ACTIVITY REPORT

PRIVACY

2020

The Hamburg representative for
Privacy and Freedom of Information

Hamburg

29. Activity report data protection of the Hamburg Commissioner for Privacy and Freedom of Information

2020

Published by
Hamburg Commissioner for Data Protection and Freedom of Information
Ludwig-Erhard-Strasse 22
20459 Hamburg

Tel. 040/428 54 40 40
Fax 040/428 54 40 00
mailbox@datenschutz.hamburg.de

Edition: 800 copies
Front page photo: Thomas Krenz

Layout & printing: Druckerei Siepmann GmbH, Hamburg

This print product has been awarded the Blue Angel.

You can access this activity report at
www.datenschutz-hamburg.de

---

presented in February 2021
Prof. Dr. Johannes Caspar
(editorial deadline: December 31, 2020)

TABLE OF CONTENTS

foreword

Personal data is in particular information, values, illustrations, dimensions, records, numbers, properties, all together information that relates to natural persons. Behind it are people, personal destinies.
You, me, the family, the children. People, their dignity and the protection of their personality are the reason that data protection exists. For this reason, independent bodies, the data protection authorities, have been set up in all European member states and in all federal states. These are completely independent of state authorities and are intended to support people, among other things, in enforcing their rights and freedoms to protect their privacy. To do this, they have a mandate to control government, administration and other public bodies, as well as all the many private bodies that process personal data for completely different purposes.

With this brief digression, I would like to start by drawing your attention to the central point to which our work has been devoted again in the past year: data protection is about guaranteeing one of the fundamental rights of people in the digital world. In view of the wide range of possibilities associated with data processing in the information age, it is hardly surprising that the question of the permissible use of personal data in society and the state is often a polarizing and controversial topic.

Especially in times of a pandemic, “data protection” is often (mis)understood as an obstacle in the public eye. It is often overlooked that the fundamental right to informational self-determination is by no means absolute even under pandemic conditions and is subject to considerable restrictions.
At the same time, even in times of a pandemic, privacy is a legal good that must be appropriately balanced with other fundamental rights and the general goal of health protection.

Against this background, the 2020 reporting year shows that almost all areas of society are affected by the corona pandemic and will probably remain so for a while.

But health protection and data protection do not go hand in hand rigid relationship of "either-or" to each other. In the rule of law, it is not a matter of generally subordinating one goal to the other, but of striving for appropriate solutions that enable a proportionate balance to be struck between conflicting fundamental rights positions based on individual considerations in the specific case. Following this principle is not easy, especially in difficult and challenging times associated with many restrictions and losses. It is entirely understandable that the greater the problems that have cut us off from our previous lives, the louder the call for seemingly simple solutions becomes louder. But it is also clear that a sense of proportion is part of the DNA of a functioning constitutional state and democracy, especially in difficult times.

In this activity report on the 2020 reporting year, the data protection aspects relating to the corona pandemic therefore occupy a large part. The usual main chapters such as inspections, reports, orders/fines and advice/data protection communication were preceded by a separate main chapter on the pandemic. The numerous different individual contributions in this new main chapter demonstrate the wide range of data protection legal issues associated with the corona pandemic.

In addition to this unexpectedly added main focus of work in 2020, other topics also have white

afterwards determines the work of the HmbBfDI in the reporting year. To pick just a few from the large amount: the fine imposed by the authorities on the company H&M in the amount of 35.3 million euros, the consequences of the Schrems II judgment of the European Court of Justice and the clearly emerging problems of a Europe-wide inconsistent and overly cumbersome law enforcement in cross-border data traffic.

The further increase in the number of complaints received from citizens has caused the workload at the HmbBfDI to increase sharply in recent years. This cannot and could not be compensated by the existing human resources of the HmbBfDI. As in previous years, there is still a clear need for improvement in the personnel situation.

Finally, a word on my own behalf: This activity report is the last that falls entirely within my term of office. After a total of twelve years, my job as Hamburg Commissioner for Data Protection and Freedom of Information ends in June 2021 at the end of the maximum second term of office provided for by the constitution.

Accompanying the digitization of society and state over this long period was both an exciting challenge and a rocky road. The many past discussions and consultations with people as well as private and public bodies, especially the interventions for the rights and freedoms of those affected and the commitment to a transparent rule of law have made me realize that it is important to recognize the tremendous dynamics of the development of digital Using technologies in the best possible way, but always accompanying them critically and not leaving them to their own devices. In times when data and information are the resources for economic power, social control but also democratic participation, it is not only worth asking critical questions – it is rather an imperative to ensure a humane future.

