivalent level of protection in the third country as in the EU. If no appropriate measures are available, a transfer of personal data is unlawful. The ECJ justified the lack of protection in the USA in particular by stating that the legal provisions on the basis of which American security authorities could access personal data transferred to the USA were disproportionate and thus violated Article 52(1)(2) of the EU Charter of Fundamental Rights (Schrems II judgment, loc. cit., para. 184 et seq.). Secondly, there was no effective legal protection against access by the American security authorities that met the requirements of Article 47 of the EU Charter of Fundamental Rights (Schrems II judgment, loc. cit., para. 199).

The significant impact of the ruling on data transfers – not only to the USA, but to third countries in general – as well as the audit requirement of an implementation of "supplementary measures", not only with regard to the standard data protection clauses, but also with regard to other transfer instruments (appropriate safeguards) within the meaning of Art. 46 GDPR, have since posed great challenges to controllers, processors and also supervisory authorities. Promptly after the ruling, which did not contain any further explanation of the term "supplementary measures", the EDPB had published Recommendations 01/2020[29] in this regard, which contain examples of potentially effective technical, organisational or contractual measures to secure a data transfer. It should be noted, however, that data exporters (explicitly emphasised by the ECJ) have the responsibility to examine the level of protection in the third country for each data transfer (Schrems II judgment, op. cit., para. 134) and, if necessary, to provide for "supplementary measures" for the protection of data transferred to a third country (op. cit., para. 131).

Against this background, and in order to achieve legal certainty, it is important that data transfers to the US are placed on a new, consistent legal basis. However, this goal could not be achieved without changes in US law.

**Developments on the EU-U.S. DPF:**

In a joint statement on 25 March 2022, EU Commission President von der Leyen and U.S. President Biden announced that an agreement in principle had been reached on a new EU-U.S. data protection framework (EU-U.S. DPF)[30]. This is now intended to be the successor to the Privacy Shield, which was declared invalid by the ECJ in its Schrems II ruling.

25 WP 257 rev.01, available at: https://ec.europa.eu/newsroom/article29/items/614110/en

26 Standard application form (WP 265), available at: https://ec.europa.eu/newsroom/article29/items/623848/en

27 "Schrems II" ECJ judgment of 16/07/2020, Case C-311/18, available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=40595668

28 Executive Order 14086 available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

29 EDPB Recommendations 1/2020, available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

30 Joint Statement EU COM/ USA available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

The first significant provision for a Privacy Shield successor came on 7 October 2022 with Executive Order 14086 on 'Enhancing Safeguards for United States Signals Intelligence Activities' signed by President Biden[31]. Together with the Data Protection Review Court (DPRC) Order issued by the Attorney General[32], the Executive Order now fleshes out the agreement in principle announced in March. The purpose of the Executive Order is to introduce safeguards to address and remedy what the ECJ has found to be legally insufficient. The amendments concern in particular the proportionate restriction of access by US intelligence services to data of non-US citizens, the stronger internal monitoring of data protection within the intelligence services and the establishment of a complaints mechanism for non-US citizens.

The Department of Justice's Executive Order and regulations for the DPRC are supplemented by Department of Commerce regulations regarding data protection certification for companies covered by the EU-U.S. DPF, which is a prerequisite for being able to make data transfers from the EU to the U.S. on the basis of the envisaged EU-U.S. adequacy decision.

**Further procedure/outlook:**

The European Commission has now prepared a draft adequacy decision on this basis and launched the procedure for its adoption on 13 December 2022[33]. This includes obtaining a non-binding statement from the EDPB. In the context of the statement, the European data protection supervisory authorities will now discuss the draft for the new adequacy decision in detail. I will be intensively involved in this work and, together with my European colleagues, will in particular check whether the ECJ's requirements from the Schrems II ruling have been effectively implemented by the changes in US law and whether the other data protection requirements have also been met.

In the procedure, the European Parliament can also adopt a resolution on the adequacy decision and, finally, the Committee of Permanent Representatives of the EU Member States must confirm the draft decision in accordance with Article 5 of Regulation (EU) No. 182/2011 (Comitology Regulation). Provided that the aforementioned procedural steps can be successfully completed, the European Commission will publish the decision in the Official Journal of the European Union. Companies can then certify under the EU-U.S. DPF.

Data transfers from the EU to the US could then take place on the basis of the adequacy decision without further measures.

### 3.3.10 Guidelines on approved certifications and codes of conduct as instruments for third-country transfers

**The General Data Protection Regulation (GDPR) provides that personal data may only be transferred to third countries without an adequacy decision if appropriate safeguards are provided for. These guarantees may, for example, consist of approved codes of conduct or certification mechanisms as transfer instruments for third-country transfers. To this end, the European Data Protection Board (EDPB) adopted two corresponding guidelines in the reporting year based on the preliminary work of the Expert Subgroup International Transfers (ITS ESG).**

On one hand, there are the guidelines on certification as a tool for transfers (Guidelines 07/2022)[34], and on the other, the guidelines on codes of conduct as tools for transfers (Guidelines 04/2021)[35]. I was the main rapporteur for the former and co-rapporteur for the latter. On the one hand, the guidelines serve as orientation for the development of certifications or codes of conduct, and on the other hand, they also set the framework for the data protection supervisory authorities who approve the instruments. In addition, in the case of certification, they supplement existing guidelines on national certification and accreditation for data transfers to third countries.

The special feature of the two transfer instruments lies in their nature as self-regulatory mechanisms. Companies and organisations that become certified or join the approved codes of conduct must permanently comply with the specified requirements. In turn, these controllers may use the transfer tools to meet their accountability (compliance with the GDPR). Compliance with the specified requirements is primarily monitored by a certification body or a monitoring body. Moreover, secondarily, possibilities of control and sanction remain with the supervisory authorities.

31 For the link to the Executive Order, see Footnote 2

32 Regulation on the DPRC, available at: https://www.justice.gov/opcl/redress-data-protection-review-court

33 EU COM press release and publication of the draft adequacy decision on the EU-U.S. DPF, available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_7631

34 Guidelines 07/2022 on certification as a tool for transfers: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en

35 Guidelines 04/2021 on codes of conduct as tools for transfers: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en

Thus, the EDPB has now published on all transfer instruments ("appropriate safeguards" within the meaning of Art. 46 GDPR)[36]

**Cross-references:**

3.1 Overview of committee work, 3.3.8 Binding internal data protection rules - News from the Binding Corporate Rules, 3.4 G7 Roundtable

## 3.4 G7 Roundtable

**On the occasion of this year's German G7 Presidency, the second edition of the Roundtable of Data Protection Supervisory Authorities of the G7 countries took place under my chairmanship. The main topic was "Data Free Flow with Trust", i.e., the issue of trustworthy international data transfers. In the adopted communiqué, the G7 data protection supervisory authorities stress the importance of respecting democratic values and rule-of-law standards. The G7 Roundtable meeting is to be continued as a permanent format in the coming years.**

In 2021, the British G7 Presidency initiated a meeting of the G7 data protection authorities (G7 DPA) for the first time, which dealt with the important issue of Data Free Flow with Trust (DFFT) (cf. 30th AR No. 3.4.1). In 2022, Germany had assumed the presidency of the G7. I particularly welcomed the fact that DFFT remained a priority topic under the German Presidency. For example, in their declaration[37], the G7 digital ministers underlined the importance of democratic values for DFFT and adopted a G7 action plan to promote DFFT[38]. This action plan is explicitly supported in the declaration of the G7 heads of state and government[39] and also provides for the continuation of the roundtable meetings (G7 DPA Roundtable).

It was a great honour for me to host the G7 DPA Roundtable 2022. For the first physical meeting of this format, I invited the data protection commissioners of the G7 countries, the chair of the European Data Protection Board and the European Data Protection Supervisor to Bonn in September 2022.

**G7 Leaders Communiqué can be found here:**

(Scan QR-Code or click)

The President of the Federal Cartel Office as well as representatives of the OECD and civil society also participated as guests. This roundtable focused on the main topic of DFFT, an exchange of experience and knowledge with regard to possible perspectives on international data spaces. The Communiqué 2022[40] emphasises that the promotion of DFFT includes, in particular, respect for democratic values and the rule of law. This goes hand in hand with limiting state access to privately stored data to what is necessary and proportionate in democratic societies. Discussions on DFFT focused on identifying elements of alignment between existing regulatory approaches and transfer instruments (such as standard contractual clauses, certifications and codes of conduct) in order to promote interoperability between different legal systems and instruments. Also of particular note is the work on data minimisation and purpose limitation, two fundamental principles of the GDPR that also play an important role for the data protection supervisory authorities from the UK, USA, Canada and Japan. Consistent enforcement of these principles is crucial to bring data-based business models in line with the legitimate expectations of consumers. It specifies that only the personal data required for the use of the respective service be collected. Other important topics of the exchange were the promotion of privacy-enhancing technologies, legal and technical standards for de-identification tools and the role of data protection in an ethical approach to artificial intelligence.

Although the 2021 and 2022 meetings were each part of the official G7 Digital Track, this is a stand-alone format of independent data protection supervisory authorities. It is important that they are involved in the discussions on the free movement of data. That is why, in Communiqué 2022, G7 data protection supervisory authorities encouraged their governments to ensure that dialogue between policymakers and regulators beco-

36 To be found at: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

37 The "Ministerial Declaration G7 Digital Ministers' meeting" is available at: https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration.pdf?__blob=publicationFile

38 The "G7 Digital Ministers' Track - Annex 1 G7 Action Plan for Promoting Data Free Flow with Trust" is available at: https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile

39 The "G7 Leaders' Communiqué Elmau, 28 June 2022" is available at: https://www.g7germany.de/resource/blob/974430/2062292/9c213e6b4b36ed1bd687e82480040399/2022-07-14-leaders-communique-data.pdf?download=1

40 The Communiqué 2022 is available at: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.html?nn=422292

mes an integral part of the G7 digital agenda where data protection issues are concerned. This notwithstanding, it was agreed that the annual high-level meetings would continue regardless of whether or not they are an official item on the agenda of the respective G7 Presidencies. In addition, an intra-year exchange at expert level is also planned in three new working groups on the topics of emerging technologies, enforcement cooperation and free and trusted data flows (DFFT). The working groups are preparing for the upcoming G7 Data Protection Roundtable, which will take place in 2023 under the Japanese chairmanship.

**Cross-references:**

3.3.9 EU-U.S. Data Privacy Framework (Privacy Shield successor), 3.3.10 Guidelines on approved certifications and codes of conduct as tools for third-country transfers, 3.5.1 44. Annual conference of the Global Privacy Assembly 2022

## 3.5 Other international bodies

### 3.5.1 Annual conference of the Global Privacy Assembly 2022

**For the first time since 2019, representatives of data protection authorities from around the world were able to meet again for their annual conference in person. The Turkish data protection authority had invited to the 44th annual conference of the Global Privacy Assembly (GPA) in Istanbul. Questions of principle on international data transfers and new technologies were discussed. My second term on the GPA's Executive Committee began in autumn 2022.**

After two virtual meetings in 2020 and 2021, the 44th GPA annual conference was hosted by the Turkish data protection authority "Kişisel Verileri Koruma Kurumu" (KVKK) in Istanbul from 25 to 28 October 2022. Several hundred participants gathered under the motto "A Matter of Balance. Privacy in The Era of Rapid Technological Advancement". New members include the Kenyan data protection authority and the California Privacy Protection Agency (CPPA), which was established at the level of the state of California in the USA as the first dedicated data protection authority. Accompanied by a delegation of experts, I took part in the conference and contributed in various formats.

The keynote presentations and discussion sessions, which were open to all participants, focused on advancing technological developments in the field of facial recognition, artificial intelligence and blockchain technology, as well as related challenges for data protection. Other focal points were questions on cross-border data transfers and data protection risks in the field of humanitarian aid, as well as for vulnerable groups such as children and minors. Together with the chairwoman of the French data protection authority "Commission National de L'Informatique et Libertes" (CNIL), Marie-Laure Denis, I gave a keynote speech on "Convergence of data protection rules in cross-border data transfers". Several of my colleagues from the European Data Protection Board (EDPB) participated in various presentations and discussion panels, expressing the positions of the General Data Protection Regulation (GDPR). In the closed session of the conference, to which only GPA-accredited members and observers are admitted, the working groups, the strategic direction sub-committee and various GPA members and observers reported on significant results and activities since the last annual conference in autumn 2021. In this context, I was able to report on the work of the "International Working Group on Data Protection in Technology" (IWGDPT), also known as the Berlin Group (see No. 3.5.2).

In addition, the GPA members adopted the following resolutions[41]:

- Resolution amending the roadmap and timetable for the establishment of a member-funded secretariat,
- Resolution on capacity building for international cooperation to improve cyber security regulation and understanding of the damage caused by cyber incidents,
- Resolution on the principles and expectations for the appropriate use of personal data in facial recognition technology.

From an organisational point of view, there was a new composition of the GPA's governing body, the "Executive Committee". The Jersey Information Commissioner, Paul Vane, was elected as a new member. I myself was confirmed as a member of the Executive Committee for a second term until autumn 2024. The next GPA annual conference will be hosted by the Bermuda Privacy Commissioner in October 2023.

**Cross-references:**

3.5.2 Berlin Group, 4.4.3 EDPB Guidelines on the use of facial recognition technology

41 Resolution of 28 October 2022, available at: https://www.bfdi.bund.de/gpa

### 3.5.2 Berlin Group

**After I assumed the chairmanship of the International Working Group on Data Protection in Technology (IWGDPT) on a permanent basis last year, the so-called "Berlin Group" was able to meet again this year and gain new members.**

In March 2021, I took over the chairmanship of the International Working Group on Data Protection in Technology (IWGDPT) from the Berlin Commissioner for Data Protection and Freedom of Information (cf. 30th AR, No. 3.4.2). The IWGDPT, also called the "Berlin Group" because of its history, is an international group of data protection supervisory authorities, non-governmental organisations, experts from the fields of science and research and think tanks.

After the work of the Berlin Group in 2021 was still marked by the restrictions of the coronavirus pandemic, the group was able to return to its usual rotation of two meetings per year in 2022 under my leadership in Tel Aviv and London. After focusing on smart cities and facial recognition technology in 2021, this year the group finalised the corresponding working papers. Furthermore, the topics of telemetry data and digital central bank money were taken up again, on which working papers will be adopted in the coming year.

In order to provide the Berlin Group's recommendations to companies, legislators, data protection authorities and other stakeholders even earlier, the group will increasingly look at which technologies and fields of application are about to enter the market and draft papers on them. In preparation, the relevant work of the members ("future foresight", "tech radar") was presented and discussed.

In addition to the substantive work on the aforementioned working papers, I was able to win over new participating organisations to join the Berlin Group in 2022 in discussions with international data protection authorities and interest groups, e.g., the UN Special Rapporteur on the Right to Privacy. My aim is to further increase the diversity of the group and the intensity of the dialogue, as well as to make their expertise and work results more visible.

### 3.5.3 New ETIAS advisory body on fundamental rights

**The independent ETIAS advisory body on fundamental rights has been newly established to monitor the so-called ETIAS monitoring rules. One of my staff members also represents the EDPB on this committee.**

The new European Travel Information and Authorisation System (ETIAS) is scheduled to become operational in 2023 and concerns third-country nationals who wish to enter the EU and are exempt from the visa requirement. The system aims to check whether the presence of these people poses a risk to EU security, a risk of illegal immigration or a high risk of epidemics. One means by which this check is to be carried out is the so-called ETIAS monitoring rules, a profiling algorithm based on specific risk indicators. An independent ETIAS Fundamental Rights Guidance Board has been created especially with regard to the definition and application of these risk indicators. It consists of the Fundamental Rights Officer and a representative of the Fundamental Rights Consultation Forum of the European Border and Coast Guard Agency Frontex, as well as the European Data Protection Supervisor, the European Union Agency for Fundamental Rights and the EDPB. I am pleased that the EDPB has appointed one of my employees as a representative and that he has also been elected chair of the ETIAS Fundamental Rights Guidance Board. In this way, it is possible for me to actively work towards the respect of fundamental rights, in particular the protection of privacy and personal data, as well as non-discrimination.

**Cross-references:**

3.3.4 EU systems: Central coordination of supervision in the CSC

### 3.5.4 Report from the SCGs

**In the framework of the different Supervision Coordination Groups (SCGs), the European data protection authorities and the European Data Protection Supervisor (EDPS) work together to coordinate data protection supervision of the EU's large-scale IT systems. The focus this year was on the coordination of controls, the planned digitalisation of the visa procedure, the interoperability of the various EU systems, the implementation of the new Schengen legal acts and the revision of the Schengen evaluation mechanism.**

**VIS/Eurodac SCG**

The current discussions focused on the far-reaching changes to the VIS Regulation and the Visa Information System. Legal changes have created significant opportunities for automated matching of VIS data with other systems. The circle of authorities potentially entitled to access has thus been expanded. The representatives of the data protection authorities agreed that the entire architecture of the information systems must be analysed from a data protection point of view in order to counteract risks for data subjects arising from the interoperabili-

ty of the various systems. In addition, the data protection implications of the planned digitalisation of the visa procedure were discussed with representatives of the EU Commission. The consultations on this are still ongoing.

**Visa Information System**

The Visa Information System (VIS) is a system for the exchange of visa data between the Schengen States in connection with the application for, examination of and decision on short-stay visas in the Schengen area.

**Eurodac Regulation**

Eurodac (European Dactyloscopy) is a database of fingerprints of asylum seekers and illegal immigrants apprehended in the EU to ensure the effective application of the Dublin Convention on the processing of asylum applications.

Regarding the planned amendment of the Eurodac Regulation and the associated data protection risks (e.g., lowering the age for mandatory fingerprinting from 14 to 6 years), the group adopted a letter to the European Parliament to raise its awareness accordingly. In particular, it criticised the fact that the necessity and proportionality of lowering the age were not sufficiently justified. In addition, while the group welcomed the provisions on "child-friendly consultation", it saw a lack of criteria for this wording.**SIS II SCG**

In the SIS II SCG, I deal with the coordinated supervision of the second-generation Schengen Information System (SIS II). In addition to the controls on Article 36 alerts in the SIS, a focus of work for this SCG was the implementation of the new SIS Regulations (EU) 2018/1860, 2018/1861 and 2018/1862. In this regard, I have also been intensively involved at the national level within the framework of the departmental consultations on the law for the implementation of these regulations (SIS III law). These regulations create new categories of alerts in the SIS and partially expand the collection of data for existing categories of alerts; in addition, more authorities will have access to data in the SIS. Legal and technical developments were continuously monitored by the SIS II SCG. In order to also sufficiently inform the public about significant changes in the new legal acts, for example, information campaigns as well as further information on data subjects' rights were discussed, which are currently being implemented.

Another focus of the SCG's work was the revision of the Schengen evaluation mechanism. Schengen evaluations involve a review of the Schengen states by teams composed of experts from the Member States and the Commission. National authorities are also reviewed with regard to the implementation of data protection. My staff regularly participate as experts in evaluations in other countries, this year for example in the evaluations in Norway and Iceland. The mechanism underlying these evaluations has now been adapted by Regulation (EU) 2022/922. In the run-up, I was involved in the legislative process at both national and European level. In the context of the SIS II SCG, for example, a letter was drafted to the European bodies involved in the legislative process to draw attention to relevant data protection aspects in the implementation. From my point of view, important points have been legally anchored or have been promised, such as special training for the experts.

**CIS SCG**

In this coordination group, I deal with the coordinated monitoring of the Customs Information System (CIS), in the reporting year in particular the coordinated, Europe-wide review of data protection training on the CIS by the authorities connected to the system. For this purpose, a questionnaire was first developed by the SCG, which was distributed to the responsible bodies via the national data protection authorities for their response. During my review of the Customs Criminal Investigation Office in this regard, I did not find any indications that there were deficits in data protection training. The collected national responses to the questionnaire are currently being analysed at European level.

**Cross-references:**

9.2.8. Coordinated checks on alerts for covert/targeted checks in the Schengen Information System

# 4 Main topics

## 4.1 Research data

Research is the foundation of social progress. Increasingly, research requires large amounts of data for this purpose, including personal data. Therefore, it is right that the General Data Protection Regulation gives research a privileged position. The coronavirus pandemic has shown us, sometimes painfully, that there are still major challenges, especially in research with health data in Germany; in addition to data protection issues, the focus here is on inadequate recording, incompatible data formats and insufficient digital reporting channels. As the BfDI, it was important to me to make this topic the focus of my work in the reporting period and to use various initiatives and events to promote greater understanding between the stakeholders involved and to show how more research with personal data that complies with fundamental rights can succeed.

### 4.1.1 Research with Health Data Symposium

**There were controversial and constructive discussions at the BfDI Symposium 2022. All participants agreed that changes are needed in the future, especially in research with health data. The event was so successful that further symposia are planned for the future.**

On 3 November 2022, numerous stakeholders met for the BfDI symposium with the topic "Research with Health Data – Challenges in the Sign of the General Data Protection Regulation" in the auditorium of the Kaiserin Friedrich Foundation in Berlin.

About 80 invited guests from politics, science & research, authorities and companies exchanged views with representatives of the BfDI on the status and possibilities of data protection-compliant research with (health) data. Interested citizens also had the opportunity to follow the event in parallel via a stream on the internet.[42]

**Recording of the event can be found here:**

(Scan QR-Code or click)

Particular emphasis was placed on the current legislative developments both in Europe and in Germany. The discussions were lively, controversial and at the same time constructive.

With regard to developments in Europe, it was very clearly shown that the European Commission, in its currently submitted draft regulation of 3 May 2022 on a European Health Data Space (EHDS), has not sufficiently taken into account essential legal principles (e.g., Art. 8, 52 EU Charter of Fundamental Rights), at least from the perspective of the data protection authorities. For example, it was pointed out that the circle of bodies obliged to provide data and the circle of bodies entitled to submit applications were both defined too broadly in the draft regulation. The currently envisaged obligation to provide data without exception and the insufficient granting of data subjects' rights, especially in the area of secondary data use, were also criticised.

In the course of the symposium, the speakers emphasised several times that there is still sufficient room for improvement not only in Europe, but also in Germany.

So, it is certainly to be agreed with when – as was the case several times during the symposium – the German supervisory authorities are called upon to make even more efforts towards unified legal views. The supervisory authorities are already working on this, for example, in a taskforce jointly led by the Hessian State Data Protection Commissioner and myself.

42 The recording of the event is still available at: https://www.bfdi.bund.de/aufzeichnungenhttps://www.bfdi.bund.de/DE/Service/Mediathek/Veranstaltungen/2022-Symposium-Forschungsdaten/Symposium-Forschungsdaten-2022_mit_iframe.html

Prof. Dr. Specht-Riemschneider during her lecture at the symposium on health data


However, it also became clear that the demand for uniform legal practice is not so much a matter for the supervisory authorities as for the legislator. In this regard, I pointed out several times during the discussions that the partly contradictory state hospital laws in the individual federal states, unused opportunities for national legal clarification on the research opening clauses of the General Data Protection Regulation and ultimately also an unsuccessful regulation of data protection supervision for nationwide research projects in the "wrong" legal code (Section 287a SGB V [Book V of the German Social Security Code]), still hold sufficient potential for the legislator here.

It is planned to hold the BfDI symposium regularly in future and on changing, current topics.

**Cross-references:**

5.1 European Health Data Space

### 4.1.2 Health Research Data Centre

**The project of a rese arch data centre for health data from the electronic patient record (ePA) and the data transparency procedure is progressing and approaching the home straight.**

I have already reported on the development of the Health Research Data Centre, a database with the pseudonymised billing data of all statutorily insured persons, which is maintained by the Federal Institute for Drugs and Medical Devices (BfArM) as a register office, in recent years (30th AR 6.4). The Health Research Data Centre received a new conception due to legislative changes in the Digital Care Act from 2019 and the Patient Data Protection Act in 2020 (see 28th AR No. 5.6 and 29. AR No. 7.3).

In this reporting year, I advised the Robert Koch Institute (RKI), where the trust centre responsible for the pseudonymisation of data records is located. Together with the Federal Office for Information Security (BSI), details of the procedure, the cryptographic methods, the hosting architecture as well as the delivery pseudonyms and the so-called cross-period pseudonym were dealt with, so that I was finally able to give my consent to the procedure.

Every year, the Health Research Data Centre receives the billing data of those with statutory health insurance and makes it accessible for research purposes. Various pseudonyms are used to protect data subjects from identification: the delivery pseudonym is used by health insurance companies when delivering the data sets to the Research Data Centre and replaces identifying information such as the health insurance number. The so-called cross-period pseudonym is formed by the RKI. It is used for allocation at the Research Data Centre and replaces the delivery pseudonym, and thus also the health insurance number. In the case of a data release from the electronic patient record, the cross-period pseudonym ensures the allocation in the Research Data Centre.

In the case of an evaluation by third parties, the data is always anonymised, i.e., the data set is prepared in such a way that it is not possible to draw conclusions about a person from the factual information.

In parallel, I regularly supported and advised the BfArM and the Federal Ministry of Health on the individual development steps of the register and its technical implementation. This is because a suitable anonymisation procedure tailored to the data structure, which is currently being developed on behalf of the BfArM, is essential for the safe use of the data for research purposes. To ensure optimal application to the later overall data set, I went along with the BfArM's plan to use a partial data set for development under certain conditions. The partial data set consists of the data from the reporting year 2016 and was processed in advance using special methods agreed with me in order to protect data subjects, but without losing the characteristics of the real data set.

In addition to the data from the data transparency procedure, the data from the electronic patient record that is voluntarily released for research purposes is an important data source for the Research Data Centre. Structured data, so-called medical information objects (MIO), such as vaccination certificates, can be selected for release. Before transmission to the Research Data Centre, the identifying data fields, for example, the name or date of birth, are removed or pseudonymised. I am also involved in the development of this pseudonymisation procedure.

Overall, the Health Research Data Centre project continues to make progress and is well on its way to finally being available to authorised users. Nevertheless, there is still some important work to be done and issues that need to be addressed. For example, I still miss clear regulations on the right to object.

### 4.1.3 Research Data Taskforce

**Research projects with collaborative partners in different federal states have to deal with different legal bases and supervisory authorities. In order to facilitate coordination with and among the supervisory authorities and thus ultimately support research, the Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK) has formed its own expert committee.**

The Research Data Taskforce, co-chaired by the BfDI and the Hessian Commissioner for Data Protection and Freedom of Information, was established by the 102nd session of the DSK in November 2021 as a further expert body, similar to the working groups. The aim was to provide a flexible and timely opportunity to address current issues in health research. In addition, it was intended as a point of contact for the Medical Informatics Initiative (MII), which is funded by the Federal Ministry of Education and Research, and the Technology and Methods Platform for the vernetzte medizinische Forschung e.V. association. (TMF) and to structure and facilitate their consultation.

One of the first topics was dealing with the research project RACOON, which was formed in connection with the coronavirus pandemic within the Network of University Medical Departments (NUM) and aims at the structured acquisition and comprehensive evaluation of X-ray images of the lungs. Here, the well-known problem became apparent that in the respective federal states, different regulations in the hospital and data protection laws allow or prevent the use of patient data to different extents and with different prerequisites. The meetings of the Research Data Taskforce enabled an exchange among the supervisory authorities and coordinated communication with the project promoters.

In further meetings, the work of the Research Data Taskforce was structured in relation to expected legislative proposals on research with health data. Current publications and expert reports were evaluated in four working groups. The results of the work finally led to a draft resolution for the DSK: the Petersberg Declaration.

In addition, possible adaptations and a module for the international exchange of the model texts on MII consent were discussed and deliberated.

### 4.1.4 The Petersberg Declaration

**On the priority topic of "research", the Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK) adopted two resolutions this year on my initiative. In the GDPR, research is privileged as a purpose; extensive research with personal data or data derived from it is possible with additional data protection measures. The DSK gave concrete indications above all in the Petersberg Declaration of November 2022.**

The 103rd meeting of the DSK in March 2022 adopted a resolution on the key focus of "research" ("Scientific research – naturally with data protection" and announced further proposals on this topic. As a follow-up to this conference, the Research Data Taskforce dealt with the legislative plans announced in the coalition agreement on the use of research data and on medical registers, based on legal opinions that had been written on these topics on behalf of the federal government. One of the main objectives of the Taskforce was to provide the federal government with guidance in the formulation of the draft legislation by giving it as concrete information as possible in terms of data protection law and to emphasise the importance of designing the planned research regulations in a way that complies with data protection law in order to ensure the necessary trust of data subjects. The guiding formula here can be: The higher the protection of data subjects through appropriate measures, the more extensive and specific the use of data can be.

The preliminary work of the Taskforce was the basis for the draft of a "Resolution on enabling the use of health data in scientific research in conformity with data protection", which was adopted by the 104th DSK on 23/24 November 2022.[43]

**Petersberg Declaration of 24 November 2022 can be found here:**

(Scan QR-Code or click)

This expresses key data protection concerns of the DSK:

- People must not be made mere objects of data processing. They are at the centre of research – on the one hand, they benefit from the findings; on the other, they are exposed to the possible risks. The processing operations must therefore be lawful and always transparent for data subjects. Even if the processing of their data in the public interest should be legally permitted and not based on their consent, there must always be the possibility for data subjects to participate and shape it.
- Digital management systems such as data cockpits, dashboards or portals should provide easily accessible ways for data subjects to exercise information control and participation.
- The most important protective measures include encryption, pseudonymisation by independent trusted agencies and the earliest possible anonymisation.
- The prerequisites for data access to the research community, if possible to anonymised data sets, must be checked by means of a suitable procedure (use-and-access procedure).
- Special protection requirements must be met when linking data sets from different sources. Appropriate procedures must ensure that legal and technical requirements for data use are met.
- The responsibility under data protection law must be laid down without gaps in order to make it easier for data subjects to exercise their rights.
- The DSK has also provided information on planned regulations for medical registers, for example on quality requirements, transparency and opportunities for participation. A central register of existing registers should provide a structured overview of the existing data and avoid multiple data collections with the same content. A central office could perform an advisory and pilot function with regard to the rights of data subjects.

The DSK also reiterates its call for legal regulations on research secrecy (confidentiality of personal information that has come to light), including protection against seizure of research data.

In order to enable data protection authorities to enforce compliance with data protection requirements more effectively, they should be given the possibility to order immediate enforcement of data protection supervisory measures against public bodies.

43 On the Petersberg Declaration of 24 November 2022: https://www.bfdi.bund.de/entschliessungen

**Cross-references:**

4.1.3 Research Data Taskforce

## 4.2 European Digital Rights Act

During the reporting period, the European Union adopted several new legal acts in the form of regulations in the area of digitalisation. Further legal acts are to follow, and are in part already being discussed. The declared aim is to strengthen the European economy and regulation in the digital space. Because many of these legal acts are ordinances, no national implementation is required. They apply directly and their rules must be followed by authorities, companies and private individuals. Of course, this also means that my authority has to deal intensively with the details of this European digital legal act, also in an advisory capacity for the EU Commission, the federal government and parliaments.

### 4.2.1 AI Regulation

**The European Commission presented the world's first draft legal framework for the field of artificial intelligence (AI) in spring 2021. 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. It is an important step that the principle of dealing with a regulatory framework has been initiated in this way. I will work to ensure that the principles of the GDPR are not undermined by the proposed legislation. Only in this way can an adequate legal framework emerge as a result, which effectively complements the existing rules on data protection and at the same time promotes innovation in the field of AI.**

Applications in the field of artificial intelligence (AI), algorithm-based decision-making processes and learning systems have the potential to create great benefits in almost all areas of life. In many cases, they offer solutions that would hardly be conceivable without AI. Besides the numerous potential benefits, their ever-increasing dissemination, coupled with the rapid further development of AI technologies, also harbours the danger of profound violations of fundamental rights. I have repeatedly advocated that any form of AI must be designed in accordance with data protection.

The draft for an EU Regulation on Artificial Intelligence (AI Regulation) or Artificial Intelligence Act (AI Act) is intended to provide a legal framework for these developments and thus become the first European act to regulate AI in almost all areas of life. Since April 2021, proposals have been on the table that are now part of the European legislative process and are also controversially discussed by business and civil society. The development of such a legal framework is being closely watched worldwide, as the regulations have the potential to have a fundamental impact far beyond the EU.

From the point of view of the EU Commission, the draft submitted is intended to ensure that the use of AI-based systems does not have negative impacts on the safety, health and fundamental rights of people. According to the draft regulation, AI applications are classified into four risk levels: a minimal, a limited, a high and an unacceptable risk. Depending on the classification, different approval requirements and controls are required, each with a different regulatory density. For applications that are associated with high risk, certain quality requirements are assumed, e.g., logging and documentation requirements, extensive information of users, high quality of data sets or even human supervision to minimise risks. In order to ensure security and compliance with existing legal provisions for the protection of fundamental rights throughout the entire life cycle of AI systems, comprehensive obligations are to be imposed on the providers and users of these systems. This also applies, for example, to the area of conformity assessment or the provision of information for users.

This risk-based approach provided for in the draft legal framework on AI was already welcomed in principle by the European Data Protection Board (EDPB) in a statement last year. Together with my European colleagues and the European Data Protection Supervisor (EDPS) in the EDPB, I have argued that the use of AI should be prohibited if the people's personal spheres and dignity are not sufficiently respected. As part of the EDPB's rapporteur team, I have strongly advocated the paramount importance of data protection in the design of AI (see 30th AR, No. 4.2.1). Despite the fundamentally welcome proposals for a regulatory framework in the field of AI, the EDPB, together with the EDPS, has made it clear that there is nevertheless a need for (sometimes substantial) change in several places.

For example, I am particularly critical of the possible use of AI systems to evaluate social behaviour. The procedure, also known as "social scoring", carries a high risk of discrimination. Therefore, the regulation of AI should include the prohibition of any kind of assessment of social behaviour. Furthermore, I have repeatedly advocated for a ban on AI that clusters natural persons according to biometric characteristics. Otherwise, there would be a risk of people being grouped according to ethnicity, gender, political or sexual orientation or other

characteristics that are among the grounds of discrimination prohibited under Article 21 of the European Union Charter of Fundamental Rights.

In the reporting year, several updated compromise proposals were submitted in the meantime. Currently, the EU Parliament and the EU Council are each internally negotiating the draft law prepared by the EU Commission, followed by the trialogue negotiations. The debates on the details of the regulation are, as expected, protracted due to the high complexity of the issue. I am accompanying these developments at both the European and national levels. The final form of the AI Act is expected to be decided in the course of 2023.

### 4.2.2 Digital Services Act

**The Digital Services Act (DSA), the first part of the European Commission's Digital Services legislative package to tackle illegal and harmful content online, came into force on 16 November 2022 and will apply from 17 February 2024. This also sets important impulses for data protection, which I supported in the legislative process. In the creation of the national supervisory structure for the DSA, the data protection supervisory authority should be involved for the benefit of all by respecting its independence and making use of its expertise.**

The regulations of the DSA, which is also often referred to as the "basic law of the internet", apply in particular to large online platforms, for example, large social networks. Among other things, they oblige them to significantly greater transparency and a consumer-friendly design of their services. From a data protection perspective, the regulations on the use of data for tracking and profiling in the context of online advertising are of particular importance. As I stated in my 30th AR (No. 5.9), I have advocated for a comprehensive ban on personalised advertising in the legislative process. Unfortunately, this demand did not find a majority. However, the DSA completely prohibits the use of minors' data for profile-based advertising. Advertising based on profiling using special categories of personal data pursuant to Art. 9(1) of the GDPR may also not be displayed – in this case, this also applies to the data of adults. It is a pity that this ban will not apply to micro and small enterprises.