Twelve years ago, in 2009, I took up this post. From today's perspective, that was a different world: Barack Obama had just been elected US President, Ole von Beust was in power in Hamburg, and swine flu had been declared a pandemic. 2009 was also the year in which Google replaced its camera carriages for the Street View service with German

let cities and communities go. Every corner of the planet should

being filmed for mapping, which sparked a heated debate about the importance and limits of data protection.
Since then, the requirements and the view of data protection have changed radically. Much has been achieved, but new questions and problems have also arisen with great potential for intervention in rights and freedoms. The central goal of realizing data protection that enables digitization in the service of people has remained.

I would like to take this opportunity to sincerely thank all my employees for the great cooperation and for their outstanding achievements in the area of data protection and freedom of information over the years.

It was not always easy to do justice to the many tasks.
But I think it was worth it.

Prof. Dr. Johannes Caspar
February 2021

I. INTRODUCTION

INTRODUCTION

In the 2020 reporting year, the corona virus and its effects on the state and society raised significant questions and challenges, including for data protection. It shows once again: data protection is a cross-cutting issue that has entered all areas of everyday life. Although the pandemic is primarily a health policy issue, a wide variety of measures have been taken in recent months

Pandemic control affects the right to informational self-determination in different ways and raises fundamentally new questions in practice. This gives reason to focus on the corona pandemic in the 2020 activity report (see II. Corona pandemic).

With this 2020 activity report, the Hamburg Commissioner for Data Protection and Freedom of Information is taking the opportunity to sum up after 12 years in office, to look back on the past, to describe the focus of current work and to look ahead to the future. A

A key point is the substantive discussion of data protection problems in recent years. This is about the technical and economic changes in the age of digitization, which entail increasing potential for interference with the rights and freedoms of those affected, but also offer development opportunities for a modern society. It is also important to look at the procedural changes in the daily dealings with data processing by private and public bodies. The difficulties in obtaining modern and appropriate public authority equipment, meeting the many challenges of digitization, effectively protecting the right to informational self-determination and helping to provide advice on digital applications in state and society are unfortunately a worrying constant in recent years been.

The last 12 years of data protection in Hamburg – review, inventory and outlook

1. Data protection through the ages - By Google Street View to billions of face analyzes at Clearview and Co.

The handling of personal data has changed significantly in recent years. At the beginning of the 2000s, hardly anyone would have thought that the systematic collection and analysis of data by technology corporations would bring about a new dominance of companies whose capabilities had a hitherto unknown dimension of non-state power accumulation in terms of its social impact opened.

1.1 Google Street View - The future comes with camera cars

We were still a long way from these developments when Google from 2007 initially in the USA, but then also in Europe, equipped cars with panoramic cameras to take comprehensive street views and then make them available on the Internet ready. Today, more than 12 years later, it has almost been forgotten that the controversy at the time about data protection and privacy, which was sparked by photographs of houses and front yards as well as street views, was borne by mass public criticism. The debate about Google Street View in Germany largely followed the narrative of an invasion of the old world by a successful non-European digital company. This could be illustrated by legions of cars

with high camera structures that suddenly appeared and drove into towns and communities in order not only to acquire the views of people, cars, houses and properties without being asked, but also to make them available to everyone free of charge.

In this situation, compliance with national data protection laws was not only urged by data protection authorities, but also massively demanded by many people in the country. The call for privacy to Google's Street View project

scholl especially in rural areas. However, other voices also spoke up, vehemently in favor of digital distribution of the panorama views and asserting a right to information. If you like, the dispute over Google Street View was the first and at the same time the last battle of the analogue world with the powerfully emerging digital modern age, which, with the uncompromising, widespread use of technology, antagonized traditional values and opinion milieus .

The data protection authority in Hamburg, which is responsible for Google throughout Germany, safeguarded the rights of those affected by agreeing with Google on more extensive guidelines for the protection of privacy than the company was willing to meet globally. All people living in the 20 largest German cities had an extensive right to object, to which Google ultimately limited itself with the Street View service in Germany. In addition to the automated pixelation of faces and license plates, this enabled them to object to the publication of their home before Google Street View was launched and to demand that Google render it unrecognizable.

The tech group itself was responsible for the fact that the Street View project had nevertheless become an image disaster for Google: When the supervisory authorities asked, it came out that the cars used by Google were simultaneously accessing the contents of open, non-encrypted WLANs when driving stored on a hard drive that you took with you, this led to a storm of indignation and an immense loss of trust. Numerous regulatory

and investigations by public prosecutors were triggered worldwide. In the end, there was a fine of around 150,000 euros in Germany. This fine would undoubtedly have been higher today. The Federal Data Protection Act in force at the time only provided for fines of up to EUR 150,000 or EUR 300,000 for negligent or intentional acts. The idea of a unified

European data protection legislation, in which the level of fines

up to 4% of the annual turnover of a company worldwide was significantly strengthened by such scenarios.