At the suggestion of the EU Parliament, a ban on so-called "dark patterns" was also included in the DSA. I have expressly supported this ban, as it can prevent users from being manipulated by the design of apps and websites and thus possibly disclosing data that they would not have passed on if the offer had been designed differently. Although certain manipulative practices are already prohibited under the GDPR, the regulations in the DSA extend this protection.

The DSA also gives research institutions access to data from large online platforms to analyse the algorithms responsible for what content is displayed to users. It is now possible for the first time to recognise how certain processes in social networks, some of which are harmful to society, function in order to combat them if necessary. Of course, I made sure in the corresponding regulation that data protection must be respected and that no unnecessary processing of personal data is performed.

Finally, central to the effectiveness of the DSA is the supervision of the companies, which will be carried out by the Digital Services Coordinator (DSC) in Member States. Therefore, in the creation of the German supervisory framework for the DSA, I am committed to ensuring that data protection supervisory authorities can contribute their expertise in profiling as efficiently as possible and that data protection assessments are mandatorily made by the independent data protection supervisory authority in order to ensure consistent supervision.

How effective the DSA will be in practice and what concrete effects it will have on businesses and consumers is still open. However, I think that the DSA is an important fundamental step towards making online platforms, online marketplaces and search engines more secure and more privacy- and consumer friendly.

### 4.2.3 Digital Markets Act

**The Digital Markets Act (DMA), which is the second part of the EU Commission's Digital Services legislative package and aims to establish fair competition by regulating major digital platforms, came into force on 1 November 2022 and will apply from 2 May 2023. In the legislative process, core data protection requirements that I supported were included in the DMA, which further strengthen the cooperation between competition and data protection supervision.**

As was already reported in the 30th AR (No. 5.9), the cooperation of the supervisory authorities was an important concern for me during my consultation in the legislative process on the DMA in order to ensure consistent supervision in data protection matters. This is because the DMA contains both directly applicable rules of conduct with data protection relevance for large central platform services – the so-called gatekeepers – as well as rules on profiling and data portability.

I am therefore pleased that core data protection requirements, for which I have campaigned, have now also been anchored in key places in the DMA.

With the European High Level (Expert) Group, a body is created in which the European Commission as the enforcement authority is to coordinate with participating European bodies and networks. Here, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), among others, can assist the European Commission in the consistent application of the DMA and the monitoring of its compliance. In particular, this is to ensure that the level of protection of the GDPR is maintained. In my view, this cooperation is indispensable and therefore very welcome, as is, for example, the obligation to also make the description of the gatekeepers of consumer profiling techniques available to the EDPB.

In addition, the DMA regulates the interoperability of messenger services. Besides end-to-end encrypted text messages, the exchange of images, voice messages, videos and other attachments in end-to-end communication between individual end users of different messenger services must also be ensured in principle. A downstream extension in terms of end-user groups and video and voice calls will then take place within two and four years respectively after the messenger service has been designated as gatekeeper. The demand for interoperability of social network services, which I also support, has unfortunately not gained political acceptance.

Overall, I am confident that the competition supervision of large platform services, which has been significantly strengthened by the DMA, will also have a positive impact on data protection.

### 4.2.4 Data Governance Act

**With its proposals for regulation of the European single market for data, the European Commission has presented further steps towards an EU-wide regulatory framework for digital space. One of these regulations is the Data Governance Act (DGA).**

The DGA came into force on 23 June 2022 and will be applicable from 24 September 2023. The DGA pursues the creation of framework conditions for a so-called data economy in various fields of action (cf. 30th AR, No. 5.9). It aims to increase trust in data sharing.

On the one hand, it creates conditions for the dissemination of data by public bodies for general use (open data). This means that in the future, public authorities will also be able to release personal data, for example, for commercial use. 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. The latter is to be welcomed from my point of view.

On the other hand, the DGA defines services for data sharing, so-called data switching services. These services are intended to bring data providers and data users together under neutral mediation. Furthermore, framework conditions are being created to encourage Member States to create so-called data altruistic organisations. The trust in such organisations should be strengthened in such a way that citizens voluntarily give up their personal data for public welfare purposes, such as research.

In all of the DGA's regulatory approaches, the problem arises that a separate supervisory structure is to be created alongside the data protection supervisory authority, although there will be overlapping responsibilities. Together with my European colleagues and the European Data Protection Supervisor (EDPS) in the EDPB, I already drafted a comprehensive statement on this and other critical points in the last reporting year.[44]

### 4.2.5 Data Act

**My authority oversees the negotiations on European legal acts both nationally within the framework of departmental consultations and through initiatives in the European Data Protection Board (EDPB). Our focus is on the draft regulation for a Data Act (DA) because it deals in particular with the data that users generate on their networked devices.**

The European Commission presented its draft Data Act on 23 February 2022. The declared aim of the DA is to establish new rules on who can use and who has access to the data generated in the economic sectors in the EU. Among other things, the proposal includes guaranteeing users access to the data generated by their connected devices, which is often collected exclusively by manufacturers. In addition, measures are to be established to restore balanced bargaining power for small and medium-sized enterprises by preventing imbalances in data sharing contracts. Public authorities are also to be allowed access to and use of data held by the private sector in special situations.

It is clear from both the Data Governance Act (DGA) and the DA that improved framework conditions for digital business models and forms of processing are at the heart of the EU legislator's efforts. However, both legislative acts pose considerable challenges to the previous concept of data protection. It is all the more important to keep a careful eye on these planned framework regulations for so-called data markets with regard to the

44 Statement 3/2021, available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_de

risks in the form of a mass exchange of data, including personal data, and its evaluation, especially for purely commercial purposes.

I have repeatedly argued that the principles of the GDPR should not be undermined by either the DA or the DGA. According to the EU Commission, the GDPR will remain unaffected by the new legal acts. However, there are many ambiguities in relation to and regarding the impact on the GDPR.

In addition, both the DGA and the DA have other intersections that will have a very significant impact on data protection in the EU as a whole. The aim of my advice is to draw attention to these problems and to work towards a 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. Together with my European colleagues and the EDPS in the EDPB, I have drafted a comprehensive statement on this and other critical points, such as the planned supervisory structure in the Data Act.[45]

In the reporting year, several updated compromise proposals on the DA have now been submitted in the meantime. Currently, the EU Parliament and the EU Council are each internally negotiating the draft law prepared by the EU Commission, followed by the trialogue negotiations. As expected, the debates on the details of the regulation are difficult due to the high complexity of the issue. Of course, I am following these developments at both the European and the national level. The final design of the DA is expected to be decided by the end of the current legislative period of the EU Parliament (2024).

**Cross-references:**

4.2.4 Data Governance Act

### 4.2.6 Political Advertising Ordinance

**The European Commission has presented a proposal on transparency and targeting of political advertising, which is also relevant to the area of data protection law.**

On 25 November 2021, the European Commission presented its proposal for a regulation on transparency and targeting of political advertising (Political Advertising Ordinance). The Commission's aim is to use the regulation to establish new Europe-wide rules to protect electoral integrity and promote democratic participation. The envisaged regulations also concern data protection aspects.

Among other things, the draft proposes a "transparency seal", according to which paid political advertising must be clearly labelled and contain a range of important information. In addition, the proposed regulation provides for stricter requirements on the targeting and amplification of political advertising that uses or derives sensitive personal data such as ethnic origin, religious beliefs or sexual orientation. According to the Commission's idea, these techniques should only be permitted in such cases with the consent of the data subject.

In my view, the proposed ban on targeting and amplification in the context of political advertising does not go far enough. I have repeatedly advocated for a complete ban on the use of any form of personal data for targeting, amplification and ad delivery in relation to political advertising. Such a ban serves in particular to protect users in the online space, who are often not even aware of such use of their data. Moreover, such a ban serves to protect the integrity of free elections and ensures that open, pluralist debate is guaranteed as a pillar of European democracy. Of course, I am also committed to ensuring that the principles of the GDPR and the regulations of the Digital Services Act (DSA) on personalised advertising are not undermined by the regulation.

In the reporting year, several updated compromise proposals were also presented regarding the regulation of political advertising. I am naturally following these developments at both the European and the national level. It is not yet possible to predict when the final form of the Ordinance will be available.

**Cross-references:**

4.2.2 Digital Services Act

## 4.3 Digital media

Digital media and services have long since become an integral part of our everyday lives. From a data protection perspective, it is crucial that these services are made legally compliant. This is all the more true for authorities, as they are supposed to be role models of behaviour. It is precisely for this reason that I repeatedly receive submissions and complaints from citizens when this is not the case. Data protection supervisory authorities in Germany and the EU are now enforcing decisions to eliminate legal uncertainties and non-compliant behaviour.

45 Statement 2/2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en

### 4.3.1 Facebook fan pages proceedings

**In May 2022, the BfDI initiated proceedings against the Federal Press Office due to problems under data protection law in connection with the operation of the Facebook fan page for the Federal Government.**

A fan page (also "Facebook pages") is a type of home page published by Facebook. The content does not originate from Facebook, but from the operators of the fan page. When visiting a Facebook fan page, extensive personal data about the surfing behaviour of users is collected in order to monetise this information via advertising. This surveillance not only affects registered Facebook users, but also people who do not have a Facebook account.

I am aware of the importance of social networks for the public relations work of the federal authorities. Nevertheless, authorities are particularly required to act in a legally compliant manner. The important task of public relations cannot justify profiling and processing personal data for marketing purposes. Therefore, and due to their status as role models, the data protection supervisory authorities are now taking them to task as a matter of priority.

I have already drawn the attention of the federal public authorities to the data protection concerns about the operation of Facebook fan pages on several occasions, and have called for remedial action to no avail. The results of the brief expert opinion on the conformity of the operation of Facebook fan pages with data protection law of 18 March 2022 by a taskforce appointed by the DSK confirmed the view that data protection-compliant operation of fan pages is not possible. After previously announcing that I would investigate the use of Facebook fan pages by federal authorities, I initiated remedial proceedings against the Press and Information Office of the federal government (Federal Press Office) in May 2022. As a first step, I sent a hearing letter to the Federal Press Office with questions about the operation of the federal government's Facebook fan page. I checked the answers received from the Federal Press Office. At the time of going to press, I have not yet made a decision on a possible remedy, but I assume that this will happen in the first quarter of 2023.

The Facebook Fan Pages Taskforce revised the short report on the occasion of changes to the privacy policy and the terms of use as well as Facebook's cookie banner.[46] However, this update does not change my data protection assessment of the operation of Facebook fan pages.

**In our opinion, it is still not possible to use Facebook fan pages in a way that complies with data protection laws. I therefore recommend switching off the fan pages.**

### 4.3.2 Decisions of European supervisory authorities (SAs) on Google Analytics

**Since the turn of the year 2021/22, various European supervisory authorities have made decisions on the tracking tool "Google Analytics".**

Immediately after the so-called Schrems II ruling of the ECJ[47], the European Data Protection Board (EDPB) set up a Taskforce (TF) to deal with 101 complaints lodged by the NGO "Non-of-your-business (NOYB)" with various EU and EEA supervisory authorities. The complaints all related to the issue of data transfers when a variety of website operators use Google Analytics and Facebook Connect. NOYB complained that such use leads to the transfer of personal data to the USA. According to the findings of the Schrems II ruling, this was not to be considered in conformity with data protection. The established TF started its work shortly after receiving the complaints. Germany is represented in this TF by various supervisory authorities.

46 The short report of 10 November 2022 can be found at www.bfdi.bund.de/entschliessungen

47 Schrems II Judgment of the ECJ (C-311/18) v.16.07.20, available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=40595668

In the meantime, various European supervisory authorities have issued decisions on the complaints submitted to them. In addition to the Austrian SA, the French and Italian SAs have published their decisions on Google Analytics[48]. In the decisions, the authorities found that the facts presented in each case did not comply with the GDPR. In their reasoning, they stated that the requirements of Chapter V of the GDPR for an adequate level of data protection in the US were not met in light of the requirements of the Schrems II ruling. The additional measures required by the ECJ (so-called "supplementary measures") were also assessed by the SA as insufficiently effective, as they could not guarantee that possible access by security authorities would be prevented. The implementation of such supplementary measures had been demanded by the ECJ in the Schrems II ruling in order to ensure a level of protection essentially equivalent to Union law in individual cases. The French and Italian SAs set deadlines for the respective website operators to bring their processing operations into compliance with the GDPR. The Austrian SA did not make a final decision because it transferred the case to a German SA due to a change in jurisdiction. The EDPS had also published a decision in connection with Google Analytics, in which it also deemed the use of Google Analytics to be unlawful.[49]

### 4.3.3 Use of a content distribution network (CDN) for the 2022 census website

**In spring 2022, I received a large number of complaints from citizens that the Federal Statistical Office was using a US-based service provider for the content distribution network of the 2022 census home page. In cooperation with the Federal Statistical Office and the Federal Information Technology Centre (ITZBund), I was able to ensure that no sensitive census data was transmitted via the network of this service provider, thus also eliminating the risk of foreign security authorities accessing census data.**

Since the Schrems II decision of the European Court of Justice (Case C-311/18), possible transfers of personal data to third countries where a level of protection comparable to the European level of data protection is not guaranteed have received increased public attention. The European Data Protection Board already developed and published recommendations on this topic in 2020. These provide guidance to data exporters (controllers or processors) on how to determine, for ongoing or planned processing of personal data, whether any data transfers to third countries comply with the requirements of the General Data Protection Regulation (GDPR) in the absence of an adequacy decision by the European Commission for the third countries concerned. To this end, I had already sent a corresponding information letter to the public agencies of the federal government as well as the companies subject to my supervision in autumn 2020. I have already reported on the topic of third-country transfers in my last Activity Report (see 30th AR, No. 3.2.2).

In spring 2022, I received a large number of enquiries and complaints from citizens who had noticed that the home page of the 2022 census was hosted by a US-based content distribution network. The enquiries often referred to the publication by IT security researcher Mike Kuketz.[50] CDN services are used when a particularly high volume of demand is expected for certain websites, so that the operator of the website fears that the bandwidth of its own network connection or the performance of its own systems might not be sufficient to respond to the high number of requests. In this process, the contents of the websites are no longer delivered by the actual operator, but stored by the operator of the CDN and transmitted to the browsers of the users. Depending on the type of web offer, any feedback such as form entries or uploaded documents are first transmitted via the CDN network or processed there.

For the website of the 2022 census, the ITZBund had commissioned a US-based provider of CDN services to host it on behalf of the Federal Statistical Office in anticipation of a high volume of requests. After investigating the matter in cooperation with the ITZBund, I was able to achieve in the short term that login information and form data were in any case transmitted directly to the ITZBund without passing through the CDN service provider's networks. The entry page itself was still delivered by the CDN service provider for a while, so that when the 2022 census home page was called up, the IP address of the browser was still processed by the CDN provider. After the end of this transitional period, the 2022 census home page has been fully connected directly via the ITZBund since autumn 2022.

In this context, I also advised the ITZBund and the Procurement Office of the Federal Ministry of the Interior

48 Austrian SA decision available at: https://www.dsb.gv.at/download-links/bekanntmachungen.html; French SA decision available at: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply; Italian SA decision available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9782874#english ; https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9782890

49 Decision of the EDPS available at: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf

50 Blog post on CDN services, available at: https://www.kuketz-blog.de/zensus-2022-statistisches-bundesamt-hostet-bei-cloudflare/

on the preparation of a tender for CDN services.[51] The aim here was to ensure, through a suitable formulation of the call for tenders, that submitted tenders also comply with data protection requirements from the outset.

**Cross-references:**

8.8 2020 census

## 4.4 Use of AI in the security sector

Artificial intelligence (AI) is often cited as the most important topic of the future. Yet there are already processes today in which AI has long played a central role, even if many aspects are not regulated at all. Particularly in the security sector, where a lot of data, some of it sensitive, is processed, the use of AI must be looked at very carefully. That is because there are consequences here that have a direct and significant impact on the lives of citizens. This is shown by the issues that my authority dealt with during the reporting period.

### 4.4.1 CSAM Regulation

**European lawmakers plan to require messenger and hosting service providers to find online child sexual abuse material (CSAM) by screening all private communications and files. The project is highly problematic from a data protection perspective.**

The European Commission presented a draft regulation on preventing and combating child sexual abuse on 11 May 2022. Providers of messenger and hosting services are to be obliged to screen all communications or data of their users for material showing child sexual abuse (so-called CSA material). In addition, the scanning of messages is intended to detect advances by adults towards children with the intention of sexual abuse (so-called grooming). Besides reading text messages, the draft also provides for the interception of audio communication.

Even though the goal of stopping the online spread of child sexual abuse is an extremely important one, the European Union (EU) legislator's proposal clearly overshoots this goal. This is because the so-called "chat monitoring" offers hardly any protection for children, but would be Europe's entry into unrestricted, comprehensive surveillance of private communication.

In my opinion, the draft regulation respects neither the requirements of proportionality nor the fundamental rights to which German citizens are entitled under the EU Charter of Fundamental Rights (Charter) and the Basic Law (GG). The proposal threatens to break end-to-end encryption by scanning the content of private communications of those services that have received a so-called discovery order from the competent authority across the board. There are no exceptions to such scanning, not even for professional secrecy holders. This means, for example, that confidential communication between lawyers and their clients or between doctors and their patients would also be covered. Breaking end-to-end encryption threatens security to create gaps that could also be used by criminals. As an alternative, services should be able to read content directly on the user's device (so-called client-side scanning). This leads to blatant violations of respect for private life under Article 7 of the Charter and of the secrecy of telecommunications under Article 10(1) of the Basic Law.

Furthermore, the technologies that are to be used to uncover CSA material still have error rates of up to 12 per cent in some cases. This means that for a service such as WhatsApp, with a total of around two billion users, up to 240 million users could be falsely accused of disseminating CSA material.

Data protection supervisory authorities should only be able to participate with non-binding statements before the respective technologies are deployed. However, once a technology is deployed, participation is no longer foreseen. I consider this limited role of the data protection authorities to be insufficient in the case of such serious, threatened encroachments on fundamental rights.

An EU centre, yet to be established, is to maintain a database of suspected cases, collecting reports of abuse received. These will be checked by the EU centre and forwarded to the national law enforcement authorities.

Finally, the draft regulation also provides for mandatory age checks by app and software stores and in some cases even the exclusion of certain age groups from software applications. As a result, this leads to unwanted censorship and makes it partly impossible to use the internet anonymously or pseudonymously. Lifting anonymity would have serious consequences, especially for opposition members or whistle-blowers.

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) criticised the draft regulation very sharply in a joint statement in July 2022.[52] I agree with this and, together with my European

51 Statement of the BfDI of 26 August 2022 available at: www.bfdi.bund.de/stellungnahmen

52 EDPB statement on the draft CSAM regulation, available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

colleagues, I am campaigning for a significant improvement of the regulation. Fundamental rights must be respected and must also always apply to data protection and the protection of the secrecy of telecommunications. Unless the EU legislator significantly improves the draft regulation, I will work to ensure that the regulation is not adopted in this form.

**I recommend that the federal government press for a substantial revision of the draft regulation on chat monitoring in compliance with fundamental rights, and otherwise reject the draft regulation altogether.**

Cross-references:

3.3.1 General report from the EDPB

### 4.4.2 Results of the consultation process on artificial intelligence

**In the reporting year, I published the report on the results of the consultation process – a step towards a necessary public debate. Further concrete measures must follow.**

The results of the consultation process I conducted on the use of AI in law enforcement and security are now available. I published the consultation report with my assessment of the factual and legal situation together with the comments received on my website.[53] I would like to take this opportunity to thank all participants in the consultation for their important input.

**Consultation report with my assessment of the factual and legal situation can be found here:**

(Scan QR-Code or click)

The consultation revealed that AI is already in use in the area of law enforcement and security and is becoming increasingly important in view of the ever-growing amounts of data.

The matter is very complex. Most importantly, the use of AI can have a significant impact on citizens' fundamental freedoms. Therefore, the issue urgently needs to be discussed in public. The consultation participants were largely in agreement on this. There was also agreement that the issue must be approached in a differentiated way.

The legislator is required to legally "fence off" the use of AI. For this, a comprehensive, empirical and interdisciplinary stocktaking by the legislator is indispensable. I suggest that an expert commission be set up, to which I would be happy to contribute my expertise.

At my suggestion, the Conference of Independent Federal and State Data Protection Supervisory Authorities commissioned the Working Group on Security to take stock of how AI is used in current law enforcement and security practice in Germany.

**In order to legally secure the use of AI in the area of law enforcement and security, I recommend that the legislature conduct a comprehensive, empirical and interdisciplinary review by a commission of experts.**

### 4.4.3 EDPB guidelines on the Use of Facial Recognition Technology

**The European Data Protection Board (EDPB) has published guidelines for the use of facial recognition technology by security and law enforcement agencies. The results of the public consultation allow for a positive interim assessment.**

The EDPB issued extensive guidelines on the use of facial recognition technology by security and law enforcement agencies for public consultation in May 2022. They are available on the EDPB website and initially only in English ("Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement"). All contributions from the public consultation are also available there.

The guidelines first introduce the functionality and fields of application of facial recognition technology and then address the relevant legal foundations. The focus here is on the special features that apply to security and police authorities in this context. The guidelines also contain supplementary working aids, for example for planning and implementing projects with facial recognition technology, and a presentation of practical examples.

In addition to the known problems of false results and possible discrimination, the use of automated facial recognition by security and law enforcement agencies such as the police also harbours an enormous potential for abuse (30th AR No. 4.2). I therefore expressly support

53 www.bfdi.bund.de/konsultation-2021

the fact that the EDPB reiterates in these guidelines its demands, which it already advocated in its statement on the EU Commission's draft AI regulation (30th AR No. 4.2.1). These include, in particular, the general ban on remote biometric identification in publicly accessible spaces and the application of facial recognition technology to indiscriminately collected bulk data.

Through the public participation process, numerous NGOs and Member State police and government agencies, as well as stakeholders from academia and business, have now commented on this first draft of the guidelines. The overall picture of the contributions allows for a positive interim assessment and shows that the guidelines are already essentially supported and approved of in their current form. The contributions shed light on the draft from a wide variety of perspectives and thus provide a valuable source for further improvement of the guidelines.

With this in mind, I will continue to lobby the EDPB to take into account the findings of the public consultation and finalise the guidelines. I played a leading role in drafting the guidelines.

**Cross-references:**

4.4.2 Results of the consultation process on artificial intelligence

## 4.5 Evaluation of the JHA Directive and insufficient remedial powers of the BfDI in the areas of security and law enforcement

**On 25 July 2022, the European Commission published its first report on the evaluation of the JHA Directive. It had consulted the EDPB in advance. Overall, the Commission draws a positive conclusion. Nevertheless, it also notes deficits in implementation, e.g., in Germany. In this context, two infringement proceedings were opened against the Federal Republic in summer 2022.**

Almost six years after the entry into force of the JHA Directive, the European Commission submitted its first report on the implementation of the JHA Directive in the Member States to the European Parliament and the Council at the end of 2021[54]. The Commission had involved the EDPB, among others, in its preparation last year. With my participation, an EDPB contribution to the evaluation has been drafted, which was adopted by the EDPB plenary meeting in December 2021[55]. The European Commission took up many of the EDPB's recommendations in its report. For example, it was unanimously pointed out that the effective implementation of the tasks envisaged in the JHA Directive requires the availability of sufficient human and technical resources. In addition, Member States would have to ensure that the resources of the supervisory authorities are increased in line with their workload.

Even if experience is still limited due to the short time since its entry into force, the European Commission notes overall that the JHA Directive has contributed to a high degree to raising awareness and strengthening data protection awareness among the competent authorities and basically ensures a high level of data protection.

The importance of the JHA Directive for the protection of personal data is highlighted with regard to the increasing number of data transfers to third countries in the context of cross-border law enforcement cooperation. In particular, the ongoing work on the guidelines on Art. 37 JHA Directive (data transfer subject to appropriate safeguards), in which I am involved as rapporteur-general, is mentioned as important guidance for competent authorities. However, there are still deficits in the implementation of national legislation. In this respect, the Commission announces that it will continue to monitor the implementation of the JHA Directive in the Member States on an ongoing basis and work towards full implementation in the Member States with the means at its disposal. In its evaluation report, the EDPB also pointed out that the implementation of the JHA Directive has not yet been completed in all Member States or that national regulations only insufficiently implement the requirements of the JHA Directive.

In this context, the European Commission has initiated two infringement proceedings against Germany.

The first was opened in April 2022. The European Commission criticises the fact that the JHA Directive has not yet been implemented in the area of the Federal Police. The current Federal Police Act is currently being revised and is to be replaced by a new version. The legislative process on this has not yet been completed at the time of going to press.

The second procedure was opened in May 2022. The European Commission criticises the inadequate implemen-

54 Report on the implementation of the JHA Directive, available at https://ec.europa.eu/info/files/communication-first-report-application-and-functioning-data-protection-law-enforcement-directive-eu-2016-680-led_en

55 Evaluation by the EDPB, available at: https://edpb.europa.eu/news/news/2021/edpb-adopts-contribution-evaluation-law-enforcement-directive-spe-project-plan_de

tation of Art. 47(2) of the JHA Directive. This provides that data protection supervisory authorities must have effective remedial powers. These requirements would not be met by the regulations serving to implement the JHA Directive at the federal level as a whole. The same applies to the implementation in a large number of federal states.

My recommendation from the 26th Activity Report 2015 – 2016 to regulate the powers of the supervisory authorities in the scope of application of the JHA Directive analogously to the GDPR (cf. 26th AR No. 1.2.2), has not yet been followed by the legislator at federal level. Section 16(2) of the BDSG provides for information and investigation powers. However, when it comes to remedial action, I am limited under this provision to a preventive warning to the responsible party or a legally non-binding objection to the competent supreme federal authority. The current versions of the Federal Criminal Police Office Act (BKAG) and the Customs Investigation Service Act (ZfDG) do provide for a power to issue orders in addition to the provisions of the BDSG. However, this can only take place after a complaint has been made and only in the case of "significant data protection violations". Referring to the respective explanatory memoranda to the law, the Federal Ministry of the Interior also disputes that the power to issue orders also includes the deletion of personal data that has been processed unlawfully (cf. explanatory memorandum, Bundestag document 18/11163, p. 130).

I therefore welcome the initiatives of the European Commission, with which it is working towards implementation in Germany in conformity with the Directive. In this context, it is particularly important to me that the supervisory powers are implemented in German law in a way that ensures in a legally secure manner that I, as the supervisory authority, can take comprehensive and effective remedial action in the event of unlawful data processing.

# 5 Legislation

Legislation did not stand still in 2022 either. According to the Rules of Procedure of the Federal Ministries, as the Federal Commissioner, I must be involved at an early stage in all projects that concern my area of responsibility, i.e., the processing of personal data. Unfortunately, the involvement was often not timely, which I had to criticise repeatedly in cases. It is obvious that an early involvement of my office not only gives me the opportunity to work towards fundamental rights-friendly regulations already in the drafting phase, but also protects the drafters from making incorrect preliminary basic decisions that can only be corrected later at great expense in terms of time and money.

Particularly as a result of digitalisation, legislative activity and thus my advisory work continued to increase: In 2022, my authority dealt with 119 draft laws, 109 regulations, 33 directives and 12 other projects that were initiated nationally, but also by the EU. The advisory services range from an initial exchange on key points to draft bills and support in the parliamentary advisory procedure with detailed comments to the Bundestag, including participation in public hearings. Depending on the stage and the desire for consultation, counselling takes place informally or confidentially, as well as publicly. The following examples of particularly relevant legislative consultations are exemplary and represent only a very small part of the daily advisory work of my office.

## 5.1 European Health Data Space

**The European Health Data Space (EHDS) aims to create a common European regulatory framework for the use and exchange of health data. It holds opportunities for strengthening health care and medical research, but is also a challenge in terms of data protection law.**

The EU Commission presented its draft for a "legal act on a European health data space" on 3 May 2022. The EHDS is to become the first of several sector-specific data spaces within the framework of the European Data Strategy. It aims to give citizens control over their health data via a digital interoperable format. They should be able to access prescriptions, laboratory results, discharge reports and vaccination records, among other things. In addition, it should become possible for them to grant or restrict access to their data vis-à-vis service providers such as doctors, hospitals and pharmacists. The project concerns electronic patient records, medical software products and wellness apps. In addition, the draft regulation provides numerous regulations for secondary use of health data for research and innovation.

According to the GDPR, health data is subject to a general ban on processing, for which, however, exceptions are provided. From a data protection perspective, the EHDS is therefore highly relevant.

There are completely different health systems within the EU Member States, not only in terms of the level of digitalisation. In order to ensure the rights of citizens, uniform data protection standards must therefore be created in equal measure. Due to the federal system in Germany, this applies, for example, to the various hospital laws of the individual federal states. Uniform standards are also needed from a technical point of view, for example to enable interoperability.

With the strengthening of medical research through the EHDS, there is an opportunity to improve treatment options, especially for severe diseases. However, the civil liberties of citizens must be adequately taken into account, which has not been done sufficiently in the draft EHDS regulation so far. In my previous comments on the draft regulation (as of 3 May 2022), I have therefore drawn particular attention to the following points:

- Citizens must be given the right to choose to what extent they want to use digital services at all.
- The EHDS must be fully compliant with the provisions of the GDPR; this concerns in particular data subject rights and the principles of proportionality and data minimisation.

- The secondary use of health data for research and innovation requires the active participation of data subjects. So, either their consent must be obtained or they must at least be given an unconditional right to object.
- The draft regulation is also in urgent need of substantive adjustments with regard to legal definitions, the minimum categories of health data for secondary use and the role of data protection supervisory authorities.

The legislative process should be completed in 2024 with the approval of the Council and endorsement by the EU Parliament, and the EHDS should then enter into force in 2025. I will continue to work to ensure that the right to informational self-determination is upheld, especially in the area of sensitive processing.

## 5.2 Regulations for dealing with the COVID 19 pandemic

**In "year 3" of the pandemic, there were also new regulations for combating the pandemic with new data protection challenges. In the proceedings, the periods granted for submission of observations were often far too short. The number of constant amendments and adjustments, as well as rudimentary justifications in some cases, made it even more difficult for me to advise the federal government properly and also jeopardised the quality of the legislation.**

In June 2022, in preparation for the COVID-19 situation in the upcoming autumn and winter, the Federal Ministry of Health (BMG) sent a first draft of a formulation aid for the Act to Strengthen the Protection of the Population and in Particular Vulnerable Groups of Persons from COVID-19 (COVID-19-SchG). Various amendments and revisions reached me regularly in the course of the procedure, but the observation submission periods were often far too short. This is a bad habit that I already criticised last year; for this year, however, I had hoped for a return to an orderly procedure with appropriate deadlines – unfortunately in vain. Among the annoyances that made it considerably more difficult for me to examine and advise were, for example, that in individual cases the BMG sent out adjustments at the weekend or in the middle of the night and without notice with deadlines of only a few hours. In addition, the background of the adjustments was often not presented in a comprehensible way in the updated draft versions.

The management of the COVID-19 epidemic cannot be achieved without pandemic measures such as vaccination and testing, and the numerous collections, storage, transmission and analysis of health data that accompany them. These are subject to special protection under the General Data Protection Regulation for good reason. In order to ensure the necessary legal certainty, the integrity required under data protection law and ultimately the acceptance of the processes, the early, transparent and constructive involvement of my institution should therefore be a matter of course and in everyone's interest. With proper deadlines, it would also be possible to develop and offer legally compliant and more data protection-friendly alternatives to critical proposals, which could then also withstand a possible judicial review.

**Employee data protection**

At least with regard to employee data protection, it is gratifying that my criticism of the originally too vague and broad formulations in Sections 34 et seq. of the Infection Protection Law (IfSG) of the first draft of the COVID-19-SchG was finally taken up. Thus, Section 23a IfSG was initially meant to be deleted and replaced by general, overly comprehensive employer powers to process both test data and data on the vaccination and zero status of employees with regard to insufficiently determined diseases. In the final version of the Amendment Act, this processing power was ultimately limited to institutions of care and integration assistance, formulated more specifically and restricted to 2G data (vaccinated or recovered status). The provision of Section 23a IfSG was also retained.

The general authority of employers to process 3G data ("vaccinated, recovered, tested") before entering the workplace according to Section 28b IfSG, which had been inserted by the Act to Amend the Infection Protection Act and Other Acts on the Occasion of the Repeal of the Determination of the Epidemic Situation of National Significance of 22 November 2021 (29th AR No. 4.1.4), was also omitted. It was only valid up to and including 19 March 2022. All 3G data previously collected on this basis was to be deleted. Since then, general 3G access controls based on the Infection Protection Act are no longer permitted. In individual cases, however, there are still specific statutory authorisation bases for the processing of, for example, 2G data of employees by employers, such as within the framework of Section 23a InfSG or, in the case of the institution-related vaccination obligation, according to Section 20a InfSG.

I have always pointed out that the processing of sensitive 3G data of employees is only allowed in cases regulated by law. The employer's duty of care in conjunction with Section 26(3) BDSG does not permit the processing of employee health data.

When it came to reporting coronavirus tests, the draft law initially contained a case-related reporting obligation for negative test results. Contrary to my recommendation, such reporting with a pseudonym had already been introduced with the Second Pandemic Protection Act and repealed again with the Third Pandemic Protection Act (29th AR No. 4.1.4). In the current attempt, too, the purely statistical considerations in the justification could only explain collection of the number, but not assignable, case-related collection. In fact, however, the specification of case-related pseudonymisation was then waived.

Unfortunately, the federal government did not use the COVID-19 SchG to be able to base essential measures and fundamental regulations in connection with the challenges with COVID-19 on statutory regulations. For example, the amendment to the Infection Protection Act created the possibility of allowing access restrictions in connection with 3G certification checks, provided that an epidemic of national importance has been identified by the Bundestag. I had recommended that the situation-based permissibility of access restrictions as a result of 3G certification checks be regulated in the law, as this is expedient for reasons of legal clarity and certainty, and may be necessary for public bodies in particular. Following on from this, the amendment to the law would have had to provide for confidentiality requirements for the corresponding data processing procedures by private parties, which are missing but which are mandatory from the perspective of data protection law.

Like the report of the committee of experts according to Section 5(9) IfSG – Evaluation of the legal basis and measures of the pandemic policy – I had also repeatedly called for statutory regulations instead of regulations by ordinance on the occasion of the enactment of legal ordinances. It follows from the constitutional requirement of materiality that the legislature itself regulate the purpose, scope and nature of the interference with the right to informational self-determination. I would have more than welcomed it if the federal government had taken the opportunity with the COVID-19-SchG, for example, to transfer the relevant regulations from the Ordinance on Protection against Entry-Related Infection Risks with regard to the SARS-CoV-2 Coronavirus, which obliged entrants to transmit the 3G certificates to carriers and imposed a corresponding control obligation on the carriers, into statutory regulations. No confidentiality requirements were imposed on carriers with regard to data processing in connection with 3G certificates. Once again, the increased level of protection of this health data was not adequately taken into account. The interplay with the 3G certificate checks by the Federal Police as well as electronic entry declarations also resulted in duplicate data collection and storage, which could certainly have been handled in a data protection-compliant manner.