1.2 New turning points for the protection of privacy

The data protection threats have changed and increased significantly since the days of Google Street View. Two turning points should be mentioned here: The Snowden revelations about mass surveillance by US and other friendly intelligence services in 2013 put the basic trust that prevailed among many people
en in democratic constitutional states in question. All of a sudden it became clear that the services of friendly states are also systematically investigating the entire area of global communication and are hoarding masses of data without transparent controls. While in previous years the criticism from data protection advocates had essentially focused on global tech corporations, with Edward Snowden it suddenly became clear that privacy is also being threatened by the state. Surveillance programs such as PRISM made it clear that the NSA is not limited to its own surveillance structures, but can also draw on the almost inexhaustible stock of data from global service providers such as Google and Facebook. The fact that these companies were also compensated by the state for their services documents how efficiently the network of secret service surveillance is set up.

Another turning point was the Facebook Cambridge Analytica scandal in 2018. It suddenly made it clear to the public that personal data opens up a tool for profiling that allows manipulation and control not only in the area of individual consumption, but also in to influence the will of the electorate and thus has an impact on the core area of democratic processes. For example, the company Cambridge Analytica evaluated masses of data from Facebook users in order to specifically influence voters in the US election campaign. The consequences of data power are no longer just related to the privacy of the individual, whose profile is a personalized form of advertising

enabled and brought great profits to data processors.
The microtargeting business model aims at the system of democratic decision-making itself and has turned the political parties into customers of social networks and data analysts.

What the authors of our Basic Law probably think about the activities of parties on social media such as Facebook and the one behind basic profiling of citizens would have said (on this the report with which Facebook wants to make activities on election advertising or advertising on politically and socially relevant topics and the related expenditure more transparent: https://www.facebook.com/ads / library/report/)? Art. 21 of the Basic Law, which stipulates that the parties should participate in forming the political will of the people, covered the conventional form of political advertising via radio and billboards. It would certainly have been completely unthinkable at the time, and not only for technical reasons, that the use of systematic data analysis and manipulative techniques of influencing the will by commercial providers would ultimately at least have an impact on democratic voting decisions. It is undisputed that parties must initiate political discourses and thus also broader platforms for

Information and social communication are required. As long as this practice strengthens a business model that is based in the background on profiling and microtargeting, is not very transparent and can hardly be controlled, it remains to be feared that political decision-making and the culture of democratic discussion will become dangerously sucked in and dependent on manipulation and distortions.

1.3 Automated facial recognition on the rise

One of the greatest threats to privacy currently comes from the use of automated facial recognition: biometric facial databases, which enable faces to be assigned to individual persons, have already been set up. This is especially true for China, which uses facial recognition like no other country for comprehensive surveillance of the population

uses. But private providers in the USA and Europe also offer the global option of searching for people's identities using faces.

As early as 2011, the Hamburg Commissioner for Data Protection and Freedom of Information (see 23. TB 2010/2011 IV 3.3) checked the introduction of automated face recognition by Facebook in Europe without the consent of the users and initiated administrative proceedings against it. At that time it was still about the rather harmless-looking function of making it easier to find and mark people in photos. However, this presupposes that a database is created in which the images of as many users of the service as possible are biometrically processed and assigned individual face IDs. The option of opting out, which is also difficult to access, with which an objection to this processing of one's own image could be lodged, does not replace consent. The function was therefore in breach of data protection. As a result, Facebook stopped using the facial recognition function in Europe and only started operations again after the General Data Protection Regulation (GDPR) came into force, albeit on the basis of a consent solution.

In the meantime, the technology of automated face recognition has also found its way into criminal prosecution in the Free and Hanseatic City of Hamburg: In the course of investigating the riots at the G20 summit in Hamburg in 2017, the Hamburg police set up a database that contained pictures of people who were at demonstrations, as mere passers-by on the streets or in the area of public transport. All

Images collected from different sources were evaluated using face recognition software. This reference database was then combined with photos of criminals

balanced (see 26. TB 2016/2017 II 2). The order of the HmbBfDI to delete the biometric reference database - but not the files on committed crimes and suspects - was lifted by the Hamburg Administrative Court. Unfortunately, about the admission

the OVG has not yet decided on the appeal.
As long as a decision to use such an invasive technology on the basis of a general clause in the Federal Data Protection Act has not been made, there is no legal clarity as to whether such image evaluations are permissible for criminal prosecution purposes and may in future be carried out without a special statutory regulation to protect the rights and freedoms of those affected .