At this point, I renew my repeatedly expressed offer, but also my expectation of the federal government to involve me at an early stage and to provide me not with cursory examinations, but with comprehensive, reliable advice, true to my legal mandate.

## 5.3 Changes in anti-money laundering and enforcement of sanctions

**In the last few years, I have been involved in several legislative procedures on the Money Laundering Act (GwG) with extended powers for the Financial Intelligence Unit (FIU). With the Sanctions Enforcement Act II, a central office for sanctions enforcement with extensive powers to process personal data is now to be established. However, as before, data protection requirements were only insufficiently taken into account.**

The fight against money laundering and the financing of terrorism constitutes a legitimate purpose, which is in principle also suitable to justify serious encroachments on fundamental rights. However, the GwG has undergone a number of changes in recent years that violate essential principles of data protection law.

The Financial Market Integrity Strengthening Act (FISG) of 2 June 2021 granted the FIU the power to automatically retrieve basic tax data that it could previously only request from the tax authorities by way of individual requests. I have been critical of this during the legislative process. In my view, the provision of Section 30(5) GwG, as amended by the FISG, violates the principle of proportionality as it is based solely on the FIU's performance of its tasks and does not set any limiting thresholds for intervention.

The goal of effective enforcement of sanctions also has my full support, not least because of the war of aggression against Ukraine. However, the Sanctions Enforcement Act I once again contained a problematic extension of the FIU's powers. The latter can now also carry out further analyses at its own discretion, irrespective of the existence of a suspicious money laundering report. The details of the planned evaluations, possible reasons, the data to be included and the permissible purposes remain unclear in the law, which is not compatible with the requirement of clarity and specificity. In contrast, a consistent adaptation of the GwG to the requirements of Directive (EU) 2016/680 (JHA Directive) and the cons-

titutional court case law on the right to informational self-determination has so far failed to materialise. Since the deadline for the implementation of the JHA Directive already expired in May 2018, I consider implementation in the GwG to also be in the interest of the federal government.

The Sanctions Enforcement Act II recently created a Central Office for Sanctions Enforcement (ZfS), which is allowed to process a large amount of personal data. It is given access to police and intelligence information, among other things. In addition, personal property data is to be made available with the help of the transparency register. Here, I fear that it could be used inappropriately to bridge the completion of the electronic database land register of the federal states. It is true that some improvements in data protection were achieved within the framework of the legislative process. For example, the ZfS may only cooperate with the intelligence services if there are actual indications of certain particularly serious criminal offences. Overall, however, the law passed on 1 December 2022 still has considerable deficits in terms of data protection law.

Overall, I urgently recommend that both the GwG and the Sanctions Enforcement Act be adapted to data protection requirements.

## 5.4 Whistle-blower Protection Act

**On 16 December 2022, the Bundestag passed a resolution to improve the protection of whistle-blowers in their professional environment.**

The Act adopted on 16 December 2022 transposed Directive 2019/1937 (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (Whistle-blowing Directive) into national law. The Directive creates for the first time Union-wide minimum standards for the individual protection of whistle-blowers and for the institutional handling of the inside information they disclose. With this, the federal government aims to better protect whistle-blowers in their professional environment. Anyone who reports anti-constitutional statements or other violations of national or European legislation in connection with their professional activity is now covered by the Whistle-blower Protection Act and is thus protected from reprisals. The focus of the law is on the design of internal and external reporting offices, which offer whistle-blowers the choice of a contact point for their reports. The identity of the person providing the information must be kept confidential in both cases. It should also be possible to submit anonymous tips. If the contact point has not processed the tip-off within a certain period of time, or if the whistle-blower can reasonably assume that the information may pose an immediate or obvious threat to the public interest, the newly created safeguards will also apply if the whistle-blower discloses the information publicly.

In the event of a violation of the prohibition of reprisals, there will in future be an obligation to pay damages on the part of the perpetrator. Penalties are also imposed if a company fails to set up an internal reporting office despite a legal obligation to do so, or if communication between the whistle-blower and the reporting office is obstructed.

I welcome the implementation of the Whistle-blowing Directive. Private individuals who are willing to report violations of the law and serious abuses from their professional working environment on their own initiative are acting in the interest of democratic societies based on the rule of law. Whistle-blowers thus contribute to greater transparency and to strengthening freedom of information in areas of employment that are largely opaque for the public, but often extraordinarily consequential for key social goals and values. This also and especially applies to abuses in the handling of citizens' personal information and data by governmental and non-governmental agencies alike. A range of personal data is processed when reports are made by whistle-blowers.

I welcome the fact that the scope of application has been extended, at least to a limited extent, to corresponding national law and that, in particular, information concerning violations of all prohibition norms of criminal law and the law on administrative offences have been included. This avoids contradictions in values and makes the practical application of the law more manageable for whistle-blowers.

## 5.5 Consent management services

**Even more than a year after the Telecommunications Telemedia Data Protection Act (TTDSG) came into force, there is no legal ordinance on "recognised consent management services" with which internet users should be able to manage their consents, e.g., to cookies, in a user-friendly way.**

In my last Activity Report (30th AR No. 5.1), I reported on the entry into force of the TTDSG on 1 December 2021. It is gratifying that Section 25 of the TTDSG transposes the provisions of Directive 2002/58/EC (ePrivacy Directive) in conformity with the Directive, according to which

the storage of information on end devices or access to information already stored there – for example, through cookies – generally requires consent. At the same time, Section 26 TTDSG introduced the possibility of using recognised consent management services. These are intended to enable internet users to manage consents (and thus also refusals of consent) in a user-friendly way. I expressly welcome the approach taken to curb "cookie banners". However, a lowering of data protection standards must not go hand in hand with such services, and they must not be seen as a means to achieve more, and actually unwanted, consent.

Before recognised consent management services can enter the market, a legal ordinance must regulate the requirements for such services and the procedure for their recognition. A first draft was presented this summer. However, even before it came to a departmental vote, several departments, including myself, insistently called for a comprehensive revision due to considerable concerns. Considering that several data protection principles have been called into question, I also opposed the publication of the inadequate draft.

I criticised a deviation from mandatory requirements of the GDPR as contrary to EU law. Moreover, the inclusion of recognised consent management services in the TTDSG is unsuitable for the containment of cookie banners, because such a legal ordinance can, by its very nature, only regulate consent pursuant to Section 25 TTDSG. For example, consent pursuant to Art. 6(1)(a) of the GDPR, which may be required for further processing of data collected through cookies for marketing purposes, cannot be regulated.

My recommendation for federal authorities, but not only for them, is therefore still to use cookies and similar technologies only if this is technically indispensable to provide the telemedia service explicitly requested by users. In this case, neither consent nor a "cookie banner" is required according to Section 25(2)(2) TTDSG. Unfortunately, I repeatedly find that cookies are to be found on the websites of federal authorities – and even more frequently on subsites for special situations and campaigns – among other things because these websites and subsites have been put together from modular systems.

Further information on the legal requirements for the use of cookies and similar technologies can be found in the DSK's "Guidelines on Telemedia".[56]

**I recommend fundamentally revising the introduction of data fiduciaries on the basis of the TTDSG and implementing it in conformity with the GDPR**

## 5.6 New EES and ETIAS Implementation Act

**In order to implement the EES and ETIAS regulations, the federal government has presented a bill, which will amend numerous existing laws and create new laws. It intends to allow intelligence services to access the future large-scale EU systems.**

At EU level, two new large-scale IT systems are scheduled to come on stream in 2023. This is the European Entry and Exit System (EES) on the one hand and the European Travel Information and Authorisation System (ETIAS) on the other. This requires numerous implementing rules at national level, such as clarifying responsibilities and powers. However, it is also necessary to regulate the transfer of personal data between the competent authorities and to ensure that data records are deleted from EES and ETIAS in a timely manner.

In December 2022, the federal government adopted the "Draft Law on the Implementation of Regulation (EU) 2017/2226 and Regulation (EU) 2018/1240 and on the Amendment of the Residence Act, the Freedom of Movement Act/EU, the Central Register of Foreigners Act and the Regulation on the Implementation of the Central Register of Foreigners Act" in the Cabinet. This so-called EES and ETIAS Implementation Act (EEDG) also contains two new laws: the EES Implementation Act (EESDG) and the ETIAS Implementation Act (ETIASDG).

In the departmental coordination, I was able to achieve some improvements with regard to data protection law. A positive aspect of this procedure is the constant, constructive participation of the lead Federal Ministry of the Interior. Some of my concerns, however, could not or not completely be dispelled. For example, the draft provides that the intelligence services should also have access to EES and ETIAS. From my point of view, it is in any case questionable to what extent these authorities may and should actually perform tasks of the security and law enforcement authorities under German law in the sense of the two EU regulations. As I understand it, the European legal acts only permit access by security authorities for the fulfilment of these tasks. I will therefore continue to play an active role in the ongoing legislative process.

56 Guidance of 7 December 2022, available at: https://www.bfdi.bund.de/orientierungshilfen

# 6 Freedom of information

## 6.1 Conference of Freedom of Information Commissioners

**In the report year, the Schleswig-Holstein State Commissioner for Data Protection chaired the Conference of Freedom of Information Commissioners (IFK). Under its aegis, the IFK focused on technical aspects of the further development of state transparency.**

**The IFK's main tasks include the promotion and further development of access to information at public bodies. The IFK adopted two resolutions at its 42nd meeting on 30 June 2022 in Kiel.** [57]

**All resolutions of the IFK can be found here:**

(Scan QR-Code or click)

In the resolution "SMS in the file", the Freedom of Information Commissioners pointed out that public authorities now increasingly use forms of communication such as short message services, messenger services, social media and SMS. This communication from the authorities can also be official information. According to the IFK, public bodies must always fulfil their documentation and information obligations when using communication media. The IFK calls on the administrations of the Federation and the states to also document this type of communication in order to guarantee access to information.

The resolution "No circumvention of freedom of information by establishing foundations under civil law!" dealt with access to information about the "Stiftung Klima- und Umweltschutz MV" foundation. This foundation was established by the state government of Mecklenburg-Western Pomerania for the implementation and promotion of environmental and climate protection measures. Another goal was the completion of the Nord Stream 2 natural gas pipeline. In addition to the partial public funding, the state government also had an influence on the staffing of the foundation's bodies. The state government and the foundation denied the public full access to requested information. For this reason, the IFK affirmed that transparency must also be guaranteed in the case of the performance of public tasks by foundations under civil law according to general access to information law.

In the resolution "Lower Saxony: The time for a transparency law has come!", the IFK called on those involved in the coalition negotiations in Lower Saxony to include the enactment of a transparency law in the coalition agreement. This is what happened. Besides Bavaria, Lower Saxony is the last federal state in which there is still no unconditional right of access to official information held by public bodies. In this regard, the IFK stated that public bodies in Lower Saxony must be subject to comparable transparency obligations as the public bodies of other states and the Federation.

In addition, the Freedom of Information Working Group and the IFK dealt intensively with the topics of "freedom of information by design" and the technical and legal design of state transparency and freedom of information portals in all meetings during the reporting year.

## 6.2 Exchange of experience between the supreme federal authorities

**On 6 September 2022, for the first time since the beginning of the pandemic, I invited the supreme federal authorities to a face-to-face exchange of experiences on freedom of information practices.**

We informed each other about current case law, discussed practice-relevant issues and provided a platform for

57 All resolutions of the IFK are available at: www.bfdi.bund.de/ifk-entschließungen

exchange between colleagues. At the same time, the staff of the Freedom of Information Unit, which had been newly founded within my authority, used this opportunity to introduce themselves to their colleagues from the supreme federal authorities.

The participants agreed to intensify the exchange in the future. For this purpose, a quarterly exchange of experience is offered in a one-year pilot project. This is to take place once a year in Berlin and three times a year in a shorter format as a video conference. The first exchange of experiences in the shortened format took place in December 2022. I was very pleased with the interest in this opportunity and the substantive discussions.

## 6.3 Transparency Act

**For many years, I have called in my Activity Reports for the Freedom of Information Act (IFG) to be developed into a transparency law. The SPD, Bündnis 90/Die Grünen and FDP anchored this goal in their coalition agreement in 2021.**

At the same time, the IFG and the Environmental Information Act (UIG), and perhaps also the Consumer Information Act, were to be merged into one law with proactive publication obligations. As a first sensible and overdue step, the right to unconditional access to public information is to be given constitutional status.

In my opinion, a federal transparency law can only be conceived and implemented together with the digitalisation of the administration. Even before information is requested, authorities then plan their internal processes and structures in such a way that the provision of information is possible within the shortest possible time. If they are sensibly indexed and machine-readable, digitised information stocks can be searched without this requiring a great deal of time and effort. However, I know from my advisory and monitoring practice that quite a few authorities still keep the traditional paper file.

Official information and its processes must be tamper-proof and complete. Metadata, information on data quality and the tamper-proofing of data and information help with this. An official freedom of information officer could provide advice and support as a central point of contact. Accordingly, in my opinion, the Transparency Act should establish official freedom of information officers. Ultimately, "freedom of information by design" means a public authority culture of openness and a clear legislative commitment to it.

The core of every transparency law is a transparency portal on which official information can be obtained without registration, barrier-free and with open licences. The Federal Transparency Act needs a catalogue of information subject to publication that defines a minimum standard and leaves room for the publication of further suitable information. Other key requirements include the searchability of the data stock in the transparency portal, documented interfaces and the reusability of the information.

In accordance with the principle of "access for one – access for all", information that has been made accessible upon individual request should in principle also be published in the information register. Furthermore, I consider a general balancing of interests between information and secrecy, which already exists in the UIG, to be necessary as an additional corrective.

For me, it is indispensable that it is in harmony with data protection and its regulations and enforcement possibilities. Therefore, the Freedom of Information Commissioner needs ordering and enforcement powers in a Federal Transparency Act. In case of conflict, the Freedom of Information Officer must be able to act. Leaving it up to the information seeker to always take the time-consuming and costly legal route thwarts the idea behind all freedom of information laws. In my view, there is now an opportunity for a modern, ground-breaking law with which Germany could also set standards in Europe.

**I recommend merging the Freedom of Information Act and the Environmental Information Act (and, if possible, also the Consumer Information Act) and further developing them into a Federal Transparency Act with proactive publication obligations. In a federal transparency law, the Freedom of Information Commissioner needs ordering and enforcement powers in order to be able to act in case of conflict.**

## 6.4 Consultation and inspection visit to the BSI (Federal Office for Information Security)

**Requests to the Federal Office for Information Security invoking the Freedom of Information Act (IFG) often concern complex technical issues.**

In November 2022, I conducted an advisory and monitoring visit to the BSI. Due to the large number of IFG applications, an extensive review of the procedures from 2018 to 2022 was carried out. The IFG requests submit-

ted to the BSI often concern complex technical aspects. As a rule, IFG requests require the implementation of a third-party participation procedure, as third-party rights may be affected. I have provided information and suggestions on the details of the procedure. The material and formal requirements of the Freedom of Information Act were observed. The special features of the BSI as a security authority were adequately taken into account when assessing the existence of grounds for exclusion. IFG applications are processed centrally. The evaluation of the audited transactions showed effective and targeted cooperation with the specialised units. Overall, the processing of IFG applications was citizen- and service-oriented. An open attitude towards freedom of information was evident.

## 6.5 IFG mediation procedure

Anyone can contact me if they feel their right to freedom of information has been violated. In the course of my mediation activities, I therefore also received a large number of submissions in the year under review. The mediation procedures related to a wide range of issues. Among other things, I had to deal with the question of the requirements for the specificity of an IFG application. In another procedure, I had to clarify whether a request had to be processed under the Freedom of Information Act (IFG) or the Environmental Information Act (UIG). However, my authority also regularly receives IFG requests. I had to reject one application because the exemption for the secret services also applies to my authority. The mediation procedures listed below are examples of the work of my authority and are intended to shed light on specific aspects.

### 6.5.1 Lobbying register campaign

**I received many appeals in connection with a campaign conducted by the association "Open Knowledge Foundation Deutschland e.V." together with "abgeordnetenwatch.de" on the online platform "Frag den Staat" (Ask the State).**

As part of the campaign, IFG requests regarding meetings of lobby associations with representatives of the federal government could be submitted via the online platform. This platform had provided pre-formulated applications in which the addressees and the subject of the application were already specified. Non-pre-formulated applications were also available.

The majority of the IFG applications submitted during the campaign were rejected. In the course of my mediation work, I noticed recurring justifications on the part of the authorities that were the subject of the requests. Among other things, the objection of inadmissible assertions of rights, the protection of the core area of executive self-responsibility and the requirements for the specificity of the application were frequently invoked. For this reason, I sent a circular to several supreme federal authorities in February 2022 and provided advice on how to deal with IFG applications in the campaign. [58]

### 6.5.2 The specificity of IFG requests

**The requirements for the specificity of a request under the Freedom of Information Act (IFG) are not too high. In case of doubt, the authority is required to support the applicant.**

A petitioner turned to me with the request for mediation regarding an IFG application filed with the Federal Ministry of Finance (BMF). The petitioner had made a wide-ranging request for access to documents and information on the funds from the European Reconstruction and Resilience Facility. The Federal Ministry of Finance advised the petitioner that, according to the interpretation of the request, they considered not one, but four individual requests to be too vague. The petitioner narrowed the request and reduced the subject of the application to information on the preparation of the deliberation of the German Reconstruction and Resilience Plan (DARP) in the Coalition Committee as well as on the concretisation and decision-making process. If the BMF was not prepared to split the petitioner's application into two applications, the petitioner was willing to bear the costs of processing the application. The Federal Ministry of Finance ultimately rejected the application for lack of specificity and treated the request as two separate applications. In the opinion of the BMF, the application had been made under an impermissible condition under fee law. The petitioner's application, which was narrowed once again, was rejected with reference to the validity of the previously issued decision.

I could not understand the BMF's rejection on the grounds of lack of specificity. It did not make sense that the application could be too vague at the same time, while the BMF's assessment of the content defined several applications. In this case, it would have been desirable for the BMF to have provided the petitioner with detailed information on how to achieve substantiation. Due to a lack of knowledge of the relevant documents, it is

58 The circular is available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2022/Rundschreiben-Lobbyregister-selbst-gemacht.pdf

often not possible for applicants to specifically name documents. Therefore, the requirements for specificity should not be too high.

The rejection of the application with regard to an inadmissible condition under the law on fees is, in my view, worthy of discussion. In this case, an interpretation of the application favourable to the petitioner would have led to the result that the petitioner intended to defend himself as a precaution against an unlawful (because deterrent) splitting of their application. The prohibition of deterrent effects is not only to be observed when assessing the amount of the fee, but already when determining the individual official act subject to the fee. The BMF did not follow my recommendations in this mediation matter and refused access to information.

### 6.5.3 Right to information under environmental information law

**Under the Environmental Information Act (UIG), citizens have access to the list of flights conducted by the Federal President in the exercise of his duties.**

A petitioner asked me to mediate in his application to the Office of the Federal President. On the basis of environmental information law, he had asked for a list of flights made by the Federal President in the exercise of his office.

The Office of the Federal President first interpreted the application according to the Freedom of Information Act (IFG) and then rejected it. However, the IFA does not apply to information related to the duties of the Federal President as head of state (presidential acts). These are specifically constitutional tasks. After I pointed out to the Office of the Federal President that the flights of the Federal President were likely to be environmental information and that the application would have to be evaluated according to the UIG, the original decision was rescinded. Under the UIG, there are fewer exemptions for certain federal authorities or federal bodies. Presidential records are not per se excluded from access to information in the UIG. No other reasons for exclusion were given by the Office of the Federal President. The petitioner was provided with the full information requested under the UIG.

### 6.5.4 Railway accidents on Swiss territory – successful mediation for a petitioner

**A request under the Freedom of Information Act (IFG) to the Commissioner for German Railway Lines on Swiss Territory was answered quickly after my mediation.**

I was able to successfully mediate in the context of an IFG application to the Commissioner for German Railway Lines on Swiss Territory. The petitioner had requested information on the number of railway accidents that had occurred on German railway lines on Swiss territory in the years 2017 to 2022. As an institution of the federal government, the Commissioner for German Railway Lines on Swiss Territory is subject to the IFG (Section 1(1)(2) IFG). He is assigned to the Southern Office of the Federal Railway Administration. The petitioner had submitted the application via an online platform. Here, emails are prepared with automatically generated sender addresses, some of which consist of random numbers and letters. In this case, the agency responsible for providing information was not familiar with them. The petitioner's email was therefore classified as "suspicious" and not processed further. Accordingly, enquiries about the processing status also did not reach the recipient. Due to my mediation with the Commissioner for German Railway Lines on Swiss Territory, concerns about the email address and the content were quickly dispelled. The requested information was subsequently provided to the petitioner.

### 6.5.5 The exemption for intelligence services also applies to the BfDI

**As far as my function as a data protection supervisory authority responsible for the intelligence services of the Federation is concerned, I must also refuse access to information.**

Pursuant to the Freedom of Information Act (IFG), a request was made to my authority for the transmission of all audit reports of the systems NADIS – "Intelligence Information System" or, since 2011, NADIS-WN "Intelligence Information System and Knowledge Network", as well as all communication and documents related to it, that had accrued in the years 2008 to 2021. The application was rejected.

In doing so, I referred to the fact that according to Section 3(8) IFG, there is no right to access information vis-à-vis the intelligence services as well as the authorities and other public agencies of the Federation, insofar as they perform tasks within the meaning of Section 10(3) of the Security Clearance Act. According to several rulings of the Federal Administrative Court, authorities that have a particularly close relationship with the intel-

ligence services due to their tasks are also covered by the exemption. [59]

These requirements are met with regard to my role as the supervisory and oversight authority for the federal intelligence services under data protection law. The task as a supervisory and oversight authority over the Federal Office for the Protection of the Constitution (BfV) is connected with the examination of the NADIS or NADIS-WN databases. For this reason, there are typically a large number of documents in my office which may contain not only findings and assessments of the BfV, but also internal information about the structure and working methods of the BfV.

The Freedom of Information Commissioners demand the abolition of the exemption for the protection of the constitution in general.[60] As long as the legislator does not change anything, the regulation must continue to be observed. But even after an abolition of the exemption, numerous documents and processes would have to be classified as non-publishable.

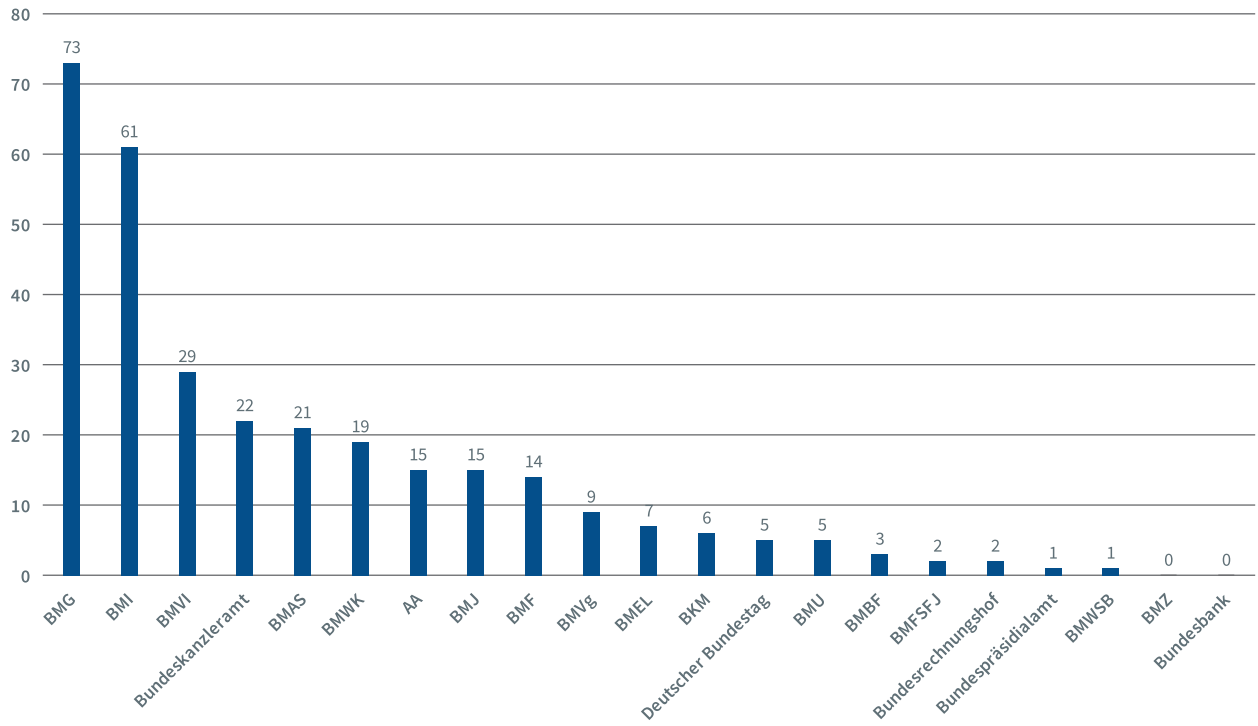
## 6.6 Statistical evaluations for the IFG (Freedom of Information Act) for 2022

**Submissions relating to the Freedom of Information Act (IFG) and the Environmental Information Act (UIG)**

I received a total of 491 submissions during the reporting period. This means that the number of submissions has decreased compared to previous years.

In 310 cases, petitioners appealed to me pursuant to Section 12(1) IFG to complain of violations of their right to access information under the IFG. Since the amendment of the UIG in March 2021, my previous role as ombudsman for the IFG has been extended to the UIG. This allows anyone to appeal to the Federal Commissioner for Data Protection and Freedom of Information if they consider their right to access information under the Federal Environmental Information Act to have been violated.

**Statistics on appeals pursuant to Section 12 (1) IFG**




59 BVerwG (Federal Administrative Court), judgement of 25 February 2016, 7 C 18/14; confirmed by: Judgment of 22 March 2018, 7 C 21/16

60 See the IFK resolution of 2 June 2021, available at: www.bfdi.bund.de/ifk-entsch ließungen

During the reporting period, I received eight requests for mediation in applications under the UIG. Compared to the previous year, the number of mediation requests remains at a low level. In addition to appeals concerning violations of the right of access to information, general enquiries were also made in the reporting period concerning legal information on the Freedom of Information Act, citizens' enquiries or referrals outside my competence.

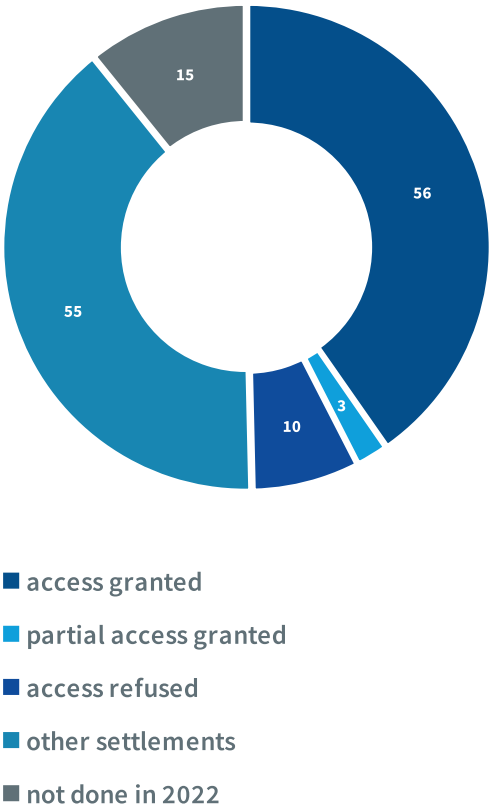
In relation to the departments and their business areas, the submissions are distributed as shown in the following chart. The highest number of submissions concerned the Federal Ministry of Health and its portfolio, which – as in previous years – is due to the applicants' strong interest in information related to the coronavirus pandemic. Among other things, the requests were related to side effects of vaccinations, quality testing of vaccines and vaccine effectiveness.

In two mediation cases in the reporting period, I had to threaten an objection because access to information was unlawfully denied or because the duty to cooperate according to Section 12 IFG in conjunction with Section 24(4) BDSG (old version) was violated. As in the previous year, these concerned the Federal Ministry of Digital Affairs and Transport because of documents in connection with the "road toll affair" and also the Federal Archives in connection with the virtual reconstruction of Stasi documents.

### IFG requests to my authority

During the reporting period, I received a total of 139 requests for access to information. These requests were directed both at access to file contents in the context of their own requests for mediation addressed to the BfDI after their conclusion, and at statements by the BfDI on draft legislation. Compared to previous years, the number of applications has declined and is therefore more or less the same as in 2016 and 2017. The proactive publication of circulars to the supervised entities or to the supreme federal authorities on my website, as well as the publication of selected inspection reports, including inspections on the topic of security clearance law and in connection with inspections of postal service providers, has, in my view, contributed to the overall decline in the volume of applications.

IFG applications to the BfDI in 2022




The chart shows the distribution of (partial) access granted, access refused and other settlements in 2022. Cases of other settlements include, for example, cases in which the application is not further pursued because it is likely that fees will be charged, and cases in which the applicant does not cooperate sufficiently. Reasons for refusals were mainly ongoing consultations or the fact that the requested information was not available to the BfDI.

# 7 Security

In 2022, my authority again dealt with a wide range of issues in the field of security. However, the list of topics is far from exhaustive. I cannot report publicly on large parts of my work in the context of the security authorities.

The reason for this is primarily the requirements of confidentiality law. These protect information and processes whose disclosure could endanger or harm the security or interests of the Federation or the states. Naturally, I come into contact with such processes and information again and again in the course of my monitoring and advisory activities in the security sector. My staff must therefore undergo a comprehensive security clearance in advance and then be specially authorised by my authority's Security Officer to handle such classified information.

In addition to mandatory legal requirements, however, reasons of trusting cooperation may also prevent public reporting. For many security authority projects, I depend on the active and early involvement of these bodies. In this way, I can, for example, counteract data protection abuses well in advance when introducing new IT systems or files in the security sector. However, especially when these authorities act secretly within the framework of their legal mandate, this information is not intended for the public. I therefore discuss with the respective security authorities responsible whether aspects of secrecy speak against publication from their point of view. This approach has proven successful in terms of trusting cooperation and has already led to data protection successes in many areas (see Chapter 12).

## 7.1 Passenger Name Records (PNR) – Landmark ruling of the ECJ confirms need for action

**Now it is certain: the processing of PNR data must be fundamentally changed. The landmark decision of the European Court of Justice (ECJ) concerned a referral from the Belgian Constitutional Court. However, its interpretation of the so-called PNR Directive is also binding for Germany. In my biennial report to the federal government, I also come to a critical conclusion – as I have done several times before.**

On the basis of Directive (EU) 2016/681 of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive), Member States have adopted rules obliging air carriers to transfer passenger information to so-called Passenger Name Record (PNR) units. In Germany, this is set up within the Federal Criminal Police Office. It stores this data and also compares it with police databases and previously created patterns (e.g., type of booking, chosen flight route, etc.). In Germany, these requirements are regulated by the Passenger Name Record Act (FlugDaG).

In my previous activity reports, I have regularly pointed out the disproportionate processing of passenger data by security authorities (see 22nd AR No. 13.5.4, 26. AR No. 2.3.2, 27. AR No. 1.3, 28. AR No. 6.4, 29. AR No. 6.6, 30. AR No. 6.24). Several cases concerning the legality of the PNR Directive were also before the ECJ.

The Grand Chamber of the ECJ has now made a landmark decision following a referral from the Belgian Constitutional Court. According to this, the PNR Directive continues to apply, but the ECJ draws clear boundaries for the interpretation of the Directive. These limits are not only to be observed in Belgium, but also apply to the way in which the PNR Directive is to be implemented in Germany and in all other Member States.

The ECJ had to rule on numerous aspects, many of which are also directly relevant to the German FlugDaG. For example, the ECJ clearly rejects the blanket inclusion of intra-EU flights, i.e., flights without a third-country connection, in the PNR system. This is only permissible if there are sufficiently concrete circumstances to assume that a Member State is confronted with a terrorist threat that could be classified as real and current or fo-

reseeable. Moreover, this should only apply for a limited time. Similarly, it would exceed the limit of what was absolutely necessary if data records of persons were stored for longer than six months even though there were no objective indications of a risk in the area of terrorist offences or serious crime with an at least indirect connection to the flight. I, too, had long criticised the inclusion of intra-EU flights in the FlugDaG and the five-year storage period, which is tantamount to data retention.

In addition, the ECJ emphasises the strict purpose limitation of PNR data, specifying that processing for purposes other than the prevention, detection, investigation and prosecution of terrorist offences and serious crime is inadmissible. In particular, Member States would have to ensure that ordinary crime or petty offences are not included. The ECJ also took a clear position with regard to the model function provided for in the PNR system, i.e., the use of pre-determined criteria: "Pre-determined" is opposed to the use of so-called machine learning systems, which – without human influence and control – can change the evaluation process and, in particular, the evaluation criteria relevant to the result as well as the weighting of the criteria. It must remain recognisable why a hit was scored.

This model functionality is also the subject of the report that I submit to the federal government every two years pursuant to Section 4(3)(9) FlugDaG. I sent this report for the first time in February 2022. In it, I communicated my justified doubts about the proportionality of the encroachments on fundamental rights. In the German PNR system alone, an extensive data set on many millions of passengers is stored and processed. Nevertheless, in the above-mentioned biennial reporting period, the countless pattern matching exercises were unable to promote the legal objective (cf. 30th AR No. 6.24). I also explicitly pointed out the general monitoring of intra-EU flights, which is not required under EU law, and the numerous encroachments on fundamental rights that this entails.

All these are clear indications that the German PNR system urgently and fundamentally needs to be revised. Adjustments will also be necessary in other Member States by now at the latest. I continue to advocate for this both nationally and in the European Data Protection Board.

## 7.2 Police 20/20 – P 20 (Internal police IT system modernisation and harmonisation)

**The first software applications of the joint "data house" of the federal and state police authorities have been programmed. However, cross-procedural research and analysis within P 20 also plays a role in my reporting period.**

I regularly report on the overall P 20 programme as a large-scale IT project of the federal and state police authorities, most recently in my 30th Activity Report.

**Development of the overall project**

As in the previous year, one of the focal points of development in the past year was to standardise the case processing, case management and the network systems (see 30th AR No. 6.14). But there is also progress on the joint "data house" project of the federal and state police authorities. First of all, the focus here is on the selection of a suitable technology. In this context, the first product tests have already taken place. Three test installations are to be filled with fictitious data sets by the end of 2022. The use of real data is planned for the end of 2024. A legacy data qualification service is also being developed with the data house. This serves, among other things, to implement the principle of hypothetical data recollection or to support it automatically.

**Hypothetical data re-collection as a special case of purpose limitation**

The principle of hypothetical data re-collection developed by the Federal Constitutional Court crystalises the principle of proportionality. It formulates constitutional requirements that the legislature must observe when enabling the security authorities to use data that has already been collected for a different purpose. This legal concept should not be misunderstood as making a clear definition of the purposes of processing unnecessary. Nor is the blanket invocation of the principle of hypothetical data re-collection as a justification for the creation of a network information system with far-reaching query and research possibilities appropriate.