Evaluating photos from social networks and others

Services, but also from video surveillance databases or private recordings, makes it possible to break up the anonymity of people in all conceivable situations. Whether videos from

Gatherings or gatherings, in front of and in religious meeting places or simply when shopping in the supermarket – in future, with the help of facial recognition software, depicted people can be identified both in real time and afterwards, even in large crowds.

An important task of the supervisory authorities in the area of data protection was and is therefore to counteract the considerable dangers to privacy that emanate from the extensive and unregulated use of facial recognition software and the creation of corresponding reference databases.

Companies that extract publicly accessible image files by so-called scraping, i.e. by browsing websites, and thus fill huge biometric databases, which can then be searched for individual image data, must be checked to see whether they meet the requirements of Art. 9 2 GDPR regarding the processing of special categories of data, which include biometric facial models.

The business model that enables paying customers to identify and match people's faces from anywhere within seconds is currently on the rise. A company that primarily offers its services to security agencies in the USA and through a database with billions of faces

should have, is the US company Clearview. Based on a complaint, the HmbBfDI initiated administrative proceedings against the company and is examining the legal admissibility of the storage and biometric processing in this context.

Another company offering a similar service to the general public as a face search engine is PimEyes, originally based in Poland and recently registered in Seychelles under the company name 'Face Recognition Solutions Ltd'. A complaint is also pending against this company in Hamburg. Currently, the Polish data protection supervisory authority is examining whether the company is still within their jurisdiction.

In both cases, it is not only a question of the permissible processing of biometric data, but also of the applicability of the GDPR, since in both cases the companies are apparently based outside the EU. A registered office in Europe is important for the assignment of a lead supervisory authority, but it is not required to trigger regulatory action.

For the GDPR to apply, it is sufficient for a controller based outside the EU to offer services to data subjects in the EU (for the procedure towards Clearview, see V 3). In this respect, all the supervisory authorities of the Member States are responsible.

It is important to measure such offers with biometric data processing against the EU General Data Protection Regulation. Uncertainties about the applicability of the GDPR and the responsibilities of the supervisory authorities must not ultimately create a legal vacuum
create in which business models of companies undermine the rights of the persons concerned to their biometric data.

1.4 Data protection between yesterday and today

The comparison between 2009 and the present shows that

that much of what was discussed and argued about at the time is now related to the actual risks to the informational self determination right appears in a far less glaring light.
Looking back, it quickly becomes clear how much the digital-technological development and the economization of personal data have changed the concept of privacy and pushed back the right to informational self-determination. The significant impact of digital technologies on privacy are issues that are nowhere near as electrifying as they were in the days of Google Street View. This is due to a gradual adjustment to the technical specifications and the associated familiarization effect. Digital developments take place in a step-by-step process. Privacy is not a static legal concept, but is subject to a high degree of social change. In a time of massive technological innovations that are changing the entire culture of communication, the awareness of one's own private sphere is relativized by the publicity of private life and by the mass dissemination and exchange of personal data. The importance of privacy has become more and more valuable, especially against the background of the fact that personal data can be accessed at any time from social networks and via search engines. What is and should remain private and what is not is changing rapidly. The publication of a picture of one's own house on the Internet is therefore judged differently than 10 years ago. this effect

but does not make data protection obsolete. On the contrary: every individual needs a concept for their own data management, precisely in order to draw the boundaries in the digital world that are necessary to protect themselves.

It is therefore to be welcomed that the GDPR not only empowers the supervisory authorities to take action against data protection violations, but also contains the competence to continuously inform the public about the special risks of digitization and their dangers to privacy (Art. 58 para. 3 lit b GDPR).

2. The implementation problems of data protection EU level - Will the GDPR implode due to the lack of law enforcement in cross-border data processing?

The GDPR has introduced a completely new architecture for the cooperation between supervisory authorities, which makes law enforcement much more difficult. While the application of the law is usually a monocratic task of a hierarchically organized authority, the model of enforcement in the GDPR for cross-border data processing is based on a delicate network of cooperative agreements and information obligations with the aim of reaching a consensus (Art. 60 Para. 1 S 1 GDPR). If such a consensus is not reached in the cooperative administrative procedure, the final decision is transferred to the European Data Protection Board (EDPB), the highest EU body for data protection, consisting of all member state supervisory authorities. Here the majority vote applies. Unfortunately, the EDPB has only made one decision in the dispute settlement procedure since its inception. In this it has taken a restrictive stance on its own powers to review and correct decisions of individual supervisory authorities (see III 6).

At first glance, the consensus and diversity model in law enforcement, in which everyone has shared responsibility for each procedure and all specific cases have to go through the eye of a bottleneck, seems likeable and democratically well-founded. In fact, it raises massive difficulties that make effective and harmonized enforcement more difficult and prevent uniform enforcement of data protection law in favor of the rights and freedoms of those affected in Europe. Different national procedural regulations reinforce this effect. So far, the global tech companies have hardly been sanctioned despite numerous data protection complaints and serious incidents. Fines levied under the GDPR largely related to purely national procedures in which no cross-border

de data processing took place and cooperation at European level was not triggered. The number and amount of fines levied for cross-border data processing is disproportionately small compared to the fines levied for national processing. Legally binding orders in these proceedings are extremely rare. The one-stop shop procedure, according to which the supervisory authority at the location of the main office in the EU is responsible for every company, leads to a concentration of responsible bodies in a few member states and not only weakens data protection, but also proves to be a gateway for distortions of competition in the digital single market.

Despite a comprehensive evaluation of the provisions of the GDPR by the EDPB and the EU Commission, recommendations and suggestions that could be used to eliminate the weaknesses of the current enforcement procedure have not yet been asserted. The basic assumption that the GDPR will lead to better regulation of those global data processors whose business purpose is to collect and evaluate data is increasingly being disappointed.
Central issues raised by complaints to the supervisory authorities remain unanswered for years. If nothing is done here, minor legal corrections to the procedural design of the GDPR will no longer be sufficient. Instead, deep interventions in the GDPR would have to be discussed – such as shifting the supervision of large companies to a pan-European supervisory authority to be created for this purpose.

3. The local view: The appropriate equipment of the Supervisory authority – A recurring basic problem in times of increasing task responsibility

3.1 The current development

In recent years, budget negotiations have changed
different assessments of the

measured equipment to fulfill the tasks of the authority of the Hamburg Commissioner for Data Protection and Freedom of Information. In the course of the introduction of the GDPR, the HmbBfDI registered further needs, which were, however, significantly reduced in the budget process. Counteracting this by hiring staff for a limited period has been a means of briefly compensating for the qualitative and quantitative increase in tasks in recent years. This is currently no longer sufficient.

The following was already pointed out in the last activity report for 2019: "Despite an increase in staff in the meantime ... the question arises as to the medium-term ability of the authority to act.", 28th TB 2019 I 1). The situation has deteriorated further within a year. More and more people are demanding their rights or advice. This is definitely positive, as it shows a sensitization for privacy.

At the same time, it leads to a worrying processing backlog that is growing dangerously. The demand for additional reinforcements, even if only temporarily, to work through the backlog has not yet been met.

The situation of the supervisory authority in the reporting period was in characterized by a continuous flow of submissions and complaints, a significant increase in OWi proceedings (see VII 1.3) and, in particular, by a major proceeding that led to the imposition of a fine of 35.3 million euros. New issues arising from the pandemic in very different areas of data protection have led to the situation in the complaints processing at the end of the year not developing as well as hoped. The pandemic-related shift to the home office certainly played its part. The response to this was a further change in the organization of the authority. In the future, a more efficient and modern structure is to be created by focusing on fewer specialist departments and subdividing them into specialist areas and by creating responsibilities for old cases. A differentiation

between data protection in the public and private sector, which was already passed by the GDPR, will no longer take place in the future. Instead, content-related competencies that are more closely related to each other are combined.

3.2 The efficiency of the authority in retrospect

Even if publicly funded authorities are not pro
fit center, the ten-year balance sheet includes a budgetary review. In this respect, it may come as a surprise that while there were repeated debates about the appropriate level of equipment, the authority has not only been able to fully finance its own budget over the past decade, but has also paid into the budget of the FHH. This is based on the revenue from fines and fees on average in the last 10 years from 2010 to 2020 and in particular by

the non-recurring effect of the EUR 35.3 million fine from the current reporting year, the HmbBfDI has a surplus of around EUR 1.4 million annually after deduction of all personnel and material costs corresponds to data protection, the activities of the supervisory authority have nevertheless been economically successful over the last few years.

3.3 New proposals to strengthen the position of the HmbBfDI

Data protection and freedom of information are central pillars of digital democracy and the rule of law. As a state institution, the HmbBfDI, like any other independent supervisory authority, is committed to protecting the rights and freedoms of citizens. This guiding principle of the GDPR will make further efforts necessary in the future to strengthen the concerns of data protection, but also freedom of information.