*Extract from my position paper on the principle of purpose limitation in police information systems of 6 April 2021. Available at: www.bfdi.bund.de/stellungnahmen*

I have a first technical concept paper on the joint "data house". However, the project group at the Federal Ministry of the Interior and Home Affairs (BMI) has also promised me a specialised concept in terms of data protection law, though this was not yet available to me at the time of going to press. Without such a document,

a data protection assessment of the joint "data house" is not possible.

**Cross-procedural research and analysis**

Since 2022, the Bavarian State Criminal Police Office has had a "cross-procedural search and analysis system" (VeRA). After a Europe-wide tendering process, the company Palantir Technologies GmbH was awarded the contract. The framework agreement also allows other federal and state police authorities to use the VeRA system. The BMI is currently examining whether the federal authorities will also make use of the software product operated in Bavaria. However, a decision has not yet been made. The BMI has agreed to my involvement. In the past, I have repeatedly pointed out the data protection risks and requirements with regard to the evaluation and analysis of personal data. These are significant encroachments on fundamental rights. In addition, such analysis systems must not undermine the purpose limitation of stored data. Against this background, my office initiated a consultation procedure on the topic of "AI in law enforcement and security" (see 30th AR No. 4.2.2) and published the above-mentioned position paper on purpose limitation in police databases.

**Data consolidation Proof of Concept (PoC)**

I had already reported on this sub-project in the past. With the PoC, another network system is to be operated outside the police information network according to the Federal Criminal Police Office Act (BKAG) (30th AR No. 6.14, 29. AR No. 6.1). At the beginning of 2021, I had issued a formal warning to the Federal Criminal Police Office (BKA) pursuant to Section 16(2)(4) of the Federal Data Protection Act (BDSG) against the data processing intended with the PoC. Some state data protection supervisory authorities have also warned their state police authorities against this data processing. At the beginning of 2022, I once again spoke out in detail against the PoC in a letter coordinated with the AG INPOL (a working group of the DSK's Security Working Group). The BMI responded to this statement at the end of the year and continues to consider the data processing intended by the PoC to be lawful. It now remains to be seen whether or how the sub-project will develop further. I will report on progress made.

**European Police Records Index System (EPRIS)**

The BMI lists EPRIS-ADEP as a sub-project of P 20. The aim of the project is to create an EU-wide directory system for police crime files. For this purpose, the prototype of a decentralised software solution (ADEP technology) had been developed by selected EU Member States. The technical specifications should make it possible to compare certain personal data with decentrally stored data files in a standardised form according to uniform regulations. The legal basis under European law for such an EU-wide directory system has not yet been created. Since the BKA has taken over the project management throughout Europe, I have asked them for a statement on data protection law. I am particularly interested in the legal basis on which the EPRIS-ADEP pilot project is currently operated and how it is ensured that legal requirements of the BKAG are observed. I had not yet received a response from the BKA at the time of going to press. In general, it is important to me that this project does not undermine fundamental rights. This includes, in particular, recognising that police data retention is an interference with fundamental rights that can have a significant impact on the data subjects. This is also true because criminal records often only hold persons on a suspicion basis. The interference is deepened here because these persons and suspicions can then be retrieved throughout Europe. The thresholds provided for this data retention in the BKAG must not be undercut at the very least.

**Register of processing activities**

My advisory and monitoring duty is not only subject to the P 20, but also to the "old" police information order in the BKA. I have been asking the BKA for the list of processing activities since 2019. Since such a document was not submitted, I issued an objection to the BMI as the supervisory authority pursuant to Section 16(2) BDSG.

The BMI informed me that the QSEC management system would be introduced after a Europe-wide tender. This also enables the mapping of data protection impact assessments. Since the BKA-wide introduction of the system is not scheduled until the third quarter of 2023, I have asked the BMI for an interim solution. The BKA is currently working on such a bridging solution. However, the preliminary list of processing activities had not been submitted to me by the time of going to press.

## 7.3 Involvement of third parties in source tapping and online searches

**Police authorities and intelligence services use IT products from third-party manufacturers. However, in the case of intrusive measures such as source tapping and online searches, they may only use third-party products within narrow legal limits.**

Secret surveillance measures always provide material for controversial discussions. On the one hand, the security

authorities must be able to effectively perform the tasks assigned to them. On the other hand, they have to respect the legal boundaries and data subject rights.

Carrying out intensive surveillance measures is part of the genuine sphere of state responsibility. The greatest caution is called for if the investigating authorities involve third parties. This applies in particular if the security authorities and intelligence services perform tasks with the help of third-party IT products.

I published a position paper on this subject in the reporting period. [61]The paper shows where, in my view, the legal boundaries run in conceivable cases of the use of third parties. Of course, the circumstances of each individual case remain decisive.

I formulated the following requirements for the use of third parties in intensive measures on the basis of the legal guidelines outlined in the paper:

- Decision-making powers regarding "whether" and "how" to carry out individual surveillance measures may not be transferred to private third parties.
- The processing of personal data on behalf of the controller in the context of the implementation of intrusive measures should be kept to a minimum. The possibility of uncontrolled storage or other misuse of personal data must be excluded.
- In-house developments are preferable to software solutions developed by private third parties (cf. 28th AR 2019, P. 57).
- The data processed with the help of third-party IT products must not be outside the influence and control of the controller. The controllability of the hardware and software by the controller must be fully guaranteed.
- The involvement of (private) third parties must not restrict the supervisory powers of the data protection supervisory authorities.

## 7.4 The Federal Police and number plate recognition

**In 2022, the Federal Police used systems for the automatic registration of vehicle number plates and their comparison with wanted person databases for the first time. According to the case law of the Federal Constitutional Court (BVerfG), they may only be used within limits because of their surveillance-state character.**

**Although I had been actively requesting status updates since 2020, I was only included in the process at short notice before the first deployment.**

Ad hoc automatic registration of number plates is a relatively new instrument that can only be used to prevent imminent danger to the life, limb or freedom of a person or to prevent and prosecute serious criminal offences. The number plates of all vehicles that pass a registration system are read and compared with a previously defined database.

In a departure from its previous case law, the BVerfG (Federal Constitutional Court) ruled in 2018 (decision of 18 December 2018, Ref. 1 BvR 142/15) that even the recording of number plates, and thus even more so the comparison with wanted persons files, constitutes an encroachment on the fundamental right to informational self-determination. Legal bases that allow such an interference are therefore not entirely ruled out under constitutional law, but they must meet strict requirements as to their proportionality.

After corresponding legal foundations were created in the Federal Police Act (BPolG) in 2017 and in the Code of Criminal Procedure (StPO) in 2021, such systems have now been used by the Federal Police since 2022. My monitoring role is of particular importance since data subjects are regularly not informed about the implementation of the measure. Although I had repeatedly asked about the state of affairs regarding number plate recognition systems at the Federal Police since 2020, I only found out about the planned deployment a week beforehand. At the same time, the Federal Ministry of the Interior and Home Affairs (BMI) had issued an opening order (so-called "emergency order") without consulting me beforehand, although, in my view, there was not necessarily any urgency for the fulfilment of the task, especially after the long lead time. The data protection impact assessment that I believed necessary was also not carried out.

As a result of the subsequent hearing on the opening order that has now taken place, I have started a review of the procedure and will work towards a data protection-compliant design.

61 Statement of 28 March 2022, available at: www.bfdi.bund.de/stellungnahmen

## 7.5 Increased activities in the area of criminal justice authorities

**Thanks to the increase in staff at my authority, I was able to significantly expand my criminal justice activities last year.**

My responsibility also includes data protection supervision of the Federal Public Prosecutor at the Federal Supreme Court (GBA) as well as the Federal Central Register (BZR) and the Central Public Prosecutor's Proceedings Register (ZStV), both of which are maintained at the Federal Office of Justice (BfJ).

At the GBA, I supervised the introduction of electronic criminal files in an advisory capacity and will continue to do so. In addition, during a fact-finding visit, I was informed in detail about how so-called structural investigation procedures are handled by the GBA and which legal considerations have to be taken into account. Structural investigation procedures are, for example, procedures in which as yet unknown members of known terrorist organisations are to be identified.

At the BfJ, I was active in an advisory capacity on various occasions. On the one hand, this concerned the national implementation of the ECRIS-TCN (European Criminal Record Information System for Third-Country Nationals). On the other hand, I was able to fulfil my advisory mandate in the redesign of the protocol in the ZStV as well as in the creation of European certificates of good conduct. In the latter case, the problem was that due to incorrect identification of persons in other EU countries, the certificates of good conduct received from these countries concerned other persons than the applicant. In addition, I carried out a check regarding the handling of witness protection cases in the BZR according to Section 44a of the Federal Central Register Act.

## 7.6 The Office for the Protection of the Constitution and the Federal Constitutional Court

**Once again, the Federal Constitutional Court (BVerfG) has called for fundamental and far-reaching changes in intelligence law. Many norms of the Bavarian law have to be changed due to unconstitutionality. The same applies to the Federal Protection of the Constitution Act (BVerfSchG). The adaptation of the disclosure regulations to the requirements of the ruling is likely to be particularly interesting. In a second decision in the course of the year, the BVerfG explicitly confirmed the unconstitutionality of individual norms of the federal law.**

On 26 April 2022, the BVerfG issued a ruling on the occasion of a constitutional complaint on the Bavarian Law on the Protection of the Constitution (BayVSG), the effects of which reach far beyond Bavaria. It declared many provisions of state law unconstitutional and gave the local legislature until 31 July 2023 to remedy the situation. Many other state constitutional protection laws and also the Federal Constitutional Protection Act (BVerfSchG) contain similar or even identical regulations to those of the BayVSG, so that action is also required there. The BVerfG's decision had already been foreseeable on the basis of previous case law. I had therefore already called for a comprehensive reform of the BVerfSchG on several occasions (cf. 29th AR No. 5.5).

**Differences and similarities between constitutional protection authorities and police authorities in requirements for encroachments on fundamental rights**

On the one hand, the court recognised the activities of the constitutional protection authorities for the preservation of democracy, because they act to protect particularly important legal interests such as the protection of the free democratic order. On the other hand, it also made clear the conditions under which the Office for the Protection of the Constitution is allowed to observe efforts. The thresholds above which the Office for the Protection of the Constitution may become active and thus also interfere with fundamental rights are, as a rule, permissibly lower than those of police authorities, for example. Constitutional protection authorities cannot draw any direct operational consequences for individuals from a surveillance measure, such as searches, seizures or arrests. However, these thresholds are higher if the intensity of the encroachment increases significantly. This is the case, for example, if particularly extensive information can be obtained through surveillance measures, which makes it possible to monitor individuals. In such cases, the same standards are to be applied as for comparable police measures, namely online searches and residential surveillance. For this purpose, an urgent danger to public safety must be present for the measures just mentioned to be ordered and, in addition, appropriate police assistance cannot otherwise be obtained in time. Especially with the latter requirement of subsidiarity, both measures – for residential surveillance this was already the case anyway – can only in theory be used by the constitutional protection authorities. After all, it is hardly imaginable that the police are not on the spot in time in such cases.

**Court defines requirements for the transmission of data by constitutional protection authorities, among other things**

The court makes many other important statements, e.g., the conditions under which third parties may exceptionally be involved directly or indirectly in a surveillance measure. Furthermore, the court establishes requirements for the specificity and clarity of intervention norms in the area of intelligence law. In the case of certain intrusive measures, it stipulates the requirement of a prior check by an independent body, as is provided for by the judge's prerogative in the area of criminal prosecution. Above all, however, it also comments on the conditions under which personal data may be transmitted by the Office for the Protection of the Constitution to various domestic or foreign agencies.

**First considerations by the federal government and the federal states on the implementation of the ruling**

Immediately following the court's decision, the federal government and the federal states met in a working group to discuss the implications of the ruling and to develop proposals for the necessary adjustments to the regulations. This report, including several annexes, was published by decision of the Conference of Interior Ministers on 27 September 2022. This shows that the contributors disagree on many points. On the one hand, how certain statements of the court are to be understood and, on the other hand, what changes in the laws might look like. This concerns, among other things, the question under which conditions constitutional protection authorities may in future transmit information to authorities with so-called operational coercive powers as well as to law enforcement authorities. According to the BVerfG, more stringent requirements apply to transfers to these bodies because the information cannot be used by the constitutional protection authority for such measures. In contrast to the aforementioned authorities, the Office for the Protection of the Constitution does not have such coercive powers.

**What is an "authority with coercive operational powers"?**

The court has newly introduced the concept of operational coercive powers without clearly defining it. However, it only mentions them in comparison with police authorities. From this, it is predominantly concluded that it must be a matter of powers against which the data subject cannot obtain legal protection in advance, such as in the case of seizure, arrest or search. It is then still questionable whether the increased transmission requirements generally apply to transmissions to such authorities or whether the specific transmission must be aimed at using the information for the application of operational coercion.

**Open questions regarding the transfer of data to law enforcement authorities**

According to the court's ruling, transmission to law enforcement agencies may only take place for the prosecution of particularly serious criminal offences. This concept is shaped under non-constitutional law by the catalogue of offences in Section 100b(2) of the Code of Criminal Procedure (StPO). According to this, law enforcement authorities may only use the intrusive measure of online searches for the criminal offences in question. The BVerfG itself also took its cue from this in an earlier ruling. The main task of constitutional protection authorities is to protect the free democratic order and the security and existence of the Federal Republic. If transfers were allowed solely for the offences listed in Section 100b(2) of the StPO, some offences that become known to the Office for the Protection of the Constitution in the course of its work would not be allowed to be transferred to law enforcement agencies. Examples in this context include bodily injury offences with an anti-Semitic background or certain state security offences such as secret service agent activities under Section 99 of the Criminal Code. The federal/state report therefore partly doubts that the court could have wanted this result and tries to find alternatives. There are some calls for the introduction of a separate notion of a particularly serious offence specific to constitutional protection. It would also be conceivable to significantly increase the range of punishment for such offences. Many questions are still open here. Special attention will also have to be paid to the second decision of the BVerfG from September 2022 mentioned below, in which the court also comments on this complex of issues.

**Regulations are also needed for comprehensive monitoring of intelligence activities**

With regard to the necessary amendments to the BVerfSchG, I approached the Federal Ministry of the Interior and Home Affairs (BMI) at an early stage. In this way, I was able to take note of the BMI's considerations even before the official start of the legislative process. I made it clear that, from my point of view, not only this judgement, but also older judgements have called on the legislator to act and that the BVerfSchG needs a fundamental reform. In addition, through my monitoring activity, I also see the need for clarification in some areas, for example, in the storage of data of unknown or uninvolved persons as well as in the right to information.

When adapting the law, it is also important to me that the cooperation between the body that will carry out the prior checking for intrusive measures and the BfDI is ensured. Only in this way will comprehensive monitoring and also comprehensive exchange be possible. For example, in 2021 I reviewed the area of observation, which the BVerfG considers to be such a measure in the ruling, among other things, and which will be subject to independent prior checking in the future, at both the Federal Office for the Protection of the Constitution (BfV) and the Federal Office for the Military Counter-Intelligence Service (MAD). These results could be helpful for the new supervisory body. Other diverse points of overlap are conceivable.

**Further decision of the BVerfG in September 2022**

In its decision of 28 September 2022 (1BvR 2354/13), the court explicitly transferred parts of its determinations from the April ruling to the BVerfSchG. A constitutional complaint against Sections 19-21 BVerfSchG had already been pending since 2013. The disclosure norms of Sections 20 and 21 BVerfSchG in connection with the Right-Wing Extremism Filing System Act were declared unconstitutional. Section 20 BVerfSchG standardises the BfV's duty to disclose data to law enforcement and security authorities for the prevention or prosecution of state security offences. Section 21 BVerfSchG regulates these duties of disclosure for the State Offices for the Protection of the Constitution. With regard to Section 19 of the BVerfSchG, the constitutional complaint was inadmissible, so that no substantive decision was issued in this respect. I have submitted several statements in this procedure because I, too, consider the norms in question to be too vague and disproportionate. The court took up my demand for documentation of the disclosure of intelligence gathered by intelligence means and urged the recording of disclosures. Moreover, it has followed my view that this must also be enshrined in the law. Due to the requirement to adapt the unconstitutional norms by 31 December 2023, the legislator is now also called upon to act with particular haste here. It is therefore to be feared that my long-standing demands for a comprehensive reform of the BVerfSchG cannot be taken into account given the time available.

## 7.7 Complaints at the BAMAD (Federal Office for the Military Counter-Intelligence Service) and the BfV due to the violation of the duty to provide support

**In the past, there were considerable delays in the involvement of my authority in the area of responsibility of both the Federal Ministry of Defence (BMVg) and in the data protection unit of the Federal Office for the Protection of the Constitution (BfV). This constitutes a breach of the duty to inform me in a timely manner and to support me comprehensively in my supervisory activities in all matters relating to data protection law. I have objected to this in each case.**

**BAMAD**

The Federal Office for the Military Counter-Intelligence Service (BAMAD) is required by law to issue a file order (DAO) for each automated file and to consult me before issuing it. If there is particular urgency with regard to the fulfilment of the task, the BAMAD has the option of issuing the file by means of an emergency order (Section 8 of the MAD Act in conjunction with Section 14(3) of the BVerfSchG). However, the hearing must then be held without delay. As I learned during the reporting period, the BAMAD had already issued a new file by means of an emergency order in September 2021. However, there was a failure to ensure that the order placed in the outbox actually reached my authority for immediate completion of the prescribed procedure. It was only after my request that I was consulted, over a year later.

I objected to this and clarified that there is an explicit legal duty for the BAMAD to support my authority in the fulfilment of its tasks. In the meantime, the BMVg has informed me in its statement that the file in question has no longer been used by the BAMAD since October 2021.

**BfV**

In spring 2021, I exchanged views with the BfV for the first time on possible changes in the cooperation between the BfV and the Financial Intelligence Unit (FIU) (30th AR. No. 8.2.7). Special attention was paid to the creation of technical interfaces through which simplified data transfer within the framework of the provisions of the Money Laundering Act was to be implemented. At the end of April 2021, the BfV presented its current planning status to me in writing. The project raised various data protection issues, especially regarding automated processing procedures. Therefore, at the beginning of June 2021, I sent a letter to the BfV with my concerns

and questions about the implementation of the planned interfaces. In the following months, the BfV announced several times that it would reply to the letter, without actually doing so. After several reminders, I finally objected to this in a letter dated 4 May 2022 for breach of duty to provide support. This duty includes, amongst other things, providing information on my questions (Section 28(3)(2)(1) BVerfSchG).

In its statement, the Federal Ministry of the Interior and Home Affairs, which is responsible for technical supervision, regretted the delay. The BfV had promised to establish processes to improve communication with me. I finally received the requested information on 31 May 2022. According to this, the BfV has largely put plans for the introduction of interfaces on ice. The previously questionable projects will not be pursued.

In recent years, the BfV has repeatedly encountered cases with excessively long processing times. I attribute this to the fact that the responsible data protection department has not grown in personnel to the same extent as the rest of the authority.

I therefore continue to advocate for better staffing of the data protection departments of the authorities so that tasks can be processed in a timely and appropriate manner. This will also improve communication with my office.

## 7.8 Personal data in information letters of the BfV

**If the exchange of the Federal Office for the Protection of the Constitution (BfV) with other authorities and the information of the federal government on trends contains personal data, this also constitutes a transfer for which a legal basis is required. In my view, this is lacking in individual cases, so the procedure must be changed.**

The general exchange of information on findings, history and trends in the various areas of responsibility of the BfV with other authorities, in particular with the constitutional protection authorities of the federal states, but also the provision of information to the government, represent an important part of the BfV's work. This exchange takes place not only on an ad hoc basis, but is also institutionalised on a regular basis. For many years, the BfV has sent weekly reports with developments on various current topics to a number of authorities.

While these reports initially served primarily to inform the state constitutional protection authorities and later also the federal government, the circle of addressees became larger and larger over the years. This development would not be problematic in itself if the reports did not occasionally contain personal data on individuals from the BfV's respective areas of responsibility, such as left-wing or right-wing extremism, extremism against foreigners or counter-intelligence. This is because the sending of this information is legally associated with a data transfer that requires a corresponding legal basis.

Various disclosure regulations from the Federal Constitution Protection Act come into consideration for this, which can be relevant in a large number of cases. However, in view of the large distribution list in individual cases, the question arises whether there is actually always a relevant authorisation.

It does not distinguish clearly enough whether all recipients need the respective personal data to carry out their duties. Authorities whose areas of responsibility only relate to one of the above-mentioned areas of responsibility of the Office for the Protection of the Constitution do not usually require personal data from other categories. For some recipients, I question the power to disclose in general.

I expect the BfV to submit a data protection-compliant proposal for a solution that has been agreed with the supervisory authority in early 2023. From my point of view, this could consist, for example, of a reduced circle of addressees or different partial reports for individual groups of recipients.

## 7.9 Finally: a legal basis for ZITiS (Central Office for Information Technology in the Security Sector)

**The Central Office for Information Technology in the Security Sector (ZITiS) was created in 2017 without any legal basis. The federal government now finally wants to tackle this project. I will support it closely in this.**

The ZITiS was established in 2017 by ministerial decree, i.e., without creating a legal basis. Since then, the ZITiS has experienced a significant increase in staff every year. The current coalition agreement states that a legal basis for the work of the ZITiS is to be created. I see this as overdue in view of the importance of technical support for the security authorities.

In summer 2022, the Budget Committee had obliged the federal government to define key points for the future law. The BMI, within whose area of responsibility the ZITiS belongs, involved me in the development of these

key points. The key points are relatively general and essentially based on the 2017 Establishment Decree. According to this, at least the creation of an authority for the ZITiS to process personal data is to be examined. This applies in particular to personal data which it has received from its users for the purpose of testing or training IT systems. Such a legal basis is necessary in my view because this data processing is a change of purpose. The data was not originally collected for this purpose, but for police or intelligence purposes. Every change of purpose constitutes a new encroachment on fundamental rights and therefore requires a legal basis. So far, the ZITiS and the federal government have always stated that the ZITiS does not process any personal data.

The key points do not yet define the so-called federal authorities with security tasks for which the ZITiS is to be active. Only the Federal Police Headquarters, the Federal Criminal Police Office and the Federal Office for the Protection of the Constitution are mentioned as direct users. In the legislative process, I will insist that the federal authorities with security tasks be named conclusively.

It is also important that in the event that a specific legal basis for the processing of personal data is created in the ZITiS Act, my authority is granted remedial powers against the ZITiS directly. In addition, in the case of a restriction of data subjects' rights, my monitoring and compensation functions must be enshrined in law.

Finally, I am critical of the announcement that all new ZITiS employees are to be subjected to a security check. The Security Clearance Act provides that only those persons who are to be entrusted with security-sensitive tasks are subject to security clearance. This means that the persons would have to have or be able to gain access to classified information or be employed in a security-sensitive position within a vital or defence-sensitive facility. Entrustment with a security-sensitive activity must be foreseeable. Security clearance in advance is inadmissible. I have not yet received a justification according to which the entire staff of the ZITiS (e.g., including persons working in administration) must be entrusted with security-sensitive tasks. I find the tendency to declare all new hires at certain authorities to be engaged in security-sensitive activities questionable.

## 7.10 Uncontrolled proliferation of clearance procedures

**More and more people have to undergo background checks in their professional life, and the trend is rising. The problems arising from this are tackled entirely according to the motto: What doesn't fit will be made to fit!**

The requirements and procedure for federal security clearances are regulated in the Security Clearance Act (Sicherheitsüberprüfungsgesetz, SÜG). The purpose of security clearance is to enable the state to determine which persons it can entrust with particularly sensitive official and state secrets or allow access to security-sensitive positions within a vital or defence agency.

Already in my 22nd Activity Report, I reported an increasing proliferation of security and background checks (22nd AR No. 4.8). There are various regulations on background checks besides the SÜG, e.g., in the Atomic Energy Act and the Aviation Security Act. However, other regulations also govern the necessity to conduct a security clearance by referring to the SÜG. The Satellite Data Security Act, the Soldiers Act, the Reservists Act or the Federal Criminal Police Office Act are worth mentioning here. The broad wording in Section 1(2)(4) SÜG provides the gateway for this. According to this, anyone who is subject to security clearance under other provisions is also engaged in a security-sensitive activity, insofar as reference is made to the SÜG. Current plans show that the legislator will continue to make increased use of the possibility to refer to the SÜG and identify more and more fields of activity in which the requirement for security clearance exists. The result is thousands of new clearance procedures and increasing confusion.

From my point of view, the problem is that the legislator does not have to overcome any major hurdles here. It is sufficient if the reference standard mandates security clearance according to the SÜG. However, this is a departure from the actual purpose of the SÜG, namely the protection of secrets and against sabotage. On the other hand, in view of current world events, it cannot be denied that the Federal Republic must arm itself against increasing threats due to infiltration by extremist groups or foreign intelligence services. Insofar as the definition of a "security-sensitive position or activity" within the meaning of the SÜG is no longer in line with the reality of life, an adjustment in the wording of the SÜG could be more expedient than the increased mandating of security checks for the entire (future) staff of individual authorities. The respective competent authorities would thus have the possibility to identify the security-relevant fields of activity in their authority and to check only the group of persons employed there.

The current procedure leads in many places to multiple checks of data subjects under Section 1(2)(4) SÜG on the one hand, and Section 1(4) SÜG on the other, due to overlaps with the existing sabotage protection regulations.

This is because the extended security check in sabotage protection (Ü2-Sab) does not currently replace the basic security check (Ü1) due to a different scope of testing. However, the aim should be to subject each person, if possible, only to a review according to the highest level required for them.

The problem of multiple checks is further exacerbated by the fact that checks are added for individual persons under state law. In the year under review, for example, I was approached by a commercial enterprise that handles contracts related to classified information nationwide. The employees of this company are forced to undergo security checks in several federal states (sometimes up to four). The reason for this is that some federal states do not recognise the security clearances of other federal states as equivalent. This is surprising from my point of view, as all state regulations contain a provision that allows for the waiving of security clearance if equivalent or higher security clearance was already successfully completed within the previous 5 years. This is precisely to prevent unnecessary multiple checks. However, this is different in practice. I presented the topic at the "Security Working Group" of the Data Protection Conference to share experiences and raise awareness. In future, it would be desirable to have a precise, case-by-case examination based on the information in the security declaration and the measures carried out to determine whether the existing security clearance of the employee can be recognised. An overall system coordinated between the federal and state governments would be even better.

In addition, the increasing number of security checks leads to consequential problems. The duration of the procedures has also increased noticeably in recent years. This is a particular problem in security agencies. Time plays an overriding role here. The deployment of security-checked personnel is sometimes required there overnight. In one of my inspections, I found out that this problem has been dealt with pragmatically, in that the findings of other agencies are also requested through an in-house review of the (freelance) employees. In my opinion, there is no constitutional, legal basis for this. The responsible body has asked me for advice on a legally compliant arrangement. The consultations are ongoing.

On the occasion of the upcoming European Football Championship 2024, the topic of identity checks without a nationwide uniform legal basis is once again gaining topicality.

The current and, in future, increasing "proliferation" of security checks in the various areas of responsibility should be counteracted. The legislator should merge the various regulations on background checks and create a uniform legal basis applicable to all types of checks. In particular, the relationship between personnel secret protection, preventive personnel sabotage protection and checks under other laws should be regulated coherently. In this way, multiple checks of data subjects could be avoided.

**I recommend that the legislator use the upcoming evaluation of the SÜG to develop a coherent overall concept for identity checks at the federal level. Instead of a sprawling application of the opening clause to entire authorities, different clearance formats outside the SÜG as well as multiple checks due to different activities, the scope of the law should be redefined.**

# 8 Other issues

## 8.1 News from the telematics infrastructure and its applications

**The telematics infrastructure (TI) and also its applications such as e-prescriptions or electronic patient records (ePA) are constantly developing. In this context, data protection-compliant implementation is becoming more and more important.**

**E-prescriptions**

As early as 2020, the Patient Data Protection Act stipulated in Sections 360 and 361 SGB V (Book V of the German Social Security Code) that medical prescriptions must be transmitted electronically via the TI from 1 January 2022. The so-called e-prescription is thus a mandatory application – and the first medical one ever. The e-prescription application was intended to be launched on 1 September 2022, initially in the test region of Westphalia-Lippe. It was stopped again by the Association of Statutory Health Insurance Physicians of Westphalia-Lippe.

Electronic SHI-accredited medical care prescriptions are always stored in a central repository in the TI. Patients can only choose whether they want to receive access information in electronic form or – along the lines of a train or airline ticket – as a paper printout with a barcode to be redeemed at a pharmacy. The advantages of digitalisation arise when patients can do without paper printouts because they can retrieve their prescriptions with the e-prescription app via the TI and then also assign them securely to pharmacies. To do this, they have to register with the TI using their electronic health card (eGK). The NFC-enabled eGKs required for this are already widespread, but most insured persons have not yet been sent the PIN that is also required by their health insurance companies. I appeal to those responsible to provide more insured persons with NFC-enabled eGK cards and a PIN.

In order to prevent insured persons from sending e-prescriptions to pharmacies by non-encrypted email, gematik GmbH (company that manages telematics applications with the health card) has specified the procedure "Send e-prescriptions without logging into the TI": Insured persons can add their e-prescription codes by photographing them in their e-prescription app. From there, they can then send them encrypted via the internet to the pharmacy of their choice using a special service provider. Although they are not sent via the TI and there are certain disadvantages, as there is no logging of the assignment in the specialist service, my review has not revealed any fundamental obstacles under data protection law.

In parallel, I examined a procedure proposed by gematik in which insured persons insert their eGK into the card reader (without entering a PIN) in pharmacies and the pharmacy can thus retrieve all e-prescriptions from the central e-prescription server. I welcome a low-barrier option to redeem e-prescriptions in pharmacies that complements the existing options. A media disruption due to a printout or the installation of an app on the smartphone would thus not be necessary. Prescriptions could also reach the pharmacy safely via the TI. However, the specific technical implementation proposed by gematik showed considerable shortcomings that would mean a high risk for all insured persons that unauthorised persons could access their prescription data, even if they do not use this channel themselves. That is why I informed gematik that I cannot agree to the solution as it stands. At the same time, I offered proposals on how the function "redeem by inserting eGK" might be implemented securely without sacrificing convenience for insured persons. I am currently in talks with gematik about this.

**Alternative authentication procedure**

Already in my Activity Report for the year 2020 (29th AR No. 4.2), I criticised the authentication procedure for ePAs (electronic patient records), which does not comply with the requirements of the GDPR. Specifically, my criticism referred to the procedure of the "alternative insured person identity (al.vi)", with which insured persons can log on to their ePA without using their eGK in accordance with Section 336(2) SGB V. Because health

data is particularly sensitive, access to the ePA always requires highly secure authentication procedures that must always be in line with the latest state of the art. For a data protection-compliant state, al.vi also requires the guarantee of the highest possible security level, which al.vi does not offer. Thus, I only tolerated al.vi for a period of two years to give gematik the opportunity to replace al.vi with a suitable secure authentication procedure by 31 December 2022.

As such an authentication procedure has not yet been specified, gematik has asked me to extend my toleration by one year until 31 December 2023. I have had various discussions with gematik in which gematik gave a binding assurance that al.vi will be switched off by 31 December 2023 in any case. Under this condition, and the conditions that the statutory health insurance funds will equip all insured persons who have applied for an ePA by 31 December 2022, binding until 30 June 2023 at the latest, and all insured persons who apply for an ePA after 31 December 2022 with an eGK with NFC interface and PIN at the same time, I have extended my temporary agreement to al.vi until 31 December 2023.

**Status of the court case on electronic patient records**

In my 30th Activity Report (No. 6.1), I reported that five health insurance funds had filed lawsuits against data protection supervisory measures imposed by me to enforce a design of the electronic patient record (ePA) that complies with European law. In the meantime, the health insurance funds under my supervision have implemented the legal requirements of Section 342(2)(2)(b) SGB V on time and provided their insured persons with a level-2 ePA approved by gematik GmbH by 1 January 2022. This allows at least frontend users and representatives authorised by frontend non-users to give consent to authorised persons to access both specific documents and records and groups of documents and records of the ePA without barriers ("fine-grained access management"). However, for front-end non-users who cannot or do not wish to use a representative, the fact remains that only a limited, so-called medium-grained access management is available to them via the use of the decentralised infrastructure of the service providers. Moreover, due to the lack of a terminal or other solution, this user group still has no possibility to view their own ePA.

The health insurance funds concerned continue to resist the instructions I have issued at the cost of insured persons' money. The legal proceedings, which are pending before four chambers of the Cologne Social Court, are accordingly continuing.

**Responsibility under data protection law for the connectors**

Service providers such as doctors' surgeries and hospitals have secure access routers to the TI. Technical protocols are stored on these so-called connectors. In certain cases, this resulted in data protection breaches due to incorrect storage of serial numbers of the eGK certificates in the connectors of a manufacturer. [62]This has shown that the legally defined allocation of responsibility under data protection law to the users of decentralised components of the TI such as the connectors is not satisfactory. According to Section 307(1) SGB V, those who use the connectors for legally described purposes are responsible for them under data protection law, insofar as they have a say in the means of data processing. This responsibility extends in particular to the proper commissioning, maintenance and use of the connectors.

The data breaches made it clear that the users of connectors, i.e., the service providers, were powerless in the face of misconduct. They were not and will not be able to effect or initiate changes to the connectors themselves. They depend on the connectors working properly and have to rely on others such as the connector manufacturers and on gematik approval.

I have taken the data protection incident as an opportunity to suggest to the Federal Ministry of Health that Section 307(1) SGV V be amended. This could be a joint responsibility of gematik with the users in accordance with the Data Protection Conference decision of 12 September 2019 (see 28th AR No. 4.2.1).

**Opt-out debate on the electronic patient record**

The electronic patient record, ePA, as regulated by the Patient Data Protection Act in Sections 341 et seq. SGB V, is an electronic file managed by the insured person and focuses in particular on patient sovereignty. Use is voluntary for insured persons. They decide from the outset which data is stored, who may access it and whether data is deleted again. This ePA reflects a full opt-in solution.

In the 2021-2025 coalition agreement between SPD, Bündnis 90/Die Grünen and FDP, the governing parties declared their intention to accelerate the introduction of the ePA. All insured persons were to be provided with an ePA in compliance with the GDPR; its use would be voluntary (opt-out). This statement in the coalition agreement triggered or intensified the debate on an opt-out solution for the ePA.

However, it is still unclear how the opt-out solution will look in detail, i.e., it is unclear whether each of the

62 See also my FAQ, available at www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2022/01_FAQ-TI-Konnektoren.htm

approximately 73 million people with statutory health insurance should be provided with an empty digital file folder containing purely administrative data, or whether the ePA should already be automatically filled with medical data. Furthermore, it also remains unclear whether all health care providers are to be allowed to access all health data in the ePA, or whether the health data in the ePA might even be made directly available to medical research. Many different design options are conceivable, against which the insured persons could only subsequently raise an objection, i.e., opt out.