For an effective structure, it makes sense to connect to

the Subcommittee on Data Protection and Freedom of Information
to loosen citizenship. The negotiation of central issues of the rule of law and digitization in a subcommittee has not always proven its worth in recent years.
subcommittee
Due to their dependency on the specialist committee, representatives of the citizenship are only able to a limited extent to independently pursue an agenda. They are appointed by the specialist committees and receive their orders from them. Already the referral of the annual activity report from the citizenship to the judiciary committee and from there to the data protection and information-free subcommittee

It's bureaucratic and time consuming. Current topics that require rapid advice are difficult to address in this way.
In addition, the areas of data protection and freedom of information
by being delegated to the subcommittee, they are procedurally routed to a second tier, where they are then subjected to parliamentary discourse, which often has little publicity and in which, as a rule, a small number of MPs take part. It could make sense in the future to discuss current issues in the main committee without delay. In return, there should also be a stronger focus on content, so that topics with a greater depth of detail and less up-to-date orientation can continue to be dealt with in the subcommittee.

Another important aspect concerns the position of the HmbBfDI in the context of the budget process. The special importance as a control body for the senate-independent and senate-dependent authorities makes it seem sensible to anchor a procedural design here in the future that enables an objective determination of the personnel and material budgetary requirements. The previous practice is characterized by the fact that the funds required for adequate equipment, which were registered by the HmbBfDI, have only found insufficient recognition in the budget process.

In the future, this debate could be more objectified by a
Committee or commission set up by the citizenship

and a report on the status of the equipment or a concrete needs analysis is drawn up. This would create a basis for the budget negotiations, on the basis of which a transparent discussion about the appropriateness of the reported needs can take place. This body can be made up of experts, but also of members of parliament. It is important that the members of such a body familiarize themselves with the work and organizational processes of the data protection supervisory authority before writing their report.

Such a body would take into account the legal background that adequate resources are not a matter of a beneficence by the budget legislature, but of a corporate right that is directly linked to the complete independence of the supervisory authority. This right is both at the level of the primary law of the EU and at the level of the

enshrined in the state constitution. In this regard, Art. 52 (4) GDPR contains the following statement: “Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure that it needs to carry out its tasks and powers within the framework of the To be able to effectively provide administrative assistance, cooperation and participation in the committee.”

Data protection supervisory authorities have a responsibility to ensure the protection of the rights and freedoms of those affected. They must therefore be set up in such a way that they can meet the demands of people seeking legal advice or simply seeking advice men and their numerous other tasks (cf. Art. 57 Para. 1 lit a - lit v GDPR). For their part, Member States have a responsibility to ensure that the supervisory authorities have the human, technical and financial resources they need to carry out their tasks and powers effectively. Where this is not possible, the necessary support must be granted.

In order to properly assume this responsibility for guaranteeing, a corresponding process design should ensure the independence of the HmbBfDI in the future.

4. On the future of data protection

Data protection is not an end in itself, but presupposes people with rights and freedoms. The independence of supervisory authorities has a strictly supporting function. In particular, supervisory authorities have the task of independently monitoring the responsible bodies. This includes not only private companies, but also all public bodies, from government to administrative authorities, in which data is processed.

An independent supervisory authority should therefore always be ready to enforce the rights and freedoms of those affected, even if this is difficult in individual cases and resistance is too high
are squirming. At the same time, the supervisory authorities will only be successful if they see themselves as part of digital strategies and change and openly help shape this change. Bureaucratic processes, slow decision-making processes and a lack of willingness to engage in dialogue are to be avoided not only on the part of the supervisory authorities, but also on the part of the public and private bodies that implement data protection.

4.1 Supervision in multi-agency systems – No centralization of data protection supervision at federal level!

Data protection must not get lost in bureaucratic procedures.
The data protection authorities face particular risks in this regard
in a federal structure in which the supervisory authorities are split into individual factual and local responsibilities. This applies in particular to the supervisory authorities in Germany, who not only coordinate among themselves when it comes to enforcement at the national level, but also when it comes to coordination at the European level in the group of 27 supervisory authorities in the member states

have to communicate with each other.

Data is an extremely mobile asset. National borders, but also the borders of the member states of the EU do not stop the flow of data. The rights of those affected should therefore also not be affected
be bounded. It is an important legitimating criterion for the work of the supervisory authorities that they create a uniform implementation of data protection law in their areas of responsibility: This is only possible if we succeed in formulating overarching standards for the interpretation and application of the law and if these are implemented uniformly. Different standards lead to one
Fragmentation of the law and result in significant distortions of competition.