In principle, I see no need for the intended paradigm shift to an opt-out EPA. An insured-person-managed ePA also has the potential to bring benefits to healthcare if acceptance of and trust in ePAs among insured persons were more strongly promoted through increased information and advertising about the benefits of an ePA. The low usage to date is due to the not yet apparent added value for the insured, not to the implementation of an opt-in solution.

Even if, from my point of view, an ePA opt-out solution is not necessary, I welcome the fact that the coalition partners are striving for a GDPR-compliant solution and will consult on this. Initial talks have already taken place.

## 8.2 Digital health apps

**The process of being able to prove data protection compliance for reimbursable digital health applications by means of a certificate is making significant progress and is well on the way to replacing the previous, inadequate procedure of self-declaration by the manufacturers.**

With regard to the list of reimbursable digital health applications (DiGA) maintained by the Federal Institute for Drugs and Medical Devices (BfArM) in accordance with Section 139e(1) SGB V pursuant to Section 33a SGB V, agreement regarding the definition of the test criteria was declared by me within the deadline of 31 March 2022 (30th AR No. 6.9).

This marked the successful completion of a major step towards replacing the previous procedure of providing evidence of compliance with data protection requirements by way of self-declaration by the manufacturers.

In the future, proof of compliance with data protection requirements shall be provided using a certificate pursuant to Art. 42 of the GDPR (cf. No. 8.16).

The BfArM is also striving for the role of programme owner for the certification of digital health applications. This means that, in addition to the material test criteria, the BfArM also specifies how the respective criteria are to be tested and proven in the certification procedure.

As programme owner, the BfArM makes the test programme available for use by third parties who carry out the actual certification by granting licences after its completion. I am monitoring the ongoing procedure for the preparation of the audit programme in an advisory capacity and assume that it will be completed in the course of 2023.

**Cross-references:**

8.16 Certification and accreditation

## 8.3 Sormas (follow-up)

**The further development of the SORMAS programme for digital contact tracing in the health authorities again required close monitoring by the data protection supervisory authorities this year.**

This year, together with several State Commissioners, I again provided data protection support for the research project SORMAS@DEMIS, funded by the Federal Ministry of Health (BMG) and conducted by Helmholtz-Zentrum für Infektionsforschung GmbH (HZI), which involves the development of software for digital contact tracing in health authorities (30th AR 2021 No. 4.1.2).

This intensive consultation led to significant improvements, especially in its technical implementation. These improvements were achieved, among other things, through the specific adjustments and additions to the cryptography concept, the pseudonymisation concept, the IT security concept and the data protection impact assessment.

As the funding of the project by the BMG expired on 31 December 2022, the non-profit SORMAS Foundation was already established in summer 2022 to ensure the continuation of the project and the offer of the software for the health authorities. This will have the task of supporting the provision and further development of SORMAS from January 2023. The actual operation of the software will continue to be run by Netzlink GmbH. With regard to the data hosting, a migration of the data from the ITZBund to a server operated by Netzlink GmbH is also planned in the medium term. This is expected to be completed by June 2023.

Due to this reorientation, the data protection consultation within the framework of the research project, which will end on 31 December 2022, has also been completed by several state data protection commissioners and

myself. In future, this will be done by the respectively competent state commissioners.

## 8.4 Use of health insurance numbers (follow-up)

**The legislator creates the necessary legal basis for the use of health insurance numbers in the telematics infrastructure.**

In the 30th Activity Report (No. 6.5), I presented my demand for a clear basis of legitimacy for the use of health insurance numbers (KVNRs) in the telematics infrastructure. The legislator has met this demand with the Act on the Assessment of Nursing Staff in Hospitals and on the Adjustment of Further Regulations in the Hospital Sector and in Digitalisation (Hospital Nursing Relief Act – KHPflEG). Thus, Section 290(4) SGB now provides for the authority to use KVNRs within the framework of the telematics infrastructure of providers and users of applications and services within the meaning of Section 306(4)(1) and (2) for the unambiguous identification of the insured person, insofar as this is necessary for the unambiguous allocation of data and services when using these applications and services.

The legal basis for the inclusion of private health insurance companies (PKV) and other payers in the clearing procedure to exclude double allocation of KVNRs, which I also demanded, was created by an amendment to Section 290(3) SGB V with the Act to Strengthen the Protection of the Population and, in particular, Vulnerable Groups of Persons from COVID-19 (COVID-19 Protection Act) and entered into force on 17 September 2022 (cf. Federal Law Gazette. I p. 1454).

## 8.5 Coronavirus warning app: Changes 2022

**I do not find all the changes in the coronavirus warning app successful**

I also continued my consultations on the coronavirus warning app (CWA) in 2022. Due to the already established processes in the CWA and the decrease in infections, only a few of the changes were addressed. Since, according to the project team's assessment, many releases did not require any changes with regard to data protection law, my advice was only used in a few cases. And so, unfortunately, I only learned about some of the changes through the press. This also concerned the innovations to a changed colour design of the certificate view. The idea was to indicate through a green display whether the conditions for exemption from the mask requirement would be met if a federal state ordered this. Only after my critical enquiry were these plans then presented to me by the Federal Ministry of Health and the Robert Koch Institute. Unfortunately, not all the recommendations made during my consultation were heard in this case. Rather, contrary to my recommendation, the CWA was equipped with an automatic calculation and colour display of the mask requirement in the certificate view. Of course, it can be very helpful for a user to have the respective valid mask obligation calculated for the respective federal state. If the user presents the certificate, a verifying authority (e.g., an innkeeper) can read directly in the app whether a mask obligation exists or not. However, the calculation could also have been carried out only at the request of the person using the certificate and the result of the calculation could also have been displayed away from the certificate view in the CWA. The CovPassCheck app has been explicitly developed for the data-saving verification of certificates. Consequently, an assessment of the mask requirement for the examining body should have been implemented only in this app, and not in the CWA!

Here, too, data protection-compliant implementation should be kept in mind as early as the formulation of regulations. The obligation to provide evidence encroaches on the fundamental right to informational self-determination and requires careful justification. If verification is indispensable for reasons of health protection, target-oriented checking must be possible. A brief glance at a coloured indication in the display does not fulfil the requirements.

However, as far as I know (up to the editorial deadline of this Activity Report), no federal state has enacted a corresponding regulation on the mask requirement, so that this feature does not apply.

Overall, it should be noted that in the case of possible further developments of the CWA, care should be taken not to impair the high level of trust that citizens have in the app by adding additional functions that are more complex in terms of data protection.

## 8.6 Register modernisation/implementation of the OZG (Online Access Act)

**Register modernisation between a new departure and detailed work: Can the right to informational self-determination be guaranteed even if the state holds the strings for data aggregation?**

With the promulgation of the Register Modernisation Act (RegMoG) in the Federal Law Gazette on 06 April 2021, a new phase of this major project of administrative digitalisation began. The BMI, which is in charge, as well as Bavaria, Hamburg, North Rhine-Westphalia and Baden-Württemberg jointly set up the overall control of register modernisation in October 2021 in order to be able to fulfil the numerous requirements from various legal areas. The requirements include, among others, the implementation of the once-only principle, both in terms of the OZG and of the GDPR, as well as the introduction of a register-based census. The self-imposed goal of the overall management is to create a comprehensive inter-agency communication system (OOTS). This system is intended to ensure the direct exchange of evidence between both national and European authorities. The tax ID now used as an identification number – contrary to my advice – forms the central backbone of this.

**Once-only principle**

The aim of the once-only principle is that citizens and businesses only have to provide certain standard information to the authorities and administrations once. With the inclusion of data protection provisions and the explicit consent of the users, public administrations are allowed to reuse and share the data with each other.

As already mentioned in my previous Activity Reports (see 29th AR No. 5.1, 28. AR No. 5.5, 27. AR No. 9.2.2), I consider the current design of the ID No. to be incompatible with the fundamental right to informational self-determination and thus the IDNrG (Act on the Introduction and Use of an ID Number in Public Administration) as part of the RegMoG to be unconstitutional. Together with the Data Protection Conference, I have expressly warned against relying on the tax ID as a uniform, cross-sectoral personal identifier. There is still a danger that the technical backbone of citizen-centred administrative digitalisation has been built on a constitutionally unsafe foundation. This is a danger that has been recognised not only by the Bundesrat and the Scientific Service of the Bundestag, but also by the current federal government, which itself calls for a constitutionally sound modernisation of the registries (see Coalition Agreement, p. 15).

This fundamental issue has not been solved with the implementation of the overall control of register modernisation. Rather, it hangs like a sword of Damocles over this phase, which should actually be devoted entirely to the implementation of this important building block. This situation also has an impact on my advisory work. On the one hand, I continue to work with senior agencies and decision-makers to develop an alternative approach to the current ID No. Both familiar data protection-friendly models, such as the use of sector-specific identifiers, and completely new approaches are under discussion. The primary goal remains establishing an eye-level relationship between the state and the citizenry. For this, transparency, participation and structural obstacles to mergers remain the decisive factors, which any alternative discussed must also guarantee.

On the other hand, I, together with representatives of the DSK, have gladly participated in the overall control of register modernisation since the beginning, despite the fundamental concerns. My authority and I are currently active on several levels and, with regard to other elements besides the ID number, are working towards establishing informational equality as far as possible there as well. These levels of overall control are divided into strategic control (steering group, transformation unit), operational control (project board, advisory boards and competence teams) and individual sub-projects. The steering committee reports directly to the IT Planning Committee. The IT Planning Committee remains the policy steer for register modernisation. In an advisory capacity, I am currently mainly active in the steering committee and in the so-called Legal / Data Protection Competence Team.

My consultations currently focus in particular on the conceptualisation of the aforementioned OOTS (comprehensive inter-agency communication system). This communication system is to become the technical and architectural basis for being able to implement the once-only approach in Germany. The OOTS is divided into the national and the European part. The national part is intended to enable communication between national authorities and registries in such a way that relevant evidence for digitised administrative processes (e.g., within

the framework of the OZG) can be exchanged directly, without repeatedly having to collect it from the citizen.

The basics of the planned process were developed in collaboration with the lead agencies, with a special focus on ensuring transparency. At the same time, I advised the Legal / Data Protection Competence Team on questions regarding the planned legal implementation (so-called once-only general clause). In this context, I particularly welcome the planned establishment of a technical preview function, which is intended to provide citizens with a visual representation of the intended proof before the actual transmission within the framework of their digital application process. In my opinion, this is a function that is absolutely necessary in order to carry the constitutional balance between the right to informational self-determination and the state's interest in administrative efficiency over into the digital age.

In addition, the planned general clause is also intended to allow the use of the ID No. for entities that have not been directly covered by the IDNrG so far (as a rule, non-register-keeping entities that offer OZG services). The idea of such a holistic approach to the law is not necessarily questionable under data protection law. In my opinion, however, it is particularly important that at least the requirements for processing the ID No. that already apply under the IDNrG are then also made obligatory centrally for the newly registered offices. The special compensatory measures of the ID No., such as the data protection cockpit, must always follow this. This principle still applies even if I consider the measures regulated so far, as already mentioned, to be insufficient in themselves.

The data protection cockpit as a sub-project associated with the overall control of register modernisation is the subject of intensive consultation. The project has been in the implementation phase since September 2021. The DSK and I, together with the leads Bremen and the BMI, have mainly advised on the technical design, including the data transmission standard, as well as on various legal issues arising from the IDNrG. In particular, in my opinion, even the initial storage of the ID No. in the registries / public bodies as "use" falls under the logging obligation in terms of Section 9 IDNrG and display in the data protection cockpit. From the outset, citizens must be granted the necessary transparency to be able to easily trace the course of their personal data, which is easier to record through the ID No.

Only a holistic approach that allows the right to informational self-determination to flourish in a new, digital environment can sustainably achieve the goal of register modernisation.

## 8.7 Corporate integration management (BEM)

**A trusting cooperation between the employment office and the affected employees based on transparent data processing is especially indispensable for the BEM procedure. Against this background, the question of whether the Equal Opportunities Officer may receive a copy of the invitation letter must be assessed.**

The BEM is an instrument to help employees with longer periods of incapacity to work to return to work. The purpose of the procedure is to find out the causes of incapacity for work and to jointly look for a way to avoid or reduce future periods of incapacity for work. Since data on illnesses is regularly processed in the procedure as sensitive data within the meaning of Art. 9 GDPR, and since this may only be done on the basis of informed and voluntary consent of the employee according to Section 167(2) Social Code Book IX (SGB IX), this aspect is a recurring topic in my practical work.

Trusting communication and cooperation between all parties involved is indispensable for the BEM procedure to be successful. Only when a basis of trust has been created and the employee has been informed about which of his or her personal data will be used by whom and for what purpose can he or she engage in the BEM without fear.

As the BMI has stipulated in its personnel file guideline, it is therefore imperative that the BEM procedure is not carried out by employees who are entrusted with career support tasks. All data collected in the course of a BEM must be kept outside the personnel file. A separate BEM file must be set up for this purpose, which is to be kept as a dedicated file outside the personnel administration office. Personnel administration employees may not access this file.

Due to a request for advice, I have currently been dealing with the question of whether the Equal Opportunities Officer (GleiB) can receive a copy of the invitation letter to the employee as standard when a BEM procedure is initiated. As far as can be seen, this question has not yet been decided by the highest courts.

In my opinion, the decisive factor in the current legal situation is how the relationship between the provisions of Section 25(2)(2) in conjunction with Section 27(2)(2) Federal Equal Opportunities Act (BGleiG) and Section 167(2) SGB IX is interpreted in relation to each other. In terms of the basic system, there is no general precedence for one of the two areas of regulation between the BGleiG and the SGB IX. Equality as well as rehabilitation

and participation of people are, first of all, equally valid as legal goods.

Purely from the wording, the BEM procedure can be subsumed under the term "social affairs" with the consequence that it would be the task of the GleiB to monitor these procedures and provide it with all information on them at an early stage in accordance with Section 27(2)(2) BGleiG. However, the term "social affairs" is in itself a relatively vague term, which does not suggest that when enacting the relevant provisions, the legislator gave specific thought to the BEM procedure and deliberately wanted to make regulations on it.

In contrast, Section 167(2) SGB IX contains specific and detailed individual provisions on the BEM procedure. In particular, the provision specifies who can be a party to the proceedings, in some cases with what specifications. The staff council is specifically assigned a monitoring role. The fact that the provision deals very explicitly with different participants (staff council, representatives of the severely disabled, company/works doctor, etc.) and their tasks, and at the same time says nothing about the Equal Opportunities Commissioner, indicates that the legislator does not want to assign a task to the Equal Opportunities Commissioner within this specific procedure.

In addition, in the context of the Participation Strengthening Act of 2 June 2021, the legislator has once again dealt with the group of participants and has created the new possibility for the person concerned to additionally consult a person of trust in Section 167(2)(2) SGB IX. Furthermore, the legislator did not include the GleiB separately in the specific BEM procedural regulation.

Overall, in my view, Section 167(2) SGB IX is to be regarded as a lex specialis in the current legal situation, which prevents recourse to the more general provisions of Sections 25(2)(2), 27(2)(2) BGleiG as a legal basis. There is thus no sufficient legal basis for the standard transfer of personal data in connection with the BEM procedure to the GleiB.

## 8.8 The 2022 census

**The implementation of the census has again led to numerous submissions from citizens this year. In particular, the involvement of a US IT service provider in the operation of the census website has caused the number of complaints to skyrocket.**

After being postponed by one year, the census was officially launched in May 2022. The state statistical offices and their survey agencies conducted the building and housing census and the household survey. Among the submissions and complaints about the concrete implementation of these surveys, there were also repeated questions and criticism about the legal provisions. For example, many respondents and callers expressed incomprehension regarding the requirement to provide the names of home owners as auxiliary characteristics of the building and housing census. In this respect, an insufficient explanation by the statistical offices about the necessity of this information is to be noted at minimum.

In further submissions to me, an exclusion of data subjects' rights under the GDPR was also addressed and my help was requested. Since such restrictions, which are in principle permissible under the GDPR, are based on regulations under state law, I had to refer to the competence of the colleagues of the data protection supervisory authorities of the federal states in these cases. For their part, they had to forward numerous submissions to me regarding the online procedure for the census offered for the first time by the Federal Statistical Office. I see this involuntary "exchange" between the federal and state supervisory authorities as evidence of the definition of the concrete responsibilities of the data processing agencies of the Federation and the states involved, which I had already criticised as inadequate during the legislative process.

The majority of enquiries and complaints in my area of responsibility have reached me since mid-May 2022. The main subject matter of these submissions was the involvement of a US IT service provider in connection with the provision of the websites for the 2022 census and the related fear of an unauthorised outflow of personal census data to the USA. For its part, the Federal Information Technology Centre (ITZBund), which was commissioned by the Federal Statistical Office to operate the websites, had commissioned the service provider to secure them against attacks and to improve performance. I immediately examined the matter in detail and, as an immediate measure, ensured that the problematic involvement was suspended. As a result, I have also initiated a data protection supervisory procedure against the ITZBund.

Even if it turned out early on that access to the access data and content details entered via the online portal for the census surveys was not technically possible, I did not consider the agreed precautions against the transmission of the IP address of the user devices as personal data, which is unavoidable as is typical for the service, to be sufficient insofar as it could also include recipients outside the scope of protection of the GDPR. As a result, the

ITZBund has not used the services of the said company since around mid-October.

**Cross-references:**

4.3.3 Use of a content distribution network (CDN) for the 2022 census website

## 8.9 Data protection with online virus scanners

**Before using an online service for virus or malware protection, it should also be checked whether personal data can be entrusted to it.**

In the report year, I dealt with the data protection aspects of the use of online virus scanners. The detection of and defence against computer viruses and other malware is not only an important information security task, but it is also important for data protection. In order to ensure an adequate level of protection for the processing of personal data, companies and public authorities are obliged under Art. 32 GDPR to take appropriate technical and organisational measures. The use of virus and malware scanners is standard in electronic data processing. Corresponding products, processes and services are offered in many forms, both as desktop or server applications and via online services.

All solutions regularly have in common that they not only serve information security and data protection, but that data protection must be observed before and during their use. Usually, files that contain personal data must also be checked for viruses and other malware. It is irrelevant whether the texts, images, metadata or other content refer to identified or identifiable people.

It is therefore particularly important to check how personal data is processed, whether this is done in compliance with data protection law and what risks are involved before using new protection tools. If the check shows that data protection-compliant use is possible in principle, but that a high risk must be assumed, a data protection impact assessment must be carried out. If no mitigation measures are taken, the supervisory authority must be consulted. If a protection instrument cannot be used in accordance with data protection, it must not be used. Where this appears difficult, the supervisory authorities are there to advise. Even exceptional situations, such as the restrictions due to the coronavirus pandemic, must not result in a data protection check of new protection instruments not being carried out, not being carried out with due diligence or not drawing appropriate conclusions.

In the reporting year, the Federal Office for Information Security (BSI) published a warning[63], which is also relevant to data protection law. As part of an incident, it was discovered that suspicious email attachments were uploaded to an online virus scanner for virus/malware scanning at one institution. This was an online service that has uploaded files checked by a variety of different antivirus programmes and malware scanners to improve detection. However, with some of these online services – which are sometimes offered free of charge to users – not only IT and IT security service providers but also other customers gain access to all uploaded files. Clients who gain access to the data may include, for example, academics, journalists, various companies and even intelligence agencies, including those based outside the European Union.

An example of such an online service is "VirusTotal" operated by Google Inc., whose mode of operation is described in its terms of service and which contains a clear warning on its upload page that no personal information should be uploaded. The warning is to be taken seriously.

The contents of uploaded confidential documents must now be considered as public. Personal data is disclosed to an undefined group of persons. Uploading personal data of third parties is therefore usually a data protection breach unless, exceptionally, a sufficient legal basis justifies the processing. Since the upload leads to unauthorised access to personal data, it must be considered a reportable violation of the protection of personal data.

Especially against the background of the tense geopolitical situation, the BSI's warning should be taken as an opportunity to become aware of the possible risks presented by online virus scanners. Special care is required in their selection, evaluation, implementation and use, not only to protect confidential data, but also as a duty under data protection law.

## 8.10 Digital data spaces and mobility data in the transport sector

**The federal government is planning a Mobility Data Act. Together with "acatech – the German Academy of Science and Engineering", the Federal Ministry of Transport has created a platform for trading mobility**

63 Cybersecurity Alert No. 2022-206270-1032, available at https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2022/2022-206270-1032_csw.html

**data. This will also involve real-time data from moving vehicles. These may also reveal a lot about routes driven and driving behaviour.**

The European Commission and the EU Member States have high hopes for the value creation opportunities in a data-driven digital economy. To this end, the EU Commission presented a draft regulation on harmonised rules for fair data access and use ("Data Act") in February 2022 to enable the economic exploitation of data in a legally secure manner. Together with my European colleagues, I have taken a critical stance on this in the European Data Protection Board[64]. This explicitly includes data from the many smart devices of the "Internet of Things (IoT)", which produce a wealth of personal data when they are used by people or are in private households. In principle, this also includes modern networked vehicles. Specifically for vehicles, the Commission has announced a special legislative provision for the second quarter of 2023 that will oblige manufacturers to provide competitors with fair access to data, functions and resources in vehicles.

Data-driven value creation requires trustworthy data spaces, in which providers can make their data available to other participants in the data space for well-defined processing purposes on a contractual basis without having to fear misuse by unauthorised third parties. Such a data space was set up for the mobility sector at the instigation of the federal government. "DRM Datenraum Mobilität GmbH" was founded in 2021 with the aim of enabling public authorities, companies and scientific institutions to make mobility data available for the development of data-driven business models in an IT-protected environment. I was involved in the foundation process and advised on the drafting of the model contracts. Participants in this trustworthy data space created in this way are not only authorities, such as the German Weather Service (DWD), but also German car manufacturers and their suppliers.

The participation of private individuals as data providers is not initially envisaged and personal data is not the focus. In this respect, I have not yet been able to push through my request to use the opportunities of digitalisation in the case of personal data to directly involve private data subjects in the contractual relationships and to provide model contracts for this. The data space created in this way thus serves primarily to protect business interests and not the interests of private individuals who may be affected. This will make its use more difficult when it comes to exploiting data from moving vehicles. As a rule, it will only be possible to use this data if it has been anonymised beforehand. It must be taken into account that a wealth of different data or data collected in close temporal succession is usually difficult to anonymise. For guidance on possible measures, I have already taken a position on this in connection with the use of telecommunications data.[65]

As far as access to data, functions and resources from vehicles for mobility services of all kinds is concerned, vehicle users must therefore also be granted comparable possibilities for usage control as we know them from the world of smartphones and tablets. Whether the vehicle sensors are also used for the vehicle manufacturer's parking space finder or another third party must not be beyond the control of the vehicle users. Together with my colleagues from the federal states, I am committed to providing practicable ways for vehicle users to have control over digital access to their vehicles at all times. Vehicle users must have easy ways to find out and control which data, functions and resources are currently being used for which mobility service. General terms of use or contractual clauses will not be the right place for this. In the data spaces to be created, the protection of the interests of private individuals must be given the same priority as the protection of business interests.

Due to the current importance of the topic, I organised a political forum on 18 October 2022 entitled "My Car. My data!", at which I held discussions with representatives of the automotive industry, consumer protection and the Federal Ministry of Transport and Digital Infrastructure. I made it clear that only those who are given the means to control the use of their data at any time can make sovereign decisions about the use of their data. This presupposes that the protection interests of these persons are also protected at a high technical level in the data spaces and, in particular, that no cyber risks arise from the networking of vehicles for the good of a digital economy.

**Cross-references:**

4.2.4 Data Governance Act, 4.2.5 Data Act

64 EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), available at: https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf

65 Position paper on anonymisation under the GDPR with special consideration of the telecommunications industry, available at: www.bfdi.bund.de/konsultation

## 8.11 TrustPid – New paths in personalised advertising

**Until now, personalised advertising on the internet has employed advertising cookies. These enable the tracking of internet users and their behaviour in order to target advertising. Fortunately, many browsers now make it more difficult to use these cookies. In a pilot, German mobile phone providers have now come up with something new to offer an alternative to the old familiar advertising models.**

This project, called "TrustPID", attracted media attention in various articles last year. It is used to recognise mobile phone users on websites. During the reporting period, two mobile network operators (Vodafone and Deutsche Telekom) worked on a feasibility test, which was conducted in Germany together with major news websites, among others.

How does the data processing take place in detail?

TrustPID uses users' IP addresses and mobile phone numbers to generate a pseudonymous identifier. The legal basis for data processing is the user's consent under data protection law, which is obtained by the website operator (in the pilot project, e.g., at Bild.de). This also includes the processing of traffic data (dynamic IP address) by the mobile network operator.

Only if this consent has been given will the user's IP address be transmitted to their mobile network operator. Of course, this only works if the respective mobile phone provider participates in the test operation. The respective network operator uses the IP address to determine the telephone number and then uses this to create a unique, pseudonymous network identifier for TrustPID.

The provider of the advertising marketing service, Vodafone Sales and Services Limited, based in the UK, in turn generates further – also pseudonymous – marketing identifiers from this pseudonym. These marketing identifiers allow advertisers to personalise online marketing. For example, this enables website operators to recognise users when they visit their website again. Advertising platforms can also recognise users in order to market ads that are appropriate to their interests.

Improvements after my consultation

I was informed about the project by the participating German mobile network operators. I am not responsible for the provider of the advertising marketing service in the United Kingdom. My supervisory responsibility is exhausted by the participation of the German mobile phone providers in the project.

In my advice, I particularly pointed out the data protection requirements of consent. Specifically, it must be explained in an understandable, easily accessible form and in clear and simple language how the data will be processed. This is not only about the creation of the identifiers shown based on the IP address by the respective mobile phone provider, but also about the use of these identifiers, e.g., in the field of advertising marketers and by all other actors involved.

Building on my advice, the consent was made more transparent and the website www.trustpid.com was fundamentally revised. The revocation and objection options have also been heavily modified at TrustPID based on my advice. For example, an objection should initially only be stored for 90 days. This was adjusted after my remonstration: revocation of data processing is now valid indefinitely until there is a contrary expression of will from the data subject.

Outlook

My advice helped to resolve many relevant concerns with TrustPID. In terms of data protection policy, the service can be viewed ambivalently. On the one hand, only pseudonymised data is processed on the basis of consent under data protection law. On the other hand, telecommunications providers in particular have a special position of trust, which I find difficult to reconcile with tracking their users. In addition, other dangers such as the merging of the pseudonymous identifier and, for example, the log-in to services of providers on the web, which would lead to re-personalisation, must be considered and prevented.

It remains to be seen how the project will develop after the end of the active project phase. In the case of a European implementation of the project, the assessment of the then competent European data protection supervisory authorities will also be decisive. My office will continue to actively accompany this process to ensure compliance with all data protection requirements.

## 8.12 Video conferencing services

**Video conferencing services have become a matter of course in our living and working environment, and new forms of virtual and hybrid collaboration have become established. Accordingly, there are many discussions about data protection in video conferencing in practice. Since the introduction of the new Telecommunications Act (TKG) on 1 December 2021, commercial video conferencing services are legally to be considered telecom-**

**munications services, making them subject to the data protection jurisdiction of the BfDI.**

In order to clarify questions of data protection law in connection with the implementation of a video conference, the various legal levels in connection with the provision of the video conferencing service and the respective data protection responsibilities concerned must be notionally separated from each other. This is the only way to determine the data protection law applicable to the respective area and the concrete obligations existing thereunder. In the TKG of 1 December 2021, the term telecommunications was broadly defined and now includes in a functional sense all ordinary services that enable the direct, interpersonal and interactive exchange of information (see also Section 3(24) TKG). This refers to services that are provided for third parties and usually in return for payment.

The provision of a video conferencing service within the meaning of the TKG

Thus, the commercial provider of a video conferencing system is also a provider of telecommunications services within the meaning of the TKG, and is therefore obliged to comply with the data protection principles of the Telecommunications Telemedia Data Protection Act (TTDSG) and the TKG. In addition, it must comply with the necessary technical and organisational measures and observe the general data protection requirements under the General Data Protection Regulation (GDPR), insofar as they are not superseded by the specific provisions of the TTDSG. This includes, for example, that the provider of the video conferencing system only processes the personal data collected in the course of conducting the video conference for its own purposes if there is a legal basis for doing so. No recordings may be made without consent and the provisions of Art. 44 et seq. GDPR must be observed in the case of transfer to a third country. Further details on this, such as the Data Protection Conference's (DSK) guidance on video conferencing systems and a checklist, can be found on my website. [66]

Pursuant to Section 29 of the TTDSG, the BfDI is responsible for data protection; the one-stop shop procedure of the GDPR does not apply. In the case of cross-border constellations, it depends on whether a telecommunications service is provided in Germany (cf. Section 1(3) TTDSG).

Data protection obligations for users of video conferencing services

What content and personal data is the subject of a video communication is determined by the respective users of the system. Insofar as a company or public authority processes personal data in the context of a video conference, it is the data protection controller in this respect. The data concerned here can include names and, where applicable, the email addresses of the invited participants as well as the content discussed in the video conference, provided it is personal data.

It is up to the company or authority to weigh up the risks as to whether a video conference takes place at all, which video conferencing system is used (e.g., own or external system) and which special settings can additionally ensure the security of personal data.

The overall risk potential of the personal data specifically concerned is of particular importance for the balancing process. There are various parameters here. For example, a particularly high risk potential is to be seen if it concerns particularly sensitive data within the meaning of Art. 9 GDPR, i.e., the processing of special categories of personal data.

## 8.13 News about email – change of responsibility to the BfDI

**While providers of email services were not to be considered providers of telecommunications services within the meaning of the (old) Telecommunications Act, at least after the Google Gmail ruling of the European Court of Justice (ECJ, 13 June 2019, Case C-193/18), the legal situation has fundamentally changed with the introduction of the new Telecommunications Act (TKG) of 1 December 2021. Now, providers of email services are also to be categorised as providers of telecommunications services under the TKG. This means that they are covered by my special responsibility for telecommunications.**

In the TKG of 1 December 2021, the term telecommunications was defined broadly and now includes, in a functional sense, all ordinary services that enable direct, interpersonal, interactive exchange of information between persons (see Section 3(24) TKG). This therefore also includes emails, voice-over-IP and video conferencing (so-called over-the-top (OTT) applications).

**Data protection requirements**

The provider of an email service is thus obliged to comply with the data protection principles of the Telecommunications Telemedia Data Protection Act (TTDSG) and

66 www.bfdi.bund.de/videokonferenzen

the TKG. In addition, it must comply with the necessary technical and organisational measures according to Section 165 TKG and Art. 32 GDPR. In accordance with Section 29 TTDSG, responsibility under data protection law lies in principle with the BfDI.

Independently of this, the sender of an email may also have obligations under data protection law. Depending on the constellation, a data protection risk assessment must be carried out in each individual case to determine whether an email is the appropriate medium for the specific data concerned, which encryption should be chosen and which email provider should be considered.

**From the BfDI's advisory practice**

Recently, I have received numerous questions from citizens who have forgotten their login details for their email account and now no longer have access to their emails. Even though I was unable to help in these cases, it shows me that the providers of email accounts obviously take their obligations under data protection law seriously and protect the email accounts effectively against unauthorised access. Access to the email account is only possible if the respective person can authenticate himself/herself as an authorised person precisely with regard to the email account. It is not enough just to provide proof of being the person in whose name the email address may be.

This strict behaviour of the email providers is good and right from a data protection point of view. In many cases, citizens store many emails in their email account, which contain an abundance of personal information and cross-references. It is therefore important to secure access to this account. On the other hand, for citizens, this means that they should not "misplace" the access information to their account, just as with their front door key. Otherwise, there is also the danger of "locking oneself out".

It can also prove unfavourable if one provides false information for the alternatively provided security queries – perhaps even "for safety's sake" – which one can then no longer remember later. Effective data protection thus also requires corresponding digital skills among all those involved as well as an awareness of the protection of one's own data. Here, I will continue to advocate both for simple and understandable but secure systems and for broader data protection awareness.

## 8.14 Data protection for digital identities

**The need for secure identification and authentication in the digital space has grown, as the debate on VideoIdent (No. 8.1) shows. In a hearing of the Committee on Digital Affairs of the German Bundestag, I pleaded for the increased use of the online function of the identity card (nPA) as a data protection-friendly solution. At the European and international law level, I have worked to protect citizens from profiling and over-identification.**

From an overarching perspective, the establishment of secure digital identities plays a key role in the successful implementation of important digitalisation projects in the health sector or the digitalisation of administration. User-friendly digital identities represent an opportunity for digital participation and are in conflict with the constitutional right to informational self-determination. The basis of my hearing in the Committee on Digital Affairs was a proposal of the European Parliament and of the Council for a regulation amending the "eIDAS" EU Regulation (910/2014) with a view to establishing a framework for a European digital identity. In the hearing of the Bundestag Committee on Digital Affairs (ADi) on 4 July 2022, I highlighted data protection risks of app-based mobile ID wallet solutions (wallet for digital identities). Such risks include, in particular, profiling through behaviour and location tracking, the danger of "over-identification", i.e., the requirement of identification for legal transactions on the net, for which registration with a pseudonym would normally be sufficient, and new lines of attack against identity theft. The hearing revealed the picture, which I also share, that the nPA offers a secure and also more convenient solution for identifying persons in cases where this is required by law. I had already advocated the use of the nPA in my 30th AR (No. 6.19).

The EU Commission sees the introduction of a European ID wallet as a priority project to strengthen the European digital single market. For the eIDAS Regulation, I argued that wallets should not be linked to a unique personal identifier for the purpose of user identity matching, as this presents a risk of user profiling. On this point, I campaigned for an improvement of the EU Commission's draft with the support of the federal government. The federal government was not able to push through this position in the Council, especially since other Member States do not have similarly advanced systems like the nPA. However, according to the current state of the draft regulation, a compromise has been reached. This compromise involves a privacy-friendly service- and sector-specific solution that is tied to the lifetime of the device with which the wallet is used. Recitals on "ledger

technologies" were also included in the draft regulation. Here, I campaigned for a technology-neutral version of the draft regulation. Unfortunately, I was not able to push this through, as the opinion prevailed in the federal government to merely improve the recitals on "ledger technologies" instead of insisting on their deletion

The digital identities project had, as already mentioned in my 30th AR (No. 6.19), planned to develop an ID wallet that would be partially based on blockchain technology. This resulted in complex data protection issues that have not yet been adequately clarified. I therefore see it as positive that this approach is not being pursued in favour of the existing system for digital identities, which is data protection-friendly and of high quality from a security point of view, and that the use of the nPA is to be promoted more strongly. The digital identities project was transferred to the inter-ministerial and inter-agency "Governance Laboratory" Digital Identities format ("GovLab DE"). A "Governance Laboratory" is an innovation laboratory for the administration, which tests new technologies, ways of working and processes. I continue to advise the Governance Laboratory on data protection aspects of German digital identity solutions.

At the level of international law, the Council of Europe has adopted Guidelines National Digital Identity supplementing the Protocol to Convention 108 on Data Protection ("Convention 108+"). The Federal Ministry of the Interior and Home Affairs (BMI) involved me in commenting on them. Fortunately, a note from me on avoiding profiling through global and permanent identification numbers was included in the convention text.

User-friendly digital identities represent an opportunity for digital participation, but they exist in an area of conflict with the constitutional right to informational self-determination. Design requirements can be met by designing the legal and technical framework in a data protection-friendly way, which I will continue to advocate for.

**Cross-references:**

8.1 News from the telematics infrastructure and its applications

## 8.15 Data protection in the smart home

**The rollout of smart metering systems in accordance with Section 2(7) of the Metering Point Operation Act has begun. Electricity meters can thus be read remotely while complying with the highest cyber security standards. This also enables consumption to be recorded during the year, giving consumers an overview of their electricity consumption at all times. The smart metering systems can also be used for gas, water and heat metering, but there is only a legal obligation to do so in individual cases. Furthermore, a transitional regulation makes it possible to bypass the privacy management functions of the smart metering system, for example for heat metering.**

With digitalisation in the energy sector, new opportunities for digital business models are also emerging there. In household energy metering, not only an annual work value is now collected, but in the case of electrical energy, a work value every quarter of an hour, i.e., about 36,500 work values per year. Due to the resulting risk to privacy through user profiles, the Metering Point Operation Act (Messstellenbetriebsgesetz, MsbG) was created in 2016 with the Act on the Digitalisation of the Energy Transition (Gesetz zur Digitalisierung der Energiewende), which took cyber security and data protection concerns into account in an exemplary manner. In particular, the so-called smart meter gateways (SMGW), which enable energy meters to be networked with the internet, not only set standards for cyber security; they also function as a privacy information management system (PIMS) at the same time. They grant consumers the greatest possible control over the use of the data available from smart meters, sometimes every millisecond. For electrical energy metering, the MsbG comprehensively regulates which body may receive and process which data for which purpose in terms of data protection law. In particular, the law regulates that only smart metering systems in which smart meters communicate via a smart meter gateway approved according to the strict technical guidelines of the Federal Office for Information Security (BSI) may be used for remote reading of electricity meters.

Unfortunately, the beneficial regulations for consumers do not extend to other sectors of the energy sector. The Heating Costs Ordinance (HKV), which was amended in 2021, provides – understandably, against the background of the costs for the use of a smart meter gateway – for compulsory use of smart meter gateways only within the framework of so-called multi-segment metering for economic reasons, if a metering point operator is responsible for both electricity and heat metering and, if applicable, for other segments. No amendment of the legal basis is planned in the area of water metering. The use of smart meter gateways also remains optional for gas metering.

With an amendment to the MsbG within the framework of the Act Amending the Energy Industry Law passed in July 2021 (Bundestag document 20/2402), it became possible to already use smart meter gateway interfaces, which are not yet sufficiently specified in terms of functional security and which are intended for the remote control of installations in the home network of the connection users in accordance with Section 14a of the Energy Industry Law. This possibility arose because this interface is distinguished by secure communication encryption as well as cryptographically secured identification of the access users, and therefore its use should be possible in particular for control purposes without having to fulfil requirements for the functional security of the remote control. This does minimise the risk of unauthorised persons being able to use the interface. However, unauthorised use of the interface by authorised bodies remains technically possible.

As has become apparent in the meantime, the feature of a functionally still undefined but secure connection is also attractive for those sectors of the energy industry that are not legally obliged to use smart metering systems. On the one hand, this is to be welcomed because at least a secure transmission to previously identified bodies can be guaranteed. On the other hand, such a connection for energy metering purposes would not correspond to the state of the art, because the precautions for data protection-compliant metering value processing on the gateway could be circumvented. For heat metering, for example, there is no guarantee that metered values will only be transmitted to the extent required. In the industry hearings conducted by the BSI on behalf of the Federal Ministry of Economics and Climate Protection (BMWK) on the further development of the smart meter gateway, I therefore made it clear that using the interface intended for control purposes for measurement purposes does not correspond to the state of the art. I also welcome the BSI's approach to also formulate security requirements for devices that are to be connected via this interface by means of an additional technical guideline.

Legal simplifications to accelerate the energy transition must not and need not be made at the expense of data protection and cyber security. The smart meter gateway basically gives consumers a high degree of control over meter readings collected in their private sphere. The possibilities to control the use of the metered values must also be expanded against the backdrop of current efforts by the EU Commission on the usability of data from data-producing IoT devices (Internet of Things) for value creation in the digital economy. In this respect, I will also advise the federal government on the upcoming amendment of the MsbG to accelerate the energy transition.

**Cross-references:**

4.2.4 Data Governance Act, 4.2.5 Data Act

## 8.16 Certification and accreditation

**The GDPR enables data controllers to voluntarily verify compliance with their requirements, which can be proven by certificates or data protection seals, and provides a basic legal framework for this in Articles 42 and 43. Trust and transparency should thus be increased and verifiable compliance with data protection requirements ensured. The bases for this are kept relatively open in the articles mentioned, in order to leave room for national specificities. As a result, the design processes have taken up a lot of time, because fundamental work first had to be done at both national and EU level so that the complex implementation could succeed. However, initial procedures at EU level have now been completed, so that certifications can be expected in the course of this year.**

GDPR certifications are intended to serve as proof of compliance with the requirements of the regulation. Certificates may only be issued by those who have previously been accredited as a certification body in a defined procedure. The purpose of this procedure is to achieve a particularly high quality of the certificates at the end of the process.

**Accreditation as a quality feature**

Pursuant to Section 39 of the Federal Data Protection Act (BDSG), the competent data protection supervisory authorities decide whether a body may act as a certification body. They do so in cooperation with the German Accreditation Body (DAkkS) (cf. Section 4(3) AkkStelleG [Accreditation Body Act]). The process of accreditation is quite complex and time-consuming[67]. It requires compliance with defined criteria. These were developed by the independent federal and state data protection supervisory authorities in the Certification Working Group, a subgroup of the Data Protection Conference (DSK), and certified in accordance with ISO/IEC 17065 with a special focus on the area of data protection. [68]

67 An overview of the individual steps of the accreditation process can be found at: https://www.dakks.de/content/projekt-datenschutz.

68 Criteria of the DSK, available at https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf

The existence of a certification scheme that contains the corresponding certification criteria is essential for the accreditation of a certification body – these must also be approved first. The Certification Working Group has also developed orientation guidelines for this purpose[69], which were reviewed again in the reporting year and published in an updated version in summer 2022.

In order to complete a successful accreditation process, a large number of steps are required at European and national level before a certification body can operate on the basis of its certification scheme. As a result, these high standards should also contribute to particularly trustworthy evidence and make it easier for applicants to embark on the path towards certification with the clearest possible specifications.

**National certification criteria approved**

The North Rhine-Westphalia State Commissioner for Data Protection and Freedom of Information (LDI NRW) was the first German data protection supervisory authority to approve national certification criteria in the reporting year. The "European Privacy Seal" (EuroPriSe) certificate is intended to certify to companies that their processing operations comply with the requirements of European data protection law. I have been intensively involved in this approval procedure and in other procedures for national certification criteria, such as the Luxembourg certification procedure GDPR-CARPA, in the committees of the European Data Protection Board (EDPB). Numerous German and other European supervisory authorities have received corresponding new applications, which are in various stages of processing at national and EDPB level. Overall, it can be stated that there is movement in the field of data protection certification.

The Federal Institute for Drugs and Medical Devices (BfArM) is one of the first authorities to develop a special certification programme to specifically strengthen the rights of patients in digital health applications (DiGA) and digital care applications (DiPA) with regard to data protection. My authority is involved in an advisory capacity in the implementation of the legal regulations in concrete inspection criteria[70] and the development of a corresponding programme. I will continue to accompany this process intensively (8.2. Digital health apps)

**First EU Privacy Seal launches**

Beyond the certifications at national level, there is also the possibility of obtaining a European Privacy Seal. Again, the criteria must be approved by the EDPB. In October 2022, the EDPB approved the first European Privacy Seal. In its opinion [71]on the Europrivacy certification criteria submitted by the Luxembourg data protection authority (CNPD), the EDPB considered that the submitted certification criteria were in line with the GDPR. The independent federal and state data protection supervisory authorities did not support the positive opinion within the EDPB because, from the German point of view, there are still ambiguities in the implementation. I would have welcomed it if individual aspects of the Seal had gone through another revision before being adopted. Now that the Seal has been approved, I will of course continue to accompany its implementation with a view to achieving the most uniform, high-quality level of data protection possible.

A vibrant certification landscape

In future, certifications are to create trust and legal certainty with regard to lawful data processing as a recognised standard. One of the aims is to create an environment in which data protection compliance is promoted.

The first national certification criteria have also been adopted for other EU Member States. Numerous other applications have been submitted, which give reason to expect a lively certification landscape.

Trustworthy, high-quality accreditation and certification procedures are an indispensable prerequisite for credible evidence that the GDPR is complied with in processing operations by controllers and processors. For this very reason, special emphasis was placed on the design of the processes at both national and European level. The wait is over – now, the first certificates can go on the market and prove their quality. They will also make it easier for small and medium-sized enterprises to design their own data processing in compliance with the law by selecting providers or processors.

**Cross-references:**

8.2 Digital health apps

69 DSK certification criteria, available at. https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_V2_0_Stand_21062022.pdf

70 BfArM certification programme, available at: https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutzkriterien.pdf

71 CNPD statement, available at: https://edpb.europa.eu/system/files/2022-10/edpb_opinion_202228_approval_of_europrivacy_certification_criteria_as_eu_data_protection_seal_en.pdf

# 9 Inspections and advisory visits

One of my main tasks is to carry out inspections at the data processing bodies under my jurisdiction. Inspections can be carried out both on an ad hoc basis – for example, on the basis of tips from citizens or media reports – and without any reason. There is also a variety of different types of inspections in terms of implementation and the range of topics; from general cross-sectional to specific focus inspections, and from written questionnaire inspections to on-site inspections lasting several days, there is a variance in the selection of the right type of inspection depending on the respective need.

Inspections are particularly important in the security sector, where – as already stated by the Federal Constitutional Court – data protection inspections fulfil a kind of compensatory function for encroachments on the fundamental right to informational self-determination, which are generally not recognisable to data subjects. For this reason, many laws in this area also provide for so-called compulsory inspections. These already oblige me by law to inspect particularly intrusive data processing at regular intervals.

Irrespective of the type of inspection in question, an essential element of my inspections is always my advisory function vis-à-vis the responsible body. In this way, data protection violations can be avoided well in advance. After all, the aim is not to uncover and sanction as many data protection violations as possible, but to consolidate data protection awareness in practical application through regular monitoring, thereby helping to protect the persons whose data is processed in the long term.

With this in mind, I have – despite the restrictions still imposed by the coronavirus pandemic – again carried out a large number of inspections in this reporting period.

## 9.1 Coronavirus-appropriate inspections

**The coronavirus pandemic again required a certain degree of flexibility and creativity in my inspection activities in this reporting year. Due to the pandemic, the previously most frequently used instrument of on-site inspections was expanded to include questionnaire inspections and inspections combined with video conferences. The positive results will also change my inspection activities with effect for the future.**

Monitoring compliance with legal requirements and reviewing regulatory instructions are two of my core activities. Until a few years ago, this meant that my staff visited the offices I supervised on an ad hoc or non-ad hoc basis and carried out on-site inspections, sometimes lasting several days.

Under the travel and contact restrictions due to the coronavirus pandemic, as well as the obligation to protect my staff, suitable ways had to be found to ensure an appropriate inspection density. In addition, many of the bodies to be inspected also had their staff working from home on a large scale, which made it even more difficult to carry out effective on-site inspections.

A solution to this new challenge was found in the form of remote inspections. On the one hand, I carried out more inspections where the inspected bodies were given a structured questionnaire which they had to answer and return by a certain deadline. Through a variety of closed and open questions, I inquired about incidents, processes or practices of the inspected bodies.

A great advantage of a questionnaire inspections is that they can be easily scaled, i.e., sent to several supervised entities with the same content. If the answers given by several inspected bodies are placed next to each other, a cross-comparison is possible, through which the general level of data protection in an area can be concluded.

Follow-up questions, however, cannot be collected immediately, but only after the first answers have been

evaluated and jointly written, which can delay the preparation of inspection reports. I also found that not all inspected bodies answered adequately at the first attempt during the written inspection, which often necessitated follow-up questions.

Withholding information, however, is never an option for an inspected body: as the supervisory authority, the BfDI has corresponding investigative powers under the General Data Protection Regulation, which also enable it to enforce its interest in information.

In contrast to the questionnaire inspections, with a combination of written inspection and video conferencing, other topics not specified by me in advance can also be inspected at short notice. In this form of inspection, I provided the questions and the content to the inspected bodies in advance, which were then explained in detail in a video conference.

Using video conferencing tools with the possibility to play back presentations or visualise processes, a constructive exchange resulted that also went beyond the given content. Such an inspection enables the inspected body to prepare the content well and is highly efficient for my staff, as they can access the modern communication infrastructure of the office and travel time is saved.

In summary, the different types of inspection complement each other excellently and enable me to ensure an appropriate inspection density, taking into account technical, ecological and other aspects, even as pandemic restrictions are lifted. Thus, depending on the content of the inspection, there will be no exclusive return to the traditional on-site inspection in the future, but the most suitable form of inspection will be chosen in each case.

## 9.2 Monitoring storage regulations in financial administration

**Overall, digitalisation in financial administration continues to make progress and, from a data protection point of view, is predominantly on a path in the right direction. To stay on this path, I have provided recommendations and guidance to the ministries of finance. Let's hope that the individual stragglers don't leave the path and catch up quickly.**

In 2020, I started an audit of the regulations on the retention and storage of personal data within the scope of the German Fiscal Code (Abgabenordnung, AO) in all 16 federal states. I was able to complete this audit in this reporting year. Special emphasis was placed on the storage regulations of the Federal Ministry of Finance and their respective implementation under state law by the Ministries of Finance of the federal states.

I gained a positive overall impression during my audit. Nevertheless, I made recommendations and suggestions on the individual focal points of the audit in order to further strengthen data protection and raise the basic level achieved. In particular, there is still much potential for improvement in the conversion to complete electronic transaction processing.

Although the federal states have already introduced electronic transaction processing in various forms, I urgently recommend a prompt and complete conversion of all tax offices to electronic files and digital processing. In this way, the principles of data minimisation and, if applicable, information claims by data subjects can be implemented in a practically effective and efficient manner.

In addition, this would make it easy to record and log all long-term items (e.g., overviews of special depreciation and increased deductions) that are stored beyond the usual retention periods in a standardised electronic form.

From a data protection point of view, it would also be welcome if uniform regulations were made in the federal states on annual cut-off dates on which paper documents are actually eliminated, and if suitable supporting programmes were made available to employees. This could easily ensure timely elimination.

In the development, conversion and introduction of the coordinated new software development of the tax administration (KONSENS programmes), which is already underway, I urgently recommend that simple and obvious options such as regular, in particular size-independent deletion of tax files be carried out in order to ensure timely deletion of electronic data in compliance with data protection requirements until the development and implementation of the KONSENS overall case administration is completed. Furthermore, I see it as necessary to push ahead and prioritise the development and implementation of the KONSENS overall case administration more decisively than before.

Unfortunately, I have discovered that the basic retention period for income tax, corporate income tax and trade tax transactions has been increased from 15 to 20 years. For this reason, I consider it necessary to take even more targeted care to limit the scope of the files to the really necessary components. This is likely to be in particular the (electronically stored) assessment data and, if applicable, the declaration data on which these are based.

Also, the storage of personal data beyond the actual conclusion of an external audit is only covered under Section 147(6)(2) AO (German Fiscal Code) to the extent that and as long as the data is still needed for the purposes of taxation (e.g., until the conclusion of any appeal proceedings). I therefore very much welcome the deletion list procedures to be used in the external audit with review by the head of the department or the internal service, and expressly recommend that all states introduce them for all audit services.

Overall, it can be seen that the advancing digitalisation in tax administration has positive and desirable effects on tax case processing and monitoring, especially with regard to retention and compliance with retention periods, but still has much potential for improvement in some areas. I therefore plan to carry out more in-depth inspections and consultations on individual key topics in the coming years.

## 9.3 Inspections of foreign representations in Kazakhstan

**European data protection standards are also binding for German missions abroad outside the European Union and the European Economic Area. The BfDI therefore also inspects Germany's embassies and consulates for compliance with these standards.**

The Foreign Service consists of the Federal Foreign Office (AA) and the missions abroad, which together form a single federal authority headed by the Federal Minister for Foreign Affairs. As part of this federal authority, the missions abroad are thus subject to my supervision under data protection law.

This year, my staff carried out an inspection and advisory visit to the German Embassy in Astana and the Consulate General in Almaty. The focal points here included the restructuring of the internal data protection organisation in the AA and the processing of personal data in the context of visa applications/processing. In this context, the involvement of an external service provider working for the AA on site was also examined.

The inspection report is currently still being agreed, so that a formal conclusion of the inspection is not to be expected until 2023.

## 9.4 Inspections in the security sector

2022 was marked by a large number of inspections and consultations in the security sector. Many of my inspections in this sector are subject to secrecy. Due to the nature of the matter, I am therefore only allowed to report on them to a limited extent or not at all. The "need-to-know" principle applies. The following inspections and consultations therefore represent only a small sample of the work actually carried out.

### 9.4.1 Mandatory inspection: Covert measures at the BKA (Federal Criminal Police Office)

**The mandatory inspection left a very positive impression overall. Only in one case was a violation of data protection law found.**

Due to the restrictions of the coronavirus pandemic in 2021, I could not conduct the mandatory inspection until 2022. Six self-security measures according to Section 34 of the Federal Criminal Police Office Act (BKAG) as well as three very extensive so-called security procedures, in which measures had been carried out according to the fifth Section of the BKAG, were to be audited. These are covert data collection measures in advance of threats of international terrorism.

I was able to inspect and review all orders and resolutions. The same applied to the documentation in the case processing system VBS and the data in the uniform case processing system eFBS. I was also allowed a data query and check in the police information system INPOL.

Overall, the documentation stood out positively. Almost all measures had been comprehensively recorded. The required notifications to data subjects and their documentation could also be verified and had generally been carefully implemented.

Only in one case concerning a measure according to Section 34 BKAG did the documentation not make it possible to fully retrace the decisions of the BKA. In addition, a rather formal breach of data protection law occurred in this process. In the run-up to the self-security measure, the court order to be obtained for the enforcement measure to be secured was missing.

However, the execution of the self-security measure then revealed that the enforcement measure was unlikely to yield any further findings, and could therefore be dispensed with. However, this is an isolated case. There was also considerable time pressure, and a court order could very probably have been obtained, as in my view

the legal requirements were met. I have therefore refrained from issuing an objection.

### 9.4.2 Mandatory inspection of intrusive measures in the Munich Customs Investigation Office

**The Customs Investigation Service Act allows customs investigation offices and the customs criminal investigation office to use special means of data collection if offences of considerable importance are suspected within their jurisdiction. These means are subject to my special duty of inspection under data protection law.**

Special means of data collection are characterised by the fact that data can also be collected covertly, i.e., without the knowledge of the data subjects. My data protection inspections are particularly important in this area. They are intended to compensate for the fact that, due to lack of knowledge of the measures affecting them, it is not possible for data subjects to seek judicial redress themselves. Since 2021, I have therefore been obliged by the new Customs Investigation Service Act to regularly monitor the use of these means.

This year, I fulfilled my inspection assignment at the Munich Customs Investigation Office. The inspection focused on the use of longer-term observations as a special means of data collection.

The restrictive use of the invasive measure should first be emphasised as positive. This led to the fact that I was able to carry out a full inspection in the inspection days available to me, i.e., that all the files available for the longer-term observations could be checked.

During my inspection, I found deficits in particular in the proper keeping of records, such that I issued two complaints as a result. On the one hand, this involved the traceability of the investigative work and the course of the procedure, and on the other hand, the documentation of how the legal notification obligations were followed.

The complaints were accepted without reservation by the Federal Ministry of Finance and the Munich Customs Investigation Office and the failures were admitted. At the same time, internal work instructions were immediately adapted and new work processes were established to ensure proper file management in the future.

### 9.4.3 International data transmission by the BKA

**During the reporting period, I attended a mandatory consultation and inspection appointment at the Federal Criminal Police Office (BKA). The subject matter of the inspection was the transfer of personal data of minors to third countries in 2020 and 2021.**

In a total of around 280 random checks for the years 2020 and 2021, I examined at the BKA whether personal data of minors was lawfully transferred to third countries.

Only in one case did I find that the data transfer had not been necessary and objected to this in accordance with Section 16(2) of the Federal Data Protection Act (BDSG). In order to identify a connection owner in a criminal investigation, the BKA made a request to Interpol Kazakhstan. Personal data of a suspect living in Germany was also transmitted. This transmission was not necessary to establish the owner of the connection. The BKA admitted this violation during the inspection.

In the remaining cases, I could not find any violations of the data protection rules according to which the BKA transmits data to third countries. Most of the cases I examined were cases in which the Federal Criminal Police Office handles the necessary official traffic with third countries for the state police authorities in its so-called correspondence function. In these cases, it is mandatory for the BKA to conduct at least a summary substantive legality review. The BKA, on the other hand, describes this function as a “messenger function” and considers a formal legality check to be sufficient.

This topic was already the subject of my last inspection (cf. 29th AR No. 9.5.4). According to a circular of the BKA, in case constellations of personal arrest procedures, which it carries out in its correspondence function for the federal states, the BKA always obtains the facts of the case, the offences as well as additional information from state police authorities before it takes action for these authorities. I conclude from this that the BKA is aware of its responsibility under data protection law and in practice certainly carries out a summary examination that goes beyond a mere formal legality examination.

However, the documentation of some of the cases audited was not transparent to me on site. In a debriefing, the responsible case workers at the BKA explained the factual and legal basis of the data transfer. However, such a follow-up discussion cannot replace proper documentation.

The BKA must file each individual decision of police action separately and comply with the principles of proper file keeping. I had already criticised deficits in this

area in the past (see 28th AR No 6.7.3, 30. AR No. 8.2.2). Against the background of the current audit results, I stand by my indications of the need for change in file management at the BKA.

### 9.4.4 Mandatory inspections of the ATD/RED

**After carrying out the mandatory inspections of the Anti-Terrorism Filing System (ATD) and the Right-Wing Extremism Filing System (RED), I stand by my basic assessment that the benefit of these files for the security authorities – incidentally, also according to the opinion of the participating authorities themselves – is very low, with at the same time far-reaching encroachment on fundamental rights due to the large number of connected authorities and the sensitive data stored. In this respect, I continue to call for the abolition of both systems in their current form.**

The Federal Ministry of the Interior and Home Affairs (BMI) has so far not responded to my criticism in past inspection reports (see 30th AR, No. 8.1.1) of the manner of automated storage in both filing systems, which in my assessment makes my inspection of the data history considerably more difficult, with a redesign of the technical solution.

Both the ATD and the RED are filled with sometimes very sensitive personal data. The resulting encroachment on fundamental rights also weighs heavily because a large number of authorities can in principle access it. However, the dimension of the encroachment on fundamental rights contrasts with the suitability of the construct. The immediate impressions on the actual use and the benefit for the work of the security authorities rather confirm my opinion that the ATD and the RED need a comprehensive reorganisation or even abolition.

**Inspection at the Federal Intelligence Service (BND)**

I carried out the inspection of the ATD at the BND in May 2022. Data records that could not be satisfactorily discussed in the written inspection in 2020 due to the pandemic were also inspected. I have not found any significant deficits in data protection law that could be objected to. However, I have made practical recommendations, among other things, on deletion resubmissions and on the documentation of the decision on concealed or limited storage. These have already been implemented, and the inspection has been completed.

**Inspection at the Federal Office for the Protection of the Constitution (BfV)**

At the end of 2021, I was able to carry out and complete the on-site inspection of the use of both the ATD and the RED at the BfV. After intensive examination, I did not make the weaknesses in the automated filling interfaces, which in my view still exist, the subject of a new inspection in the last inspections, because, as already explained above, the BMI had not initiated any improvements in the technology during the last few years, despite assurances to the contrary. Thus, no new findings were to be expected here. The standstill merely confirms the impression of a little-noticed database. In the current inspections of both the ATD and the RED, I did find data protection deficiencies in individual storage operations, but the BfV remedied these immediately. I was therefore able to refrain from issuing an objection in both cases.

**Inspection at the Federal Office for the Military Counter-Intelligence Service (BAMAD)**

At the BAMAD, I carried out the regular inspection of the use of the ATD in the reporting year 2022. During the inspection, I criticised the storage of data records that continued to be stored without basis after the conclusion of a foreign deployment of the Bundeswehr. The BAMAD then agreed to delete this data. These last remaining records of the BAMAD in the ATD were indeed deleted immediately. That is why I have refrained from issuing an objection here.

**Inspection at the Federal Criminal Police Office (BKA)**

At the end of 2021, I inspected the ATD at the BKA. In the process, I discovered that not all storage operations were in line with data protection law. In addition to two recommendations for adjustment, I therefore also lodged two objections.

I objected to the lack of possibility of a case-by-case examination – partly provided for by law – in the automated transfer of data from the source file to the ATD. Furthermore, the BKA had not deleted the data on a person until three years after the investigation had been closed and thus not without delay within the meaning of Section 58(2) of the Federal Data Protection Act (BDSG).

In several cases, I also found data on persons who have since died. In individual cases, I do not want to exclude the possibility that it may be necessary to continue to store data of deceased persons in view of the objectives of the ATD. However, this also carries the risk that legal requirements can be circumvented. I therefore recommended that the deletion of data of deceased persons be reviewed. I additionally recommended separate documentation of the storage requirements.

The inspection of the RED storage operations could not be completed by the editorial deadline.

**Inspection at the Federal Police (BPol)**

The mandatory inspection of the ATD from 2021 was completed in the reporting year 2022. There was no reason for a complaint. However, as the documentation deficits from the previous inspection in 2019 had not yet been remedied to our complete satisfaction, I again had to make recommendations for improvement. As long as my recommendation to dissolve the filing systems altogether is not implemented, it is to be hoped that, with each inspection, at least one more step will be taken towards optimising the documentation and thus towards upholding the rule of law.

The inspection of the RED in a selected BPol directorate, which began at the end of 2021, was also completed in the 2022 reporting year. The BPol checked the filing system themselves after I had given them notice of the inspection and found some deficiencies. My audit also uncovered a systemic error in the transaction processing system as well as minor documentation deficiencies. The systematic error is to be corrected with an update of the software; the documentation deficits have already been addressed in the meantime with adjustments to internal regulations.

In addition, I had to issue a complaint because not all records met the necessary storage requirements. The deficit has been eliminated in the meantime. Due to my inspection, a significant amount of data was deleted from the RED.

**I continue to recommend that the legislature abolish the Anti-Terrorism Filing System and the Right-Wing Extremism Filing System in view of their established low utility.**

### 9.4.5 PIAV (Police Information and Analysis Network) inspection

**Following a citizen's petition, I inspected the ad hoc deletion of legacy data records of the Customs Investigation Service in the narcotics database of the so-called Police Information and Analysis Network (PIAV). The inspection resulted in the deletion of 7,798 data records for which the continued existence of the storage requirements could no longer be determined without considerable effort.**

In 2021, I received a citizen's submission. The investigation uncovered a discrepancy in the storage of personal data between the internal Customs Investigation Service information system (INZOLL) and PIAV Narcotics. While the storage in INZOLL had long since been deleted, it could still be found in PIAV for all association participants. The facts suggested that it might be a systemic issue in connection with the transfer of the previous data stock from the narcotics case file (FDR) to the PIAV.

**Police Information and Analysis Network**

The PIAV is part of the joint information system of the German police. The PIAV brings together data from the BKA, state police stations, the Federal Police and also the customs authorities, each of which supplies the data from their internal systems. Within the PIAV, the "Narcotics" component is an offence-related database in which cases of narcotics crime with transnational significance are to be entered. It replaced the narcotics case file (FDR) in mid-2018. The data stock contained in the FDR at that time was migrated to the PIAV in the course of the replacement.

On this occasion, an inspection was carried out at the customs investigation office in 2022. It was discovered that the legacy records from the former FDR did not have a functioning process set up in PIAV for deletion on an ad hoc basis. Therefore, in these cases, necessary deletions that were completed in the INZOLL were not been passed on to PIAV.

After these facts had been established, the ZKA also recognised the existing data protection violation and submitted a constructive proposal for a solution on its own initiative. Since it would have taken considerable effort to determine whether the storage requirements continued to exist in each individual case, all of the 7,798 records migrated from the FDR at that time were deleted from the PIAV as a result of the inspection.

The performance of the customs investigation service's tasks was not impaired in the process. Data records that are still needed for the fulfilment of tasks are still available in the INZOLL and can be transferred to the PIAV again if required. A repetition of the error can be ruled out. Relevant data records from the INZOLL have been transmitted directly to the PIAV since mid-2018. For this purpose, a new, automated interface was set up, which ensures synchronisation of the systems.

### 9.4.6 Inspection of data retrievals in the automated information procedure

**The Federal Criminal Police Office (BKA) has technical and organisational precautions in place to prevent abusive queries of telecommunications data.**

The powers of law enforcement authorities to access data files or to demand information about personal data from public and non-public bodies harbour a potential for data misuse. As a number of publicly disclosed cases show, such powers can be abused, for example, to spy on people – such as partners, ex-boyfriends, celebrities or neighbours – for personal motives. Even though these did not concern the BKA, I carried out an inspection there on the handling of personal data in the automated information procedure according to Section 173 of the Telecommunications Act, without giving a specific reason.

The inhibition threshold for abusive retrieval could be lower with this type of retrieval procedure, if only because the retrieval of personal data can be carried out automatically. The customer data concerned is primarily telephone numbers, other connection identifiers, the name and address of the connection owner, in the case of natural persons their date of birth, in the case of fixed network connections also the address of the connection and in cases where a mobile telephone terminal is provided in addition to a mobile telephone connection, the device number of this device as well as the date of the start of the contract.

I examined the technical and organisational precautions taken by the BKA to prevent abusive data queries in the automated information procedure. In addition, the legal requirements for data queries in the automated information procedure were checked on a random basis in a number of individual cases.

The inspection did not reveal any significant deficits in terms of data protection. However, there were potential improvements that could be achieved in terms of data protection law. In particular, it was possible to find and correct a software error that led to the duplicate processing of personal data in the course of the automated information procedure.

### 9.4.7 Radio cell database of the Federal Criminal Police Office

**The Federal Criminal Police Office (BKA) has filed a complaint against measures issued by me against its radio cell database. Due to an intentional loophole in the law, the BKA is allowed to continue operating the database for the time being, at least until a final court decision.**

In the 30th Activity Report (No. 8.2.4.), I reported that I had objected to the unlawfulness of data storage and data comparison operations in a radio cell database of the BKA. In this database, the BKA processes the radio cell data collected by the police authorities of the federal states in various investigation procedures.

In my opinion, the BKA has no legal basis for the extensive data processing that I was able to ascertain in the database that was the subject of the objection. I therefore gave a binding order to the BKA not to store any further personal data in this database and to delete the personal data stored there. I forbade the BKA from carrying out further data comparisons until the personal data had been deleted.

The BKA and the Federal Ministry of the Interior and Home Affairs do not share my legal opinion. The BKA therefore filed a lawsuit against my injunction. Due to the suspensive effect of this action, the BKA is not required to comply with my order until a final court decision. The possibility of an authority to order immediate enforcement of an administrative act it has issued, which is actually customary in German administrative law, if immediate enforcement is in the public interest or in the overriding interest of a party involved, has been expressly excluded by the legislature in Section 20(7) BDSG.

The restriction of this power was introduced in isolation and purposefully only with a view to enforcing European data protection law. I see this as a significant limitation of effective data protection supervision. For this reason, I have asked the European Commission to examine the compatibility of Section 20(7) BDSG with European law.

### 9.4.8 Coordinated inspections of alerts for covert/targeted checks in the Schengen Information System

**In June 2019, European data protection authorities had agreed to systematically inspect alerts for covert/targeted checks in the Schengen Information System (SIS). In Germany, the federal and state data protection supervisory authorities then carried out coordinated inspections of 27 police and intelligence services. Several formal and material violations of the law were found. The German supervisory authorities have issued or are planning various measures and recommendations.**

Across Europe, the number of alerts for covert/targeted checks under Article 36 of Council Decision 2007/533/JHA of 12 June 2007 in the SIS has increased steadily in recent years. With this category of alerts, persons or

objects can be alerted for law enforcement or security purposes, and on the basis of this, covert or targeted checks can then be carried out and a range of data can be transmitted to the body issuing the alert. Comprehensive movement patterns of the data subject and their companions can be generated from the hit reports of such alerts. This therefore constitutes an intensive encroachment on fundamental rights.

Against this background, the European working group on the coordinated supervision of the SIS, the SIS II Supervision Coordination Group (SIS SCG), decided to take up the issue and carry out joint inspections. The aim is to get to the bottom of the increasing numbers and to get an overall picture of the use of this tool and related data protection issues. At the same time, the legality of such

The SIS II Coordination Group ("SIS II SCG") is a body established by the SIS II Regulation and the SIS II Framework Decision to monitor the protection of personal data in the SIS II information system. The group consists of representatives of the national supervisory authorities of the Member States and the European Data Protection Supervisor.

Although the number of these alerts in Germany has not increased much compared to other Member States, the federal and state data protection supervisory authorities have agreed to carry out coordinated inspections in Germany as well.

In the area of the police forces, I have therefore carried out two inspections of covert/targeted alerts at the federal level (see also 27th AR No. 9.3.5). Most recently this year, I audited the relevant alerts of the Federal Criminal Police Office and found no violations. However, I recommended that the documentation of records be improved.

In the area of intelligence services, I carried out three inspections of alerts under Article 36 of Council Decision 2007/533/JHA of 12 June 2007 in recent years (29th AR No. 9.2.9 and No. 9.2.10 and, most recently, 30th AR No. 8.2.6 and 8.2.7). In addition, 11 state supervisory authorities participated in the inspections, resulting in a total of 27 federal and state bodies being inspected. Further audits in this area are planned.

A number of formal and material violations were found during the federal and state inspections, such as errors in the ordering of alerts, the calculation of deadlines, the documentation and the retention of files. Corresponding measures and recommendations have been issued or are planned by the respective competent supervisory authorities. A Europe-wide evaluation of the results in the SIS SCG is planned to complete the process.

**Cross-references:**

9.2.9 Data protection supervision and consultation at the BfV; 9.2.10 Data protection supervision and consultation at the Federal Office for the Military Counter-Intelligence Service

## 9.4.9 Data protection supervision and consultation at the BfV

**In the reporting period, I conducted various inspections as well as information and advisory visits to the Federal Office for the Protection of the Constitution (BfV). The main focus was on the electronic file and its successor system as well as on various internet activities of the BfV.**

**Electronic file**

This year, I again advised the BfV on the large-scale project of the uniform document management system in the Constitutional Protection Network (Verfassungsschutzverbund [Verbund-DMS]). The Verbund-DMS is intended to ensure uniform case processing at the BfV, the state offices for the protection of the constitution and, in future, also at the Federal Office for the Military Counter-Intelligence Service (BAMAD) and to provide various interfaces for this purpose. The consultation with the BfV in this regard, which began last year, as well as the exchange with colleagues from the state data protection authorities, was continued.