There are much bigger problems at EU level, which result from the bureaucratic regulatory procedures, among other things
than in the national area (see I 2 above). The current debate about centralizing data protection supervision in Germany and focusing enforcement powers on the federal level has the wrong focus in this regard. This debate is a revenant and had arisen before, only to quickly disappear into thin air. The subject is problematic from a number of perspectives: In Germany, it is a constitutional principle that the federal states are responsible for enforcing the law. The interpretation and application of the law, which is not always uniform, is inherent in federalism up to a certain point. The national Be

In the past, authorities have defined common standards and guidelines in the conference of independent data protection supervisory authorities of the federal and state governments (DSK) and, with a few exceptions, have pursued a uniform, common line.
The coordination of essential legal issues in the data protection conference, in which all state commissioners and the federal commissioner are represented, enables a harmonized application of the law and serves to create and maintain a uniform line in enforcement. If you want to change this, first of all wear the

burden of argument and should provide examples of where practice is not working here.

At national level, centralizing data protection supervision in a federal authority is not an option, not only because of the constitutional argument but also because of the lack of proximity to the citizenry. Nor can this be in the interest of the regional economy, which would lose direct contact with the local data protection authority.

A closer look reveals that the problem is not in the area of national enforcement, but at EU level. There are very different standards and a backlog of enforcement, especially in relation to global tech companies based in a few EU member states. Above all, the supervisory authority procedure of the GDPR does not work, which provides for bureaucratic and cumbersome enforcement and, in current practice, invites companies to forum shop, which are naturally not interested in a strict supervisory authority. There is therefore a massive need for action at European level. In Europe, the issue of data protection must not be reduced to a question of location and give individual companies advantages because they have their headquarters in a certain member state.

4.2 Independence is to be maintained!

The future of data protection depends very much on the independence of the bodies that are supposed to monitor and control compliance with data protection rules. The full independence of the supervisory authorities is enshrined in EU primary and secondary law guaranteed for many years. This does not mean that political influence on the decisions of the independent bodies is practically not an issue. There are many connecting lines and interfaces between data protection supervision and political shaping. This begins - even without legal and technical supervision as well as official supervision of the independent body - with the trans-

parental selection of the head of the authority (Art. 53 Para. 1 GDPR) and ends with the question of equipment from a personnel and technical point of view. Equipment deficiencies in particular can very quickly impair independence. This is the case when personnel or financial deficits affect the decisions of the independent body.

The audited body itself decides on the budget of the independent bodies using the budgetary procedure prescribed by the constitution. This is the case with regard to the government when preparing the budget, but also when the budget legislature makes decisions about the budget itself. Even if the control of core parliamentary activities has not been one of the tasks of data protection supervision at the federal and state levels in the past , since at least the parliamentary administration is under their control. Recently, the ECJ also extended the validity of the provisions of the GDPR to the core activities of the parliaments (in particular the Petitions Committee) (ECJ C-272/19).

In order to maintain the independence of the control bodies, the procedure for their financial and human resources should be as objectifiable and transparent as possible. Decisions about the budget of the independent body should therefore be prepared by the decision of an independent body and geared to the actual needs (see above). This ensures the neutrality of the decision-making process and enables the independent bodies to carry out their tasks properly.

4.3 Perceive supervisory authorities as partners, not as opponents, of openness to innovation and digital awakening!

Against the background of the experience of the last few years and in particular of the present reporting period in 2020, the following must be emphasised: Digital awakening, openness to innovation and the Creation of a modern digital infrastructure are central goals and in a Europe of the charter of fundamental rights and data protection

basic regulation not against, but only with data protection. This doesn't work without a culture of communion

communication and cooperation. Whether when using video communication tools in schools and universities

or when formulating regulations for the traceability of infection chains: the data protection authorities are always too

partners of public authorities and should be involved by them at an early stage. Unfortunately, this was not always the case in the past reporting year.

In the reporting period, the HmbBfDI received a letter from a zen

central office of the Senate, in which he was recommended to confine himself to controlling the administration, since he was not the Senate's IT consultant. This shows a basic attitude that needs to be overcome. The advisory task is a central function of data protection authorities. You are on board when it comes to tackling the challenges of digitization in a humane and confident manner. Restricting the activities of supervisory authorities to control and sanctioning functions may correspond to a widespread prejudice. Putting supervisory authorities in the brake booth and ignoring them in strategy discussions and planning is not a sustainable concept. Politically and economically, this leads to a dead end, because sustainable developments cannot do without taking into account the right to privacy, informational self-determination, the confidentiality and integrity of information technology systems. Privacy by design and privacy by default are already integral components of a digital innovation that sees progress not as an end in itself, but in the service of people. Open communication and cooperation and the clear will to create modern and well-equipped data protection authorities for the implementation of these tasks are prerequisites for this. This should be a matter of course in the future.