I also took the planned introduction of the new case processing system and its great significance in terms of data protection law as an opportunity to check the current DOMUS system at the BfV. The focus was on the functionality and technical implementation of the full-text search for persons and compliance with the legal limits according to Section 13(4)(3) Federal Constitution Protection Act (BVerfSchG). The aim of the inspection was to identify possible weak points of the previous system in terms of data protection law and to include the results in the Verbund-DMS, which is still in development, at an early stage.

No objections were raised during the inspection. However, I discussed further technical organisational measures in relation to both systems with the BfV. One of these measures concerns internal data protection monitoring. Fortunately, with regard to DOMUS, the latter started with a new concept promptly after I pointed out the necessity of regular implementation, so that the inspection here was successfully concluded. Another inspection on my part, together with the official data protection body of the BfV, is planned for the coming year. In this context, it is to be examined whether person searches are exclusively used by the employees of the BfV within the legally permissible limits.

First results of the internal audit already started at the BfV unfortunately indicate that many BfV employees are unclear about the use of the person search in DOMUS. This does not automatically indicate deliberate abuse. However, it confirms the necessity of carrying out the planned joint inspection with the BfV next year and of further consolidating the already started internal audit as well as obligatory training of the employees as organisational measures without fail. The results of the inspection will be decisive in determining whether further technical measures are required for the Verbund-DMS in addition to the organisational measures already implemented with DOMUS.

**Information and consultation on new data collection and analysis systems**

As with most other security agencies, the BfV is increasingly opening up possibilities for obtaining information on the internet. There are different types of approach here, referred to in specialist circles by terms such as OSINT (Open-Source Intelligence – the gathering of information from public sources), SOCMINT (Social Media Intelligence – the gathering of information by means of social media) or ONI (operational use of the internet through covert information gathering by exploiting trust worthy of protection).

The exchange and dissemination of anti-constitutional statements, propaganda and disinformation, but also the mobilisation or the call for potentially anti-constitutional actions has been shifting more and more to the internet for years, partly openly, partly conspiratorially. For this reason, the Office for the Protection of the Constitution monitors and systematically evaluates relevant websites, but also social media platforms.

At the same time, new technical competences in modern data analysis methods are being developed. The BfV is reorganising itself and, as required by Section 14(1) of the Federal Protection of the Constitution Act (BVerfSchG), has recently submitted several file orders on new systems in this area to me for consultation.

As a result of constantly changing communication behaviour and technological advancements in society, the amount of data potentially to be searched or analysed is growing exponentially. The BfV must react to this (see below "Media file inspections"). From my point of view, it is important to store this data only to the extent absolutely necessary and for as limited a period as possible. If the data reveals no actual indications that the BfV is competent in this respect, the data must of course be deleted immediately.

I am in discussions with the BfV and the BMI about the extent to which the current legal norms are still viable for such data processing. In some cases, I see the further development of data collection and analysis systems as quite problematic.

In order to be able to better assess the actual specialist requirements and framework conditions of data processing, I carried out information and consultation visits in addition to inspections, the exact content of which I can only report here to a very limited extent due to confidentiality requirements.

In the reporting period, for example, I visited a relatively young organisational unit in the Technical Analysis Support and Data Mining Department as well as the Cyber Defence Division and consulted with the BfV specifically on individual procedures for obtaining information on the internet. My impression from these meetings is that the BfV is facing new methodological as well as technical challenges here. It may also be necessary to react to this with corresponding amendments to the Federal Protection of the Constitution Act. For this reason, I will continue to closely monitor the developments in terms of data protection law and seek exchange with the BfV and the BMI for advice.

**Media file inspections**

The problem just described entails consequential problems for the storage of large media files. What is needed is the development and implementation of technical systems that systematically process, sort and archive media files on the internet (e.g., audio, video or text files) so that they can be found. For this purpose, the BfV offers a common database for the Constitutional Protection Network for the processing of media files. During the reporting period, I began to extensively monitor this database in terms of data protection law. In addition to examining the actual functioning of the application, the main focus of my audit is its integration into the system landscape of the Constitutional Protection Network in

terms of data protection law, compliance with storage and deletion periods, the rights of data subjects and the redacting of uninvolved third parties in media files. For reasons of confidentiality and the ongoing nature of my audit, I cannot provide any further information here.

**Inspection of covert alerts in the SIS II at the BfV**

The inspection of covert alerts in the 2nd generation Schengen Information System (SIS II), which was already carried out at the BfV at the beginning of 2020 (cf. 29th AR No. 9.5.1; 30. AR No. 8.2.7), was completed in the reporting year 2022. The inspection revealed some complex legal questions, which were discussed extensively with the BfV afterwards.

In my view, in many samples, the scope of the data transmitted by the BfV to the National Access Point (Supplementary Information Request at the National Level -Bureau, the so-called SIRENE Bureau) within the framework of the alert form was not covered by the SIS II Decision. I was not convinced by the BfV's argumentation that the transmissions were permissible according to the SIRENE manual. This is because as an implementing act, the SIRENE manual cannot override the provisions of the SIS II Decision according to the hierarchy of EU secondary law and grant more extensive powers to the Member States.

On the other hand, I criticised the scope of the data transmitted to the BfV on the basis of the alert pursuant to Art. 37(1) SIS II Decision. In a large number of the random samples, the data transmitted to the BfV, mainly by the Federal Police, could not be assigned to any category of the conclusive catalogue of the Art. 37(1) SIS II Decision. Due to the so-called primacy of application under European law, national legal bases cannot be used for the transmission of data beyond this catalogue.

Although the requirements for an objection pursuant to Section 16(2)(1) of the Federal Data Protection Act were met in both cases, I did not issue such an objection. This is because the data processing in question can no longer be assessed as contrary to data protection law following the introduction of the new, expanded third-generation Schengen Information System (SIS III), which is scheduled for March 2023, and the application of the new Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 (SIS III Regulation). In future, this regulation will allow more data to be transmitted than before; in particular, the BfV will in future have the possibility to request the transmission of data not included in the catalogue of Article 37(1) of the SIS III Regulation in individual cases. I take a very critical view of this power in terms of data protection law. I have therefore already announced to the BfV that in future inspections I will in particular comprehensively examine the existence of the alert requirements as well as the corresponding documentation.

### 9.4.10 Data protection supervision and consultation at the Federal Office for the Military Counter-Intelligence Service

**In the reporting year, I critically monitored the connection of the Federal Office for the Military Counter-Intelligence Service (BAMAD) to the Intelligence Information System (NADIS) and reviewed t he processing of data on reservists. I was able to continue two extensive inspections that I had already started in the previous year with pleasing results.**

**Connection of BAMAD to NADIS**

Since an amendment to the Military Counter-Intelligence Service Act (MAD Act) and the Federal Constitutional Protection Act in July 2021, these provide for the possibility of fulfilling information obligations between the BAMAD and the federal and state constitutional protection authorities through jointly maintained databases.

The NADIS system is used for this purpose in the Office for the Protection of the Constitution, and the BAMAD is now to be connected to it. The Federal Office for the Protection of the Constitution (BfV) and the BAMAD have submitted corresponding amendments to their file orders to me for consultation. Within the framework of the hearing procedures, I demanded the implementation of such an interlinking of the file systems in conformity with the constitution.

Already in the associated legislative procedure of 2020, I had welcomed the intensification of the exchange of information between the authorities as correct in substance, but had repeatedly insisted on the creation of constitutional disclosure regulations necessary for this (see 29th AR No. 5.5). Due to this year's rulings by the Federal Constitutional Court on the laws governing intelligence services, the responsible ministries are now required to reform the corresponding regulations (cf. No. 7.8). At the time of going to press, the consultation process was still ongoing.

**Review of the processing of data on reservists**

Due to the changing responsibilities between the BfV and the BAMAD, the intelligence processing of extremist aspirations among reservists involves a large volume of data transfers and data storage. In principle, the BfV is responsible for persons with reservist status; the

BAMAD is only responsible for the period of reservist deployment.

During the reporting period, I took a closer look at the forms of cooperation created for this purpose and called for the establishment of fixed guidelines and processes. Here, my main focus is to ensure that the rights of the data subjects – in particular the right to information – are protected. My review is still ongoing at the time of going to press. Even if improvements are achieved in practice in the near future, I believe that a clarifying amendment to the MAD Act is urgently needed in order to create legal certainty for the responsible persons in the authorities.

**Inspection of covert alerts in the 2nd generation Schengen Information System (SIS II) at the BAMAD**

I completed the inspection of covert alerts in the SIS II carried out at the BAMAD in the third quarter of 2021 (cf. 30th AR No. 8.2.6) in this reporting year. I am pleased that the practical recommendations I made in the inspection report, which concerned in particular the implementation or adaptation of process flows as well as the specifications for the deletion of alerts, have been fully implemented by the BAMAD.

**Inspection of data processing in the field of observation**

At the end of 2021, I started an extensive inspection in the BAMAD's area of observation (cf. 30 AR No. 8.2.6) and continued it in the reporting year. Due to the particular scope of the data set to be reviewed, my audit could not yet be completed.

In my inspection report, I informed the BAMAD of my findings as well as my assessment of the audited observation procedures in terms of data protection law, along with additional practical advice. So far, I have been able to refrain from issuing an objection. I expect BAMAD's response to my inspection report in 2023.

I have expressly reserved the right to file a complaint if the data protection concerns noted by me in the inspection report are not remedied in a timely manner. For reasons of secrecy and the continuation of my oversight, I cannot go into further detail here.

**I recommend to the legislator to issue legal clarification regarding the responsibility for reservists between the BAMAD and the BfV.**

**Cross-references:**

7.6 The Office for the Protection of the Constitution and the Federal Constitutional Court

### 9.4.11 Data processing at the BND (Federal Intelligence Office)

**In my 23rd (No. 7.6.1) and 30th (No. 6.16) Activity Report, I reported on violations of data protection law in the context of the operation of a large database at the Federal Intelligence Service (BND). This year, I carried out an inspection visit for this purpose, which resulted in objections.**

After years of intensive consultations on the data protection issues with this large database, an archive solution for the database was established in 2011 (30th AR No. 6.16). Data records for which no deletion resubmission was implemented contrary to legal regulations, which were stored in the database for longer than 10 years and which no longer have any current reference to ongoing processes, were and will continue to be moved to this archive until 2025.

In the archive, these data records can only be used for current purposes under special conditions, which the BND has laid down in a guideline. My visit at the end of August 2022 was aimed at inspecting the use of this archival data.

At the time of the inspection, the archive contained several million documents. Documents with personal data consulted in the course of the inspection dated back to the 1960s.

The research conducted in the archives since 2011 has basically been guided by the provisions laid down in the guideline. However, the examination of the necessity of further storage of the personal data consulted in the course of an archive search, which is provided for both by law and in the guideline, was not carried out. No relevance for intelligence could be determined during the inspection with regard to the documents.

I objected to the automated storage in an archive of personal data previously stored in the database for more than 10 years without checking for relevance to the order and the omission of the necessity check after access to personal archive data. The procedure has not yet been completed.

### 9.4.12 Data protection inspections in security clearance law – from exemplary to deficient

**Violations and deficiencies in the processing of personal data in connection with security clearances occur time and again. Some of these are common and run like a thread through my inspections. However, new issues are constantly arising. This notwithstanding, some inspected sites also showed that data protection-com-**

**pliant maintenance of security files and data files is possible.**

In this reporting year, I inspected a total of 16 agencies to determine whether they complied with the data protection provisions of the Security Clearance Act (SÜG). The starting point of my inspection activities is a new audit strategy that enables me to obtain a representative overview of all bodies that fall within the scope of the SÜG. In doing so, I take into account not only major stakeholders, but also in particular those bodies where experience has shown that the right to informational self-determination of data subjects is particularly challenged. Eight business enterprises and eight public bodies were the subject of my inspections.

The inspected business enterprises belonged to the following sectors: Guarding (1x), Research (1x), Telecommunications (1x), Industry (2x) and IT/Electronics (3x).

The authorities inspected are:

- the Federal Office of Economics and Export Control
- the Federal Office for the Safety of Nuclear Waste Disposal
- the Federal Office for Family and Civil Society Tasks (BAFzA)
- the Central Office for Information Technology in the Security Sector
- the Federal Criminal Police Office
- the Federal Office of Justice (BfJ)
- the Federal Office for Radiation Protection
- the Federal Ministry for Economic Affairs and Climate Protection (BMWK).

I inspected the BMWK in its function as the competent body for the non-public sector. The Ministry is responsible for the security supervision of commercial enterprises and decides whether or not enterprises may employ a vetted person in a security-sensitive position.

I issued one or more complaints against six authorities and six companies. In addition, I found numerous other violations or deficiencies for which, however, I refrained from issuing an objection for reasons of proportionality. As a result, I completely refrained from issuing any objections in the course of four inspections.

**Various sources of error**

Overall, I found proportionately fewer violations in business enterprises than in public authorities. In part, the processing of personal data in the economy was exemplary. However, some of my observations run like a thread through the majority of the inspections (cf. 28th AR No. 6.7.4, 29. AR No. 9.5.5, 30. AR No. 8.2.8). In particular, I often found personal data of uninvolved third parties and documents that must not be processed.

I made most of my complaints to the BfJ and the BAFzA. At the BAFzA, working from home during the pandemic led to pragmatic, but not data protection-compliant, procedures. Among other things, I objected to the unencrypted email communication with external recipients via unsecured networks. The Security Officer (GSB) sent various documents from the security clearance to her private email address so that she could print them out and process them at home. Furthermore, the BAFzA violated the separation requirement by having employees of the office responsible for human resources conduct on-site examinations of the security declaration in order to relieve the GSB.

Among other things, I objected to the BfJ about the lack of organisational measures. The staffing in the area of secret protection was so inadequate that it was not possible to ensure that the data protection requirements were properly met. In addition, the flow of information from the unit responsible for personnel to the Secret Protection Unit pursuant to Section 15a SÜG was insufficient. I also complained about this to the BfJ.

Frequently, authorities did not observe deletion and destruction deadlines and therefore received a complaint. In one case, I also objected to the continuation of a security clearance although no more security-sensitive activities were to be taken up. In another case, I objected to the processing of personal data without a legal basis. Furthermore, I raised an objection due to the inadmissible transmission of data from security clearance to the HR office.

I also came across unobserved deletion and destruction deadlines at business enterprises and objected to this. Another complaint resulted from incomplete file management. By destroying the security declaration prematurely, the company could no longer prove the data subject's consent documented on it to their audit and the related data processing operations. Furthermore, I objected to the lack of consent of the data subject to carry out the so-called visit monitoring procedure, by which companies register security-checked personnel with other companies or authorities. Also objectionable was an insufficient flow of information from the personnel administration unit to the security officer regarding security-relevant changes, insofar as these also affect data protection. This is the case, for example, if this triggers deletion deadlines.

**Pragmatic advice**

Despite the deficiencies and violations found, almost all audited bodies were positive about my inspections and the advice given. In addition, I found that comprehensive consultation in advance, especially also with regard to the digitalisation of security clearance, was positively reflected in the checks (No. 13.4).

Due to some shortcomings in the law (30th AR No. 6.20), the responsible bodies are forced – until the upcoming revision of the SÜG by the legislator – to find pragmatic solutions and at the same time comply with data protection requirements. This applies equally to my counselling.

Sometimes, this involves supposedly banal issues such as the "doctor title" in visit monitoring proceedings. The consent forms used provide that business enterprises may transfer the name and other personal data of their own employees to other enterprises, but do not include the academic title by default. However, this may be of considerable importance for the external image of a company.

A small addition on the standard form can help here. Nevertheless, the current legal regulation or lack of regulation of the visit monitoring procedure is burdensome for all sides and unsatisfactory in this respect. Even if I enable more data processing with my proposed solution, this serves data protection in the end, because it shows that security and economic interests also work with data protection.

**Cross-references:**

12.4 Consultation and professional exchange on the SÜG – A fruitful addition

# 10 BfDI internal

## 10.1 New strategy for the BfDI

**During the reporting period, I started to expand the strategy for my office and to flesh out the implementation. In a first step, a vision, mission and fields of action were defined together with strategic guiding principles.**

On the one hand, a strategy reflects the fundamental goals and values of the authority and its employees. In addition, however, it also represents the starting point for the development and implementation of the actual organisational and work management. In this way, it does not serve a pure end in itself, but creates a structure for daily work and thus, in addition to improved transparency, also offers real added value for all employees by helping to better plan and coordinate work and tasks in the future.

Therefore, it was important to me to design the process of further strategy development in such a way that all colleagues with an interest were given the opportunity to actively participate. After the office management had agreed on an updated vision, the resulting mission and fields of action were developed together with the associated strategic guiding principles in a total of seven full-day workshops with staff. I was very pleased that the offer to participate was widely accepted by my colleagues and that ideas and input from all areas of the authority and representatives of all career groups were able to contribute to the project.

**Vision**

We are a sought-after contact partner for digitalisation, legislation and government action.

**Mission**

Data protection protects people, not data. That is why people are at the centre of everything we do – both externally and internally.

Data protection is a fundamental right. In order to preserve this, we comprehensively inform, sensitise and advise citizens, politicians, administrations, companies and all other interest groups in a form appropriate to the target group and at eye level. If necessary, we use our regulatory options to enforce data protection.

This is a task that can only be accomplished together. That is why we work closely with national and international partner authorities and stakeholders, also because data flows do not end at borders.

Digitalisation largely determines our living and working environment, so that more and more personal data is being generated. In order to be able to meet the new challenges associated with this, we actively and competently accompany digital developments. To this end, we also keep ourselves technologically up to date.

In addition to data protection, freedom of information is also an important prerequisite for our democratic coexistence. That is why we are committed to transparency and also live by it ourselves.

Our employees are the foundation of our successful work. To ensure their satisfaction and motivation, we support them in their work-life balance and rely on a culture of transparency and open communication at all levels that allows and encourages change and criticism. The inclusion of people with disabilities as well as appreciation and respect for all employees, regardless of gender, sexual orientation, origin, religious or political views are guidelines for how we deal with each other. We also see sustainable action in ecological, social and economic terms as an important part of our responsibility. This creates an atmosphere in which we enjoy working and work well.

Thus, at the end of the first part of this strategy project, the current vision and mission are the most important. Behind the inevitably abstract vision is the idea that my organisation sees itself first and foremost as a competent point of advice that, due to the great expertise in its fields of activity, wants to be a contact partner for everyone, from citizens to public authorities and companies to the press, NGOs and politics, whether national, European or international. The mission describes in more concrete terms how we approach our tasks in order to consistently achieve the goal set out in the vision in the long term.

In 2023, in the second part of the project, the individual work units will define individual strategic goals and steps for their measurable implementation in order to finalise the overall strategy.

**How it works**

With the help of the examination system we have developed and suitable software, the data flows of products such as apps or web applications can be examined. Virtual machines, each emulating a computer, are used for the examinations. Different operating systems can be used on these virtual computers in order to be able to examine executable products there. By using virtual machines, different scenarios can be run through quickly and easily at the same time, and the dependencies and interactions between several product components can be simulated and examined on different systems.

## 10.2 Laboratory development

**In the year under review, work began creating an extended laboratory environment for the technical examination of IT applications, services and apps for my authority. We already had some initial experience with our own laboratory examinations in the area of telemedia. The developments now taking place should also allow for larger-scale investigations in all areas of my jurisdiction.**

Due to the expansion of digitalisation into every aspect of daily life, as well as in the work of federal authorities, technical aspects of data protection are playing an increasingly important role. Whether digital health applications or the use of digital identity documents, the use of smart electricity meters or web portals to specialised applications in federal authorities, browser-based procedures, smartphone apps and smart devices are increasingly being used.

In order to be able to check whether corresponding services, applications, apps and devices take into account the legal requirements of data protection, their technical characteristics should be able to be examined even more closely and, above all, “independently”, by my authority. We gained initial experience with individual investigations of websites and apps in the telemedia sector. Now, I have set up a separate unit responsible for running such an investigative environment. A virtualised investigative environment is being set up in which products can be examined simultaneously on different issues and their behaviour, such as sending data to the manufacturer, can be tested.

There are also plans to create opportunities to conduct major investigations of applications and devices – such as sensors and actuators of the IoT (Internet of Things) – jointly with external contractors under the leadership of my agency. In principle, third parties – such as the BSI (Federal Office for Information Security) – can be asked to carry out any form of investigation and commissioned to do so. However, in order to be able to carry out independent inspections, I have to be able to fall back on my own laboratory capacities.

In the future, the unit will enable technical audits in my inspection activities, but it will also be able to deal with technical issues arising from cooperation with civil society or assist in the comprehensible presentation of complex technical issues in my information materials for the public. Furthermore, cooperation with science and research in the field of technical development of electronic data processing will be promoted. In this way, I also want to increase the attractiveness of my authority for new employees and offer my employees the opportunity to expand their competences in these subject areas.

In order to use knowledge already available in the data protection community on investigative tools and methods and to disseminate my own results and findings, I am in active exchange with other authorities; exchanges with non-governmental organisations are also planned.

## 10.3 After the organisational review – follow-up projects

**The results of the organisational review are being steadily implemented. After the organisational review, I am currently carrying out various follow-up projects to further optimise my office. This involves the introduction of a central knowledge management system, the establishment and expansion of a central crisis management system and the introduction of a central controlling system including the collection of required key figures. Furthermore, I would like to further standardise the reporting system and optimise the authority's internal regulations.**

**Further development of central knowledge management**

The organisational review identified potential for optimisation, including the handling of knowledge, so that the topic of knowledge management was taken up in the reporting year and will be continued in 2023 as part of a project.

One of the findings of the organisational study carried out in my authority is that I would like to improve the handling of knowledge as a resource. Even though the average age in my office is unusually low, I also notice the demographic change in the workforce. Experienced holders of knowledge retire and the experiential knowledge that sustains an authority could be lost. I want to prevent this as well as the multiple elaboration of certain findings and the inconsistency in the approach. In order to be able to continue to work efficiently, I would like the new staff to share in the existing experience of my experienced staff. In the year under review, a new, optimised intranet for internal information was therefore implemented as a first step. The aim is to establish a holistic, structured knowledge management system in my authority within the framework of a project that contributes to a comprehensive knowledge transfer and preservation. This was also started in 2022, so that this goal can be achieved in the course of 2023.

**Development of a central crisis management system**

The handling of the consequences of the Covid-19 pandemic at the latest showed how important structured process flows are in crisis situations in an authority. These processes are being further developed.

In order to strengthen resilience against emerging crises, such as the further course of the pandemic, security policy changes or the protection of the IT infrastructure, etc., I will push for the systematic development of an overarching official crisis management system. The strategic and operational elements of crisis management are being examined, sharpened if necessary and developed into uniform target processes with additional external professional support. The definition of a crisis, the description of reporting channels, the establishment of a special institutional organisation in the event of a crisis (crisis team) and the interaction with already existing emergency regulations will form the main part of the study. The study on the establishment of crisis management system is being carried out in a project structure. The preliminary project plan foresees first results for the first half of 2023.

**Further development of organisational structure**

Taking into account the results of the organisational review completed in 2021 and the influx of additional tasks, my authority has continued to develop its organisational structure.

The topic of freedom of information is a name-giving component of our authority and has now also been established in an independent and expanded unit outside the departmental organisation directly under the authority management.

Other changes to the organisational structure concern Departments 1 and 2. The newly established Department 16 combines the responsibilities for internal administration and the foreign service. The topics of telemedia and telecommunications are now located in two independent units in Department 2. Furthermore, the technical expansion of my supervisory activity will be further reinforced by the establishment of the Technology Development/Laboratory and Cooperation/Supervision units via the Federal Office for Information Security.[72]

## 10.4 Personnel development and budget situation in 2022

**In the financial year 2022, the budget legislator granted me a total expenditure of €43,243,000 for my work on data protection and freedom of information. The vast majority of this expenditure is tied up in personnel expenses. I thank the budget legislator for providing the financial means to enable me to exercise my independent data protection supervision.**

My authority was granted 50 additional posts in 2022, which were identified as additional needs based on the organisational review conducted in 2021. My personnel

72 See organisation chart in the appendix

budget thus increased to a total of 396.4 posts, of which 375.9 are for civil servants and 20.5 are for pay-scale employees. As before, I am on a good path to successively fill the positions made available to me. Last year, I was able to fill almost 80% of my positions despite the ongoing coronavirus pandemic and the associated contact restrictions.

As of 31 December 2022, I have a total of 301 staff in my authority. I had a total of only seven staff departures in the reporting year 2022. At the same time, I was pleased to welcome 33 new staff members, who now strengthen my organisation as junior staff or experienced employees. In addition, I expect a further 18 staff to be recruited from application procedures already completed in 2022.

My authority offers interesting career prospects and varied fields of activity. The tasks are complex and often have an international connection. As a personnel development measure, I offered a promotion procedure from the higher to the higher non-technical administrative service for the first time. After a successful selection process, this will enable students to study at the Federal University (HS Bund) from 1 May 2023.

In 2022, I again gave seven students, eleven trainees and seven aspiring candidates the opportunity to complete their training days in my authority. Thus, even during the pandemic, I was able to support many junior staff in their entry into professional life.

My agency places particular emphasis on developing and updating the knowledge and skills of its employees. To this end, I offer my staff an extensive range of training opportunities to strengthen both their professional expertise and soft skills. With the easing of the pandemic, we were again increasingly able to hold events in presence or off the premises. We continued offering many webinars at the same time.

It is also important to me to promote the compatibility of work and family. Among other things, my authority offers very flexible working hours and extensive opportunities for mobile working.

Recruiting new staff is one of my priorities. I am very aware of the shortage of skilled workers throughout Germany and the stiff competition for good applicants, especially in the technical field. I was all the more pleased that participation in career fairs was possible again. In August 2022, I was able to present my authority at the faculty day of the HS Bund, and in October and November 2022 at career fairs in Bonn and Aachen.

In the reporting year 2022, I conducted 42 staffing procedures (both individual and collective). I received a total of 326 applications. Of these, 240 applicants were invited for interviews, which were conducted both with the help of modern in-house video conferencing technology and in person. I was able to offer employment to 45 people.

## 10.5 Growing – the BfDI liaison office in Berlin

**The size and concept of the current BfDI liaison office in Berlin still reflect the needs of 2008. Just as the Bonn headquarters of my office has grown as a result of additional tasks and staff, my capital representation will now also have to develop further. The basis for this has been laid with the lease of a new, larger and more versatile property, which is expected to be ready for occupation in the fourth quarter of 2023.**

Bonn is the historical and, since 2018, also the legal seat of the BfDI. However, this is not possible without a local representative office in the federal capital. For this reason and in view of the physical distance, a Berlin liaison office existed even before my term of office to support my authority in its parliamentary and departmental advisory tasks at the seat of the Bundestag, Bundesrat and federal government. In addition to general political life in Berlin, participation in other political, economic, scientific and social discourses around data protection and freedom of information also requires adequate local representation. The current Berlin liaison office has not yet grown structurally and conceptually with the head office and its tasks and organisational units. The premises rented in Friedrichstraße have long been too small for proper representation of all my organisational units. After a needs assessment by the Federal Ministry of Finance, a joint market survey with the Federal Real Estate Agency and clarification of the conditions for conversion and leasing, I am now looking forward to moving into a new property on Spittelmarkt, probably in the fourth quarter of 2023.

In the long term, the new Berlin liaison office will provide enough space for each of my units to be represented by one staff member in Berlin. Due to a lack of space, only specific units have been represented in Berlin so far. In addition, Berlin will have modern, flexible meeting and conference rooms that can also be used for smaller events, equipped with modern presentation, sound and video technology.

## 10.6 Press and public relations report

**In the year under review, the public relations work of my authority focused in particular on individual topics from the areas of health and social media. Our success with Mastodon in the Fediverse is certainly linked to this. The publications I offer continue to be in high demand. That is why the Pixi books for children not only had a second edition of the first series this year, but also a new part of the series. In addition, interested citizens can increasingly participate in hybrid events organised by my authority.**

**Public relations**

In spring 2022, there were many public discussions on the possible introduction of a vaccination register. Accordingly, my press office received many enquiries about this during the reporting period. I repeatedly emphasised that a vaccination register would in principle be conceivable in terms of data protection law if the corresponding legal prerequisites were created. This would have included, above all, the definition of a purpose for the creation of the register. The plans have not yet been implemented. Another project in the field of health also led to many enquiries: the e-prescription. Here, it was especially the trade press that asked for information on how the individual transfer channels and the e-prescription as a whole were to be evaluated in terms of data protection law.

The second area of high media interest was related to the use of social media. In the reporting period, for example, I initiated a hearing procedure on the issue of Facebook fan pages against the Federal Press Office, which led to many press enquiries.

With the takeover of the short message service Twitter by Elon Musk in October 2022 and the associated changes, media interest in alternative platforms from the Fediverse also increased. The server of my authority, which runs an instance of the decentralised short message service Mastodon (https://social.bund.de) and the accounts represented on it experienced a high level of traffic in October and November 2022, both from "followers" and from federal authorities and institutions close to the federal government, who themselves became active there with an account. My press office received very many enquiries dealing with the complex as a whole.

In the reporting period, I issued 13 press releases – in addition to short reports and publications – and was a guest at the Federal Press Conference once. As chair of the Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK), I have also issued eight press releases on behalf of the DSK. I have written six guest articles or essays for various media. My press office answered 413 enquiries by mail and 406 by telephone.

**Social media**

In April 2021, I started running an instance of the decentralised short messaging service Mastodon myself. What was originally intended to prove that social media could be implemented in a privacy-friendly way grew more and more from a niche offering to a serious alternative.

As of 31 December 2022, the account of my authority (https://social.bund.de/@bfdi) is now followed by more than 40,000 interested citizens. In addition, accounts from more than 40 other authorities and institutions can be found on our server, including numerous federal ministries.

**The BfDI Mastodon account can be found here:**

(Scan QR-Code or click)

My staff, who also look after the Mastodon account, always try to be approachable and use it to answer as many questions as possible in an uncomplicated way. I personally also contribute to the discussion time and again, because I see great added value in the direct exchange with citizens on the topics I deal with. I would like to expand this work in the future.

Furthermore, I would like to see the federal government build its own capacity in the area of privacy-friendly social media and also support it financially. Despite my request to centrally host the federal instance, the ITZBund has so far not seen itself in a position to fulfil this task, which actually falls within its area of responsibility. However, because I believe it is important that the supreme federal authorities in particular should set a good example and use legally compliant social media, I will continue to try to offer my services with the limited resources at my disposal, which is a great challenge in view of moderation tasks and the technical safeguarding of a communication channel for a large number of authorities.

**Website innovations**

A key innovation of my website concerns accessibility for people with impairments. Thus, a total of three videos in sign language and three articles in easy language

are now available. These explain my tasks and how the website works.

During the reporting year, I also started to redesign my flyers. All newly published, printed flyers receive a digital, expanded counterpart on my website. Readers can access these via a QR code. On the website, all interested parties will then find further information, in particular also links to related articles. The printed version, on the other hand, is better able than in the past to inform citizens about the basic points and give them an overview. I will strive to continue this dovetailing of analogue with digital in all future flyers.

**Information material**

This digital linking of the information I provide with and as a supplement to print media enables me to guarantee the topicality of our information even better. Interested readers can independently display the topics relevant to them and at the same time are offered references to further topics.

With regard to the target group, the main focus in the further development of the provided information in 2022 was clearly on nursery school children, primary school pupils and the introductory classes of secondary schools. As before, early consultation and sensitisation accompanying digitalisation is an important part of my work. The continuing high demand and very positive response to our first two Pixi books shows that the topic of data protection has reached children, young people, parents and teachers. In order to make the contents of both books accessible to anyone interested at any time, I have also had the books converted into videos. Regardless of this, the demand for print copies was so high that I had to publish a second edition just six months after publication. The first edition had to be reprinted.

In order to explain my second big task – freedom of information – to children and adults, I have created a second series of "Daten-Füchse" (Data Foxes) with Carlsen Verlag. The Pixi Wissen series "What is Freedom of Information?" has been available for schoolchildren since December 2022. At the same time, the Pixi book "Aber warum?" (But why?!) on the topic of transparency was published for kindergarten children.

As in 2021, the order button was flashing permanently. We received more than 27,000 orders in the first two weeks alone. These two books will again be converted into videos in order to be able to offer the information limitlessly, regardless of the availability of print copies.

I published a flyer for parents on the occasion of World Children's Day on 20 September 2022. It addresses twelve questions and makes recommendations for parents on how to deal with smartphones, social media, games and more. In order to make the flyer accessible to a broad target group, I offer it in German and in English. This flyer is closely linked to further information in our digital offer.

**Events**

More events could be held again during the reporting period, sometimes still under strict hygiene regulations. Therefore, all events organised by my authority itself were offered in hybrid form. In the future, I will also try to offer a live stream wherever possible and the later retrieval of a recording of the event for interested citizens.

The "Bonn Days of Democracy" took place in May. For the kick-off event, I organised a panel discussion on the question "What citizens are allowed to know" on the topic of transparency and free access to information.

In September, I had the pleasure of hosting my colleagues from the data protection supervisory authorities of the other G7 nations for the Data Protection Roundtable 2022 in Bonn in context of the official G7 events.

Also in September, I participated for the first time in the World Children's Day event in Cologne. The wet weather did not stop the children and parents from visiting our stand and taking part in our quiz. I was very happy about the great enthusiasm of the little ones as well as the interest of the adults. I also want to take part in such events in the future.

In October, I organised a political forum entitled "My car! My data?", which met with a positive response and is intended to mark the start of a series of similar events in Berlin's political heart.

In November, I organised a full-day symposium entitled "Research with health data – challenges in light of the General Data Protection Regulation". The format was primarily aimed at a professional audience and was also very well received. Again, I plan to continue the series next year.

However, one of the main focuses of this year's event management was certainly on the total of ten events of the Data Protection Conference (DSK) – some of which lasted several days – which I organised as this year's chair. In addition to the closed events, I also sent out invitations to public events on the eves of the 103rd and 104th DSK in Bonn respectively. I am convinced that these formats are not only a good introduction to our work, but also provide important suggestions and impulses for future consultations.

It is my declared goal that my authority continues to remain close to all interested parties through such and similar events and that contact with citizens is thus maintained.

**Visitor groups**

This reporting period was also still strongly influenced by the restrictions of the coronavirus pandemic. The official visitor group programme of the Federal Press Office was suspended until May 2022. Nevertheless, I received and looked after five groups of visitors with up to 50 participants in the Bonn property and one in the Berlin liaison office.

**Data protection garden**

After my office moved to the property on Graurheindorfer Straße in Bonn, the green spaces were redesigned by a horticultural company to be insect-friendly. Bees in particular should now find food in the approximately 800 $m^2$ facility over a long period of the year. At the same time, an information path was created with details on the topics of data protection and freedom of information. A total of six information boards are distributed in the data protection garden. The garden and seating areas are open to the public. Information on the data protection path can also be accessed online.

**Cross-references:**

3.4 G7 Roundtable, 4.1.1 Symposium on Research with Health Data, 4.3.1 Facebook fan pages proceedings, 8.1 News from the telematics infrastructure and its applications, 8.10 Digital data spaces and mobility data in the transport sector, 10.7 Well networked: The BfDI team in the capital

## 10.7 Well networked: The BfDI team in the capital

**In my last Activity Report, I reported on the establishment of my capital city team (cf. 30th AR No. 9.4). In the meantime, it has established itself as an important interface between my agency and the political arena.**

My statutory duties include advising the Bundestag and Bundesrat, the federal government and other institutions and bodies on legislative and administrative measures to protect the rights and freedoms of natural persons with regard to the processing of personal data. In addition to participating in the discourse on data protection law and policy, I also have to follow relevant developments of a technical, scientific, social and economic nature and raise public awareness of risks.

In order to be able to fulfil these tasks efficiently and to take into account the dynamics and complexity of political processes in the federal capital, which are characterised by a multitude of stakeholders and influencing factors, I formed a small capital city team of three people in my Berlin liaison office in 2021. Linked to the management area, it coordinates and bundles, among other things, the political work and correspondence of my authority, monitors developments, ensures information flows and maintains a mutual exchange with all relevant stakeholders.

The well-networked colleagues succeeded in improving information flows and relieving the technical level of my institution. Moreover, the political-parliamentary sphere has gained permanent contact persons through my capital city team, who, in accordance with the service mandate of my authority, are available centrally and, if necessary, at short notice.

The various information and exchange formats for the parliamentary sector have also become well established: The regular parliamentary letter for MPs and their staff, published at least quarterly, is well received. It provides information on current political issues relating to data protection and freedom of information in a condensed form geared to the target group and is publicly available (www.bfdi.bund.de/parlamentsbrief).

**All parliamentary letters can be found here:**

(Scan QR-Code or click)

The workshop on the basics of data protection, which was offered several times at the beginning of the legislature, was also very popular. It was aimed specifically at new members and staff of the Bundestag and is intended to raise awareness of data protection issues. I will continue to offer it regularly. The same applies for the specialist workshops on selected, politically significant data protection issues.

The launch of my Political Forum in Berlin on the topic of “My Car! My data?” was equally successful, so I am planning regular continuation events here as well.

Overall, the capital team has improved political communication with my authority. I also appreciate the current efforts of the German Bundestag to change its procedural rules in this context. In future, I should always be called in for expert hearings when the committees are dealing with projects that significantly affect the

protection of personal data and the presence of at least a quarter of the committee members is required.

**Cross-references:**

8.10 Digital data spaces and mobility data in the transport sector

## 10.8 Secure communication with the public authority mailbox

**Secure transmission channels for the delivery of electronic documents are particularly important in the context of the digitalisation of the administration. As part of its exemplary and pioneering role, my department already opened access to this via a so-called special electronic public authority mailbox in September 2020.**

If properly implemented, the digitalisation of administration can have many benefits for both citizens and public authorities. It can be more effective, user-friendly and secure than traditional analogue administrative processes. For my office as the federal data protection supervisory authority, it has always been particularly important to take a pioneering role in the digitalisation of the administration itself and to implement it in a data protection-compliant manner. For example, paper files were transferred to electronic document management at an early stage, which – with a few exceptions, such as in the area of certain classified documents – led to fully electronic file management years ago. This made the everyday work of the employees largely paperless. Combined with the necessary IT infrastructure and modern possibilities for mobile working, it was therefore possible to maintain the operations of my authority without any problems, even during the pandemic.

But when digitising the administration, it is not only important to make internal file processing digital and secure, but also communication with other offices. Supervised bodies and citizens have always been able to reach my office digitally via input forms on my website and by electronic mail and, in addition to a DE-Mail mailbox, also by conventional email. The corresponding PGP keys for encrypted email communication, among other things, are stored on my home page.

Data-Protection-Garden at the Bonn office of the BfDI

Since 1 January 2022, public authorities and legal persons under public law have been obliged to participate in so-called electronic legal transactions (ERV) and to use certain secure transmission channels for the delivery of electronic documents for this purpose. The judiciary recommends the use of the so-called "special electronic public authority mailbox" (beBPo) for this purpose. In fact, my department had set up the beBPo long before, i.e., as early as September 2020, thus opening up access to electronic documents via a secure transmission channel for other departments as well.

My department has opened three channels of communication with regard to the ERV:

- BfDI – Mailroom – The Federal Commissioner for Data Protection and Freedom of Information
- BfDI – Legal – The Federal Commissioner for Data Protection and Freedom of Information
- BfDI – Unit Z 1 (Personnel) – The Federal Commissioner for Data Protection and Freedom of Information

This means that communication with courts can take place directly with our legal department and a separate channel has also been set up for personnel matters in the particularly sensitive area of personnel administration. For all other cases, my office can be reached via the beBPo channel of the mailroom. With this, the beBPo can also be used as a secure transmission channel by other participants of the ERV in the context of other official communication. This concerns, for example, other authorities, health insurance funds and lawyers, who can and should, among other things, also gladly contact my office via the beBPo for requests for advice or supervisory procedures.

As the federal data protection authority, I will continue to work towards a citizen-friendly, fundamental rights-compliant and secure digitalisation of the administration, including within the internal administrative projects of my own department. The history of my own early implemented digitalisation projects should make it sufficiently clear that the Federal Data Protection Agency is not a brake on digitalisation, but a pioneer of a digital and secure administration.

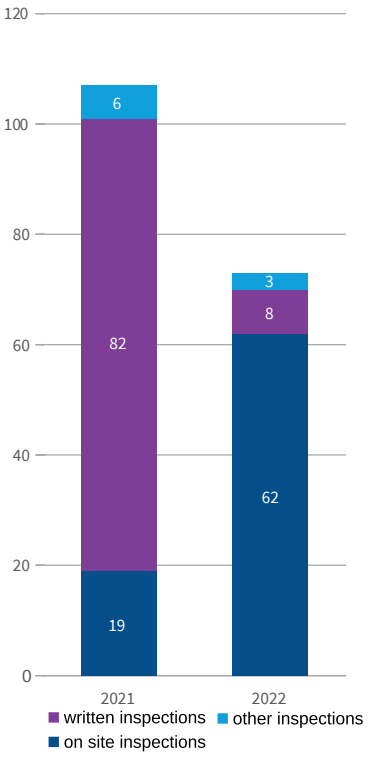
## 10.9 Statistics 2022

**In addition to the substantive insights presented in the many preceding posts, the statistics also provide a revealing look at the work of my agency. For the year under review, among other things, some trends can be identified that are associated with the waning of the coronavirus pandemic.**

### Consultation and inspection

As a supervisory authority, consultations and inspections are important areas of work that sometimes depend heavily on personal contact with the responsible bodies. Against this backdrop, it is gratifying that my staff were again able to carry out supervisory activities to a greater extent at on-site appointments during the course of the year. In particular, it was possible to make up for outstanding mandatory inspections at security authorities. These on-site inspections are usually much more extensive in terms of content as well as time and address more complex issues than written inspections, which are often used to get an overview of certain issues in an industry or a group of authorities. This explains why the total number of inspections carried out decreased compared to the previous year, while the number of on-the-spot checks more than tripled.

Controls within the framework of supervisory activities



In view of the strategic orientation of my authority as a provider of advice, it is also gratifying that the number of consulting appointments with supervised entities has risen sharply. Specific issues and data protection-friendly solutions are discussed at these meetings. Often, the issues are brought to my attention by the supervised bodies.

**Enquiries, complaints and reports on data protection violations**

In the reporting year, citizens addressed a total of 6,619 complaints and enquiries to me. I also provided telephone advice to 6,374 people. This roughly corresponds to the figures of previous years, although a slight downward trend can be observed. After the many complaints when the GDPR was introduced and the enquiries around data processing in relation to combatting the pandemic, the need for advice from citizens seems to have declined somewhat. I also attribute this to the intensive counselling, e.g., at job centres and tax offices, which has led to an improvement in processing procedures and thus to fewer complaints.

On the other hand, I observed a slight increase in the number of incoming reports of data protection violations. I received 10,658 reports during the reporting year.

| Complaints and enquiries | 2020 | 2021 | 2022 |
|---|---|---|---|
| General enquiries | 4.897 | 4.329 | 4.434 |
| Complaints re. Art. 77 GDPR | 2.861 | 2.383 | 2.115 |
| Complaints re. Art. 80 GDPR | 25 | 19 | 3 |
| Complaints re. Section 60 BDSG (Federal Data Protection Act) | 56 | 54 | 29 |
| Submissions against intelligence services | 39 | 44 | 38 |

| Reports of data protection violations | 2020 | 2021 | 2022 |
|---|---|---|---|
| Notifications pursuant to Art. 33 GDPR | 9,987 | 10,106 | 10,614 |
| Notifications pursuant to Section 169 TKG (Telecommunications Act) | 37 | 51 | 44 |

**Formal monitoring of legislative projects**

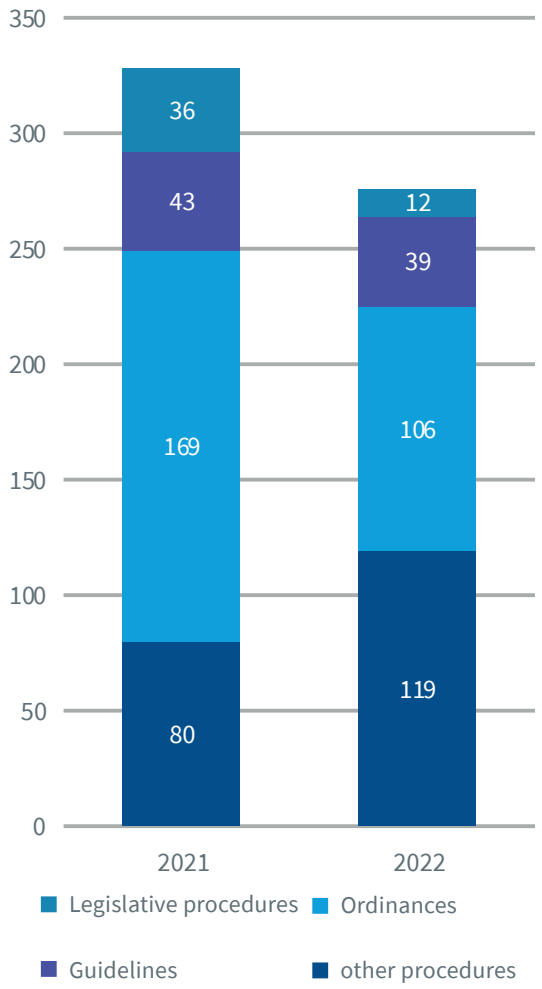
Pursuant to Section 21 of the Joint Rules of Procedure of the Federal Ministries (GGO), the lead ministries must involve me at an early stage in the drafting of bills insofar as they affect my responsibilities. As explained in several places in this report, this unfortunately does not always go smoothly. However, I was involved in formal legislative procedures more often overall; the increase was almost 50 per cent compared to the previous year. For ordinances, on the other hand, the number fell, which probably also has to do with the fact that in the first year after a change of government, the legal basis for planned ordinances could not yet be created, so that an increase is to be expected here in 2023.

In addition to the 276 participations under Section 21 GGO listed in the chart, I examined 99 file orders as well as 6 EU legal acts and commented on 12 proceedings of the Federal Constitutional Court. I was also able to contribute as an expert to 5 hearings of committees of the German Bundestag.

**Cross-references:**

6.6 Statistical evaluations for the IFG (Freedom of Information Act) for 2022

**Participations according to § 21 GGO**



# 11 Single Contact Point

The Single Contact Point (ZASt) coordinates the cross-border cooperation of the federal and state data protection supervisory authorities with the other Member States of the European Union, the European Data Protection Board (EDPB) and the European Commission.

In the federal system, which is unique in Europe, it enables the supervisory authorities of the EU Member States, the European Data Protection Board and the European Commission to communicate and cooperate with the German data protection supervisory authorities without knowledge of the German distribution of competences.

Although it is located at the Federal Commissioner for Data Protection and Freedom of Information (BfDI), the ZASt is organisationally separate from the BfDI. This organisational separation is intended to counteract any conflicts of interest and ensure that the federal and state data protection supervisory authorities are treated equally in the flow of information to and from Europe.

The tasks of the ZASt are limited to supporting the federal and state data protection supervisory authorities in their tasks without performing data protection supervisory tasks themselves.

## 11.1 ZASt review

**The settlement of cross-border complaints procedures in European administrative cooperation is gaining momentum. However, some developments appear more complex than the figures initially suggest. In 2022, the Single Contact Point (ZASt) was also active behind the scenes and played its part in improving cooperation.**

**Decline in appeals: increasing harmonisation in data protection enforcement**

Cooperation between supervisory authorities in cross-border cases is increasingly consensual. The supervisory authorities increasingly exchange information with each other, even at early stages of the procedure when all decision-making options are still open. This is a result of an informal meeting of the heads of the European supervisory authorities at the end of April 2022 in Vienna with the aim of improving cooperation.

Although it remains to be seen whether this development will continue, its first effects are already measurable. For example, the number of appeals lodged by supervisory authorities against decisions of their European counterparts is in sharp decline. The objective of the GDPR to create a harmonised, high level of data protection is thus increasingly being achieved. Many of the initially very contentious procedural questions of principle have been clarified and the European supervisory authorities are increasingly turning to the important substantive questions. The consensual approach is also in the interest of all parties involved, because a decision can be reached more quickly in this way.

The following chart shows this development on the basis of the draft decisions submitted and the appeals lodged against them. The number of submitted draft decisions is shown to be plateauing.

Amicable settlements are excepted; more on this in the following section.

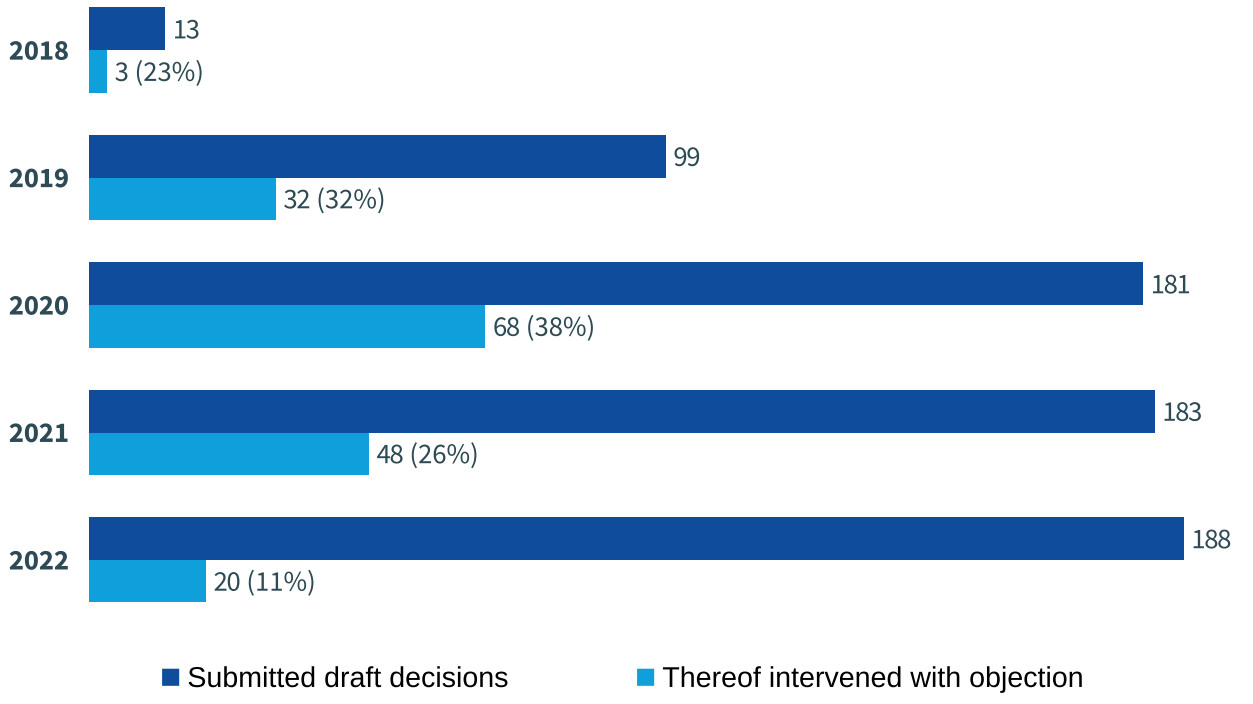
**More procedural closures equal more data protection? Unfortunately, not always.**

In the procedure pursuant to Art. 60 GDPR, the lead and the affected data subject supervisory authorities are in principle meant to agree on the manner in which a specific matter is concluded in trusting, constructive cooperation.

In the 2022 reporting period, 135 draft decisions are shown for Germany and 172 for Ireland. 160 Irish draft decisions alone were compiled in the period from June 2022 to the end of December. How can this significant increase in such a short time be explained?

In June 2022, the 66th EDPB plenary meeting adopted Guideline 06/2022. According to this, supervisory authorities that amicably settle complaint cases under their

**Draft decisions & appeals since applicability of the GDPR on 25 May 2018**




national procedural law should send a draft decision "sui generis" to the other supervisory authorities concerned in advance in each individual case.

The procedural decisions are not negotiated between the supervisory authorities involved, but solely between the lead supervisory authority, the controller and the data subjects. In this context, the queried data processing is not further clarified by the authorities. The possibilities of other affected supervisory authorities to take action against such a draft decision that ends the proceedings and to enforce a more intensive or different legal examination and assessment are greatly reduced.

It is to the credit of Guideline 06/2022 that this method of terminating proceedings, which is practised to an extremely varying extent, has now been made visible. The instrument of amicable settlements itself, on the other hand, can be viewed from different perspectives. On the one hand, it enables a large number of usually simple and often also similar individual cases to be concluded in a short time with the involvement of complainants and responsible bodies. On the other hand, with these draft decisions, there is an extremely limited possibility for the supervisory authorities concerned to become aware of the legal considerations of the lead supervisory authority. For this reason, which makes matters more difficult for procedural reasons, the possibility of influencing supervisory measures and a legal review of the lead supervisory authority's assessment by the EDPB is extremely limited.

It is now necessary to further observe what effects this way of working has on the cooperation mechanism, which is designed for transparent exchange between the supervisory authorities. As part of its strategy development, the EDPB has also suggested to the EU Commission that this practically important form of procedure termination should be outlined in greater detail in the law in the context of a "wish list".

**Training provision through the ZASt for the Internal Market Information System IMI**

Due to the cross-border case processing in the Internal Market Information System IMI provided by the European Commission, the German supervisory authorities have reported considerable need for training in practical work with this central IT system to the ZASt, even four and a half years after the GDPR came into force.

Following on from the introductory training provided by the EDPB Secretariat and the European Commission in 2018, and most recently at the beginning of 2020, the ZASt has therefore developed a training concept on its own. Building on this, employees from almost all German supervisory authorities were trained in the use of IMI in autumn 2022. In a basic training course in October 2022, the necessary basic knowledge for handling

cross-border cases in IMI was first imparted and then deepened in practical exercise units. In this context, the meanwhile numerous elaborations of the EDPB and the formal and procedural guidelines for cross-border complaint handling were also taken into account.

An advanced workshop was held in November 2022. With the creation of this forum by the ZASt, the experts of the German supervisory authorities were able to exchange information on particularly difficult cases in matters of IMI application. The result was best practice recommendations for even better coordinated opinion-forming and European cooperation as well as tactical and strategic approaches for successfully introducing the German position into the European discourse. In the future, these are to be introduced into the responsible working groups of the DSK and, if necessary, the responsible expert subgroups of the EDPB.

**IMI intruction by the ZASt**

# 12 Where is the positive?

As already described in the introduction and in some previous contributions, there are an increasing number of positive developments resulting from my consultancy and monitoring activities. Since my staff always tries to point out data protection-friendly alternatives in the discussions, we feel strengthened in our advisory approach and are pleased that this is increasingly reflected in the data processing of the supervised entities. As in the last Activity Report, I will present a few highlights of such positive cooperation.

## 12.1 Data protection organisation at DRV Bund

**The German pension insurance company DRV Bund has revised its data protection organisation and thus strengthened the independence of the official data protection officer.**

DRV Bund has undertaken a fundamental reorganisation of data protection and created a separate staff unit for the official data protection officer, which reports directly to the Directorate. Compared to the previous structure, this has resulted in an even clearer separation between the tasks of the DPO on the one hand and operational (administrative) data protection on the other. When appointing a data protection officer pursuant to Article 38(6) of the GDPR, the obligation to ensure that other assigned tasks cannot bring the data protection officer into a conflict of interest and thus jeopardise his/her independent position was implemented by the DRV Bund to the extent required. I closely advised DRV Bund during the restructuring process and welcome the reorganisation that has taken place.

## 12.2 Data protection aspects of telemedia services

**Little strokes fell big oaks. Very slowly, but nevertheless noticeably, awareness of data protection issues in telemedia services is increasing among federal public agencies.**

In this reporting year, I observed a growing sensitisation and awareness amongst authorities with regard to the problems of data protection law in the use of telemedia services. This has been particularly evident in the increasing consultations on and heightened interest in this subject from various authorities.

The focus was on three topics: cookies and cookie banners, the integration of videos on the home pages of the federal authorities and the operation of Facebook fan pages.

The data protection-compliant design of cookie banners as well as the legal basis, for example for range measurement, pose challenges to almost all responsible bodies time and again. In addition to several individual consultations, I therefore presented questions on cookie banners in particular within the framework of the exchange of experiences with the official Data Protection Commissioners of the supreme federal authorities and made recommendations. In this context, I also specifically updated some information texts and FAQs on my website.[73]

In addition, the DSK's "Guidelines on Telemedia", which are very important for many telemedia providers, were intensively revised in the DSK's Media Working Group and adapted to the new legal requirements of the TTDSG (Telecommunications Telemedia Data Protection Act). Legislators have wanted to create regulations on recognised consent management services for some time. Clear, balanced regulations could strengthen the privacy of users and curb cookie banners. However, no practical and lawful solution is yet in sight.

73 Information offered on my website, available at: https://www.bfdi.bund.de/DE/Buerger/Privatwirtschaft/Telemedien/Telemedien_node.html

Unfortunately, the federal government's public agencies still almost exclusively use YouTube to integrate videos on their home pages. The controllers are often aware of the data protection issues, but usually ignore these in favour of needs such as reach measurement. The Federal Ministry of the Interior and Home Affairs is exemplary in this respect: with the help of my consultations, it has begun to integrate videos on its home page not through YouTube, but exclusively locally.

Federal public agencies continue to operate Facebook fan pages despite years of awareness-raising and significant data protection concerns, so I have now had to take supervisory action.

In principle, it should be noted that new offers are often initially problematic in terms of data protection law because they tend to be created using prefabricated modular systems, which often use unnecessary cookies and integrate external services. Only when approached do they quickly redesign them instead of avoiding the problematic parts from the beginning.

**I recommend reviewing the integration of videos on federal websites and implementing data protection-compliant alternatives to the widespread practice of integration via YouTube.**

Cross-references:

4.3.1 Facebook fan page procedure; 5.5 Consent management services

## 12.3 Alternative provision of federal apps

**Public sector apps should also be offered outside the app stores of the operating system manufacturers.**

In my consultations with the authorities on the development of apps, I have always worked in recent years to ensure that the apps developed can also be obtained from alternative trustworthy sources. Unfortunately, I found that not all authorities followed my recommendations. Therefore, I informed the supreme authorities about the data protection assessment by means of a circular dated 22 June 2022 and called on them to act. In terms of data protection law, the body responsible for the app makes a decision on the distribution channel through which the product is offered. If an app is only made available via the app stores of the operating system manufacturers, citizens who want to use these apps must submit to the processes of these companies (third parties), which currently make it mandatory to set up an account. The terms and conditions of the store providers must also be accepted. The provision of the apps via these distribution channels thus includes a processing of personal data that is not necessary for this purpose.

Some tech-savvy people have deliberately installed free operating systems on their mobile devices. These people do not have accounts with the operating system manufacturers. In terms of the open government aspect, however, the app should also be made available for this (still small) group of people. Article 6(4) of the Digital Markets Act already provides for a mandatory opening of the stores. However, it will still take some time until the market is liberated, so that the provision of the apps on the authorities' own websites, which is recommended now, is a transitional solution.

One authority was already able to give me feedback very promptly that its entire app portfolio is available via its own website. I was particularly pleased that the Federal Ministry of the Interior and Home Affairs is already examining the extent to which federal apps can be made available via a uniform federal service. No decision has been made yet, but the first feedback already shows that good data protection solutions can be created with a few small targeted steps.

## 12.4 Consultation and professional exchange on the SÜG (Security Clearance Act) – A fruitful addition

**Proactive consultation and professional exchange with a wide range of practitioners is essential to ensure and implement a high level of data protection in the area of security clearance. For this reason, I focused on consultation and professional exchange in this reporting year. This was very positively received by all participants. In my estimation, there is a very high awareness of data protection, especially among commercial enterprises.**

In addition to my monitoring activities in the area of the Security Clearance Act (SÜG), I attach great importance to counselling. Not only is every inspection carried out in conjunction with an advisory service, but I also take a proactive approach to advisory tasks. The aim is to ensure compliance with data protection regulations in the processing of personal data not only by the inspected bodies, but also by providing comprehensive advice and information to all bodies in advance. Compliance with data protection regulations and thus the protection of informational self-determination can be achieved most effectively through this approach.

To this end, I pursue three different approaches in addition to tailored counselling of individual agencies. This is firstly the expert dialogue with specialist application providers, secondly the exchange with working groups or interest groups and thirdly the provision of working aids.

The processing of personal data in security clearance is becoming increasingly digitalised, resulting in the introduction of various electronic specialist applications. One provider of such a specialist application took up my offer of advice. This developed into a constructive technical dialogue for both sides. In the course of the consultation, the specialised application provider optimised its software in order to adapt it to the respective data protection requirements of the SÜG. This gave me a better understanding of the specialist application and the practical work with it. Since the specialised application is used by many monitored bodies, I was able to increase the efficiency of my inspections on the one hand, and on the other hand, the respective users of the specialised application have the certainty that they are using software that complies with the data protection requirements of the SÜG.

I also repeatedly exchanged views with a working group whose members are responsible for implementing the SÜG in commercial enterprises. Here, I was not only able to place my concerns, but in particular to learn from practice what problems exist in the application of the law. The constant exchange with users of the SÜG shows me which problems arise in the application of the SÜG and, in particular, which data protection challenges need to be solved. In addition to my monitoring activities, the professional exchange enables me to make recommendations on how the SÜG should be further developed (30th AR, No. 6.20).

My findings from the inspections, the professional exchange as well as feedback from the practice flowed into various working aids, among other things. In this reporting year, I published working aids on the data protection requirements for managing security files in the security clearance procedure and on the data protection requirements for processing personal data from the security clearance in files. The working aid for managing security files is aimed at the respective responsible persons in the competent public and non-public bodies. With numerous examples and data protection-related tips for practice, they will be enabled to manage security files in analogue or digital form in compliance with data protection. This is supplemented by the work aid on automated files that may be kept alongside security files. My focus here is on outlining the differences between public and non-public bodies. The legislator provides for considerable differences here.

The working aids enable a large number of users of the SÜG to evaluate their own processes and adapt them to the data protection requirements. They are to be continuously developed and supplemented with further topics from practice.74

Furthermore, I sent a circular to the security officers of the supreme federal authorities on the disclosure of information from the Federal Central Register as well as on the encryption of emails. These circulars are also published on my home page, as are several of my inspection reports, which can be referred to by the responsible bodies when reviewing their own processes.75

The different advisory approaches and the associated exchange with the various stakeholders who either process personal data themselves within the scope of the SÜG or offer products or services for the responsible bodies have borne fruit. I am pleased to see that there is a great awareness of data protection in the area of security clearance law. This is especially true for business enterprises. It should be positively emphasised that adjustments and optimisations are also being made outside of inspections in order to process personal data in a data protection-compliant manner in the future.

In the future, I will continue to invite all stakeholders to contact me with requests for advice in order to achieve a data protection-compliant design of the corresponding processes from the very beginning. Especially uncertainties, e.g., with regard to switching to electronic applications, can be eliminated most easily in this way. In 2023, I will further expand the consultation and professional exchange. For example, I will hold an event on this at the Federal Academy of Public Administration.

## 12.5 Protocol evaluation tool for Inzoll

**During an inspection of the Customs Investigation Service information system INZOLL, I identified possibilities for improvement in the design of the logging system. At my request, the Customs Criminal Investigation Office (ZKA) has begun to expand the logging system with an evaluation tool in order to better guarantee data protection controls in the future.**

In my last Activity Report, I reported on my inspection of the queries in the information system of the Customs Investigation Service (INZOLL) (cf. 30th AR No. 8.1.4). I also inspected the logging system. Due to the pandemic, however, I had initially excluded detailed technical and

content-related questions regarding logging in INZOLL from my evaluation, as an on-site appointment with the system support unit was planned for this purpose. This was carried out in February 2022.

I had identified weaknesses in the logging system beforehand. In particular, an evaluation tool that enables the display and searchability of log data directly on site was not available for my inspection. The evaluation of the queries had to be commissioned from the system administration unit, which involved a lot of manual work. Also, the result of the evaluation was hardly readable, as queries were only issued in the form of complex, technical database commands.

This type of protocol evaluation is not sufficient. Log data should provide information about who (or what) processed which personal data, when and in what way. It must be ensured that the log data can be evaluated in a timely and practicable manner for the purposes of data protection monitoring, without the intervention of a third party. An appropriate evaluation tool for log data must be made available for this purpose. In addition, protocol data must also be comprehensible to technical laypersons.

Based on these requirements, I suggested improvements in logging in INZOLL. The ZKA complied with my demands immediately. It promptly developed an evaluation tool and at the same time discussed existing problems transparently in a constructive consultation. A considerable improvement in logging has thus already been achieved. An evaluation will take place during my next regular mandatory inspection.

## 12.6 Improvements to the BKA (Federal Criminal Police Office) case processing system (VBS)

**The Federal Ministry of the Interior and Home Affairs (BMI) has presented what I consider to be a successful concept for improving the purpose limitation in the case processing system (VBS) of the Federal Criminal Police Office (BKA). The BMI commissioned the BKA to implement this concept. I welcome that very much.**

I had objected to the BKA's case processing system in 2019. A major reason for the objection was that the VPS did not sufficiently distinguish between the different purposes for which the police authority processes personal data. Consequently, access rights and search options were also too broad. I also criticised the documentation of the lawfulness of police actions as incomplete (28th AR No. 6.7.3, 29. AR No. 9.5.3, 30. AR No. 8.2.2).

The BMI initially did not follow my legal position in essential aspects (29th AR No. 9.5.3). After a joint workshop in December 2021, in which I advised the BKA on how to deal with the problematic issues in connection with the VBS under data protection law, the BKA began to draw up concepts to further develop the VBS (30th AR No. 8.2.2).

The BKA presented a successful concept in another workshop in October 2022 to better separate personal data processed for different purposes in the VBS. This is to take into account the important data protection principle of purpose limitation with regard to personal data. It aims to implement my demands from the inspection report. The BMI informed me at the beginning of November that it had commissioned the BKA to implement the concept by decree. Even though I have criticised the slowness of the implementation of my demands, I still recognise the complexity of the undertaking (30th AR No. 8.2.2) and welcome the BKA's ambitious timetable of 14 months in which it intends to adapt the VBS.

## 12.7 Conceding on the Register of Foreigner Associations

**The Federal Office of Administration partially suspends the processing of personal data in the Register of Foreigner Associations.**

Foreigner associations and foreign associations can be banned if their purpose or their activity fulfils one of the criteria of Article 14(2) of the Associations Act and thus runs counter to the fundamental values of the Federal Republic of Germany.

According to the "Ordinance on the Implementation of the Law Governing Public Associations (Associations Act)" of 1966, they are subject to a special obligation to register and provide information. The required information also includes personal data, such as names and addresses of board members or persons authorised to represent them, as well as existing sub-organisations in the federal states. The association authorities of the federal states report the information to the Federal Office of Administration, which keeps the so-called Register of Foreigner Associations (AVR).

I have been pointing out to the Federal Office of Administration for some time that there is no sufficient legal basis for data processing in the AVR. Most recently, I initiated a corresponding prohibition order pursuant to Art. 58(2)(f) GDPR vis-à-vis the Federal Office of Administra-

tion. Now, both the Federal Office of Administration and the Federal Ministry of the Interior and Home Affairs, which is responsible for supervision, have informed me that no new notifications from the association authorities will be included in the AVR from 1 January 2023. Notifications concerning deletions from the register are excepted from this. I very much welcome these measures. However, I am currently examining whether they are sufficient to ensure data protection-compliant data processing in the AVR.

## 12.8 Postal service provider repositions itself in terms of data protection law

**In recent years, I became aware of various business processes of a large postal service provider that needed to be adapted in terms of data protection law. The remedial action taken by me in this context pursuant to Article 58(2) of the GDPR prompted the controller to question its business processes in the provision of postal services and to undergo far-reaching, fundamental revisions. Fortunately, this has led to a decrease in the number of complaints and data protection breach notifications regarding this company.**

Since 2020, complaints and information from citizens have increasingly revealed deficiencies and violations of data protection law in connection with the provision of postal services and the processing of data subjects' rights asserted in this regard. These reported deficiencies included, for example, delivery lists found in the open or in parked vehicles, legible to outsiders, or the photographing of mail recipients without their consent by delivery staff. Due to these data protection violations, such as the disclosure of personal data, the collection of personal data without a legal basis or the late and incomplete provision of information on personal data, I took remedial action pursuant to Article 58(2) of the GDPR by issuing warnings for the past and instructing the introduction of a continuous improvement process and a training concept for delivery staff.

My employees supervised the necessary reorganisation of the processes in conformity with data protection through additional counselling sessions, depending on the individual case. In addition, the postal services provider implemented far-reaching changes on its own initiative in favour of an awareness of data protection issues that permeates the entire company. This ensured that new processes or software, for example, were always considered from the perspective of data protection and checked for their suitability in this regard. As a result, the increased advisory approach led to the processes being adapted in a data protection-compliant manner, thus averting further measures pursuant to Article 58(2) of the GDPR in this context.

## 12.9 Consultation and supervision – achieving more for data protection together

**Data protection is complex and contentious at the same time. I experience this again and again in my advisory and supervisory practice. Some issues in data protection require judicial clarification. Often, however, my arguments were already sufficient in the year under review to persuade responsible bodies to provide good data protection.**

Data protection must reach people quickly and efficiently. Therefore, I am particularly pleased about cases in which my advice and recommendations are directly implemented. This was the case last year, for example, with the requirements for identification on the fault hotline of a telecommunications company. Many citizens had complained to me because they were asked for their bank details when they simply wanted to report a fault. After exchanging legal arguments, the responsible body changed its position and reorganised its processes in a data protection-friendly way. Citizens benefited from a quick solution in their interest.

Data protection supervision and responsible bodies are not opponents. Many companies in particular are sensitised, have recognised data protection as a competitive factor and have aligned their business processes accordingly. My inspection then confirms to them that this continuous work pays off in the end. This is because the need for expensive adjustments as a result of an inspection regularly does not arise in the first place. A positive example of this is the inspection and consultation at Emden Digital GmbH. This consultation and inspection visit also showed the advantage of an on-site appointment. All decision-makers were involved on site. Implementation options were discussed directly and I was able to give my implementation recommendations immediately.