II. CORONA-PANDEMICS

1. Corona Containment Ordinance

The HmbSARS-CoV-2 Containment Ordinance not only determined public life in Hamburg in 2020, but also enabled numerous encroachments on fundamental rights, including the right to informational self-determination. The HmbBfDI provided assistance with the interpretation and worked towards adjustments.

To contain new infections with the coronavirus, the Hamburg Senate issued the HmbSARS-CoV-2 Containment Ordinance on April 2, 2020. It introduced far-reaching contact restrictions, business closures and event bans. Over the course of the year, the ordinance was amended 23 times to reflect the changed pandemic situation and federal-state agreements.
Among other things, authorizations and obligations for interventions relevant to data protection were added. This applies above all to the mandatory recording of the contact details of guests in restaurants, hairdressing salons and other facilities and events. Other regulations, such as the credibility of the exemption from the obligation to wear mouth and nose protection, also relate to data protection.

The ordinance is based on Sections 28, 32 sentences 1 and 2 of the Infection Protection Act (IfSG). Due to its far-reaching encroachments on fundamental rights, the HmbBfDI has spoken out in favor of regulating the main powers through a parliamentary law. The underlying constitutional concerns, which were also expressed by many stakeholders, were addressed with the creation of Section 28a IfSG on November 18, 2020, so that the particularly invasive contact data collection is now on a basis sufficient for parliamentary approval.

The constantly changing ordinance has led to numerous inquiries from entrepreneurs and those affected

the requirements to be placed on data collection and use. In addition to individual consultations, the HmbBfDI has also responded to this uncertainty with assistance such as the continuously updated internet guide “Data protection in times of Covid-19”.

The Senate did not involve the HmbBfDI either in the initial enactment or in the new versions of the CoV-2 Containment Ordinance. This is regrettable, not only because the Senate's investment guideline provides for the opportunity to comment. The HmbBfDI has repeatedly asked to be consulted on further changes so that its expertise and experience with advisory cases can flow into the further development of the ordinance.

After all, the Senate made several changes after the HmbBfDI had pointed out ambiguities in the text of the regulation in its public advisory service. For example, it was noticed that with the version of May 13, 2020, the recording of “contact data” was initially mandatory in certain facilities, but this term was not defined. This led to great uncertainty among those affected and those responsible due to the large number of conceivable communication media. After the HmbBfDI pointed out that without a concrete definition of the term, the guests have the right to choose which data they would like to disclose, the Senate decided in the amendment of June 30, 2020 that the name, postal address and telephone number must be given. Another example is an ambiguous provision contained in the regulation until June 30, 2020, which was partly understood as a requirement for innkeepers to check whether guests at a table would belong to the same household. After the HmbBfDI pointed out this Inter

pretation, the clause was removed from the regulation in the next revision. There was also a clarification of the obligation to check the bodies obligated to collect the contact data and the legal consequences of missing or incorrect information.

There is no question that the pandemic events require quick reactions. This alone does not explain the lack of willingness to communicate. The ambiguities caused by the implementation of the regulations in the area of gastronomy could certainly have been avoided in advance if the data protection authority had been involved.

2. Examination of contact data collection in restaurants

Catering establishments must implement the data protection regulations and take all necessary technical or organizational measures to protect the contact details of customers, which are collected to trace infection chains. In practice, the safe storage of the contact data on site proved to be one of the decisive factors for the acceptance of the fulfillment of the existing disclosure obligations by the persons concerned.

Numerous restaurants and those affected have in the Be reporting period to the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) because there was great uncertainty as to how contact data processing was to be implemented in accordance with the Hamburg SARS-CoV-2 Containment Ordinance. Those affected also reported on the partially widespread Pra xis to lay out open lists in the entrance area. This is problematic in terms of data protection law, since the contact details are thus disclosed to all subsequent guests without authorization.

The background to the collection of contact details in restaurants is the obligation on business owners in various sectors to record the names and contact details of all guests since May 13th, 2020. This follows from the HmbSARS-CoV-2 containment

VO and also affects the area of restaurants. So it exists an obligation and thus, in accordance with Art. 6 (1) (c) GDPR, also the right to document contact details and the time of the stay in writing and to keep them for four weeks. The contact details also include the name. With regard to further contact details, the ordinance initially did not specify any specifications, so that, according to the HmbBfDI, visitors were free to decide, for example, on a postal address, telephone number or e-mail address. Have been starting more than this data

When asked, there was obviously a violation of the principle of data minimization and consequently a violation of the GDPR by the restaurants, as they were responsible for collecting contact data.

It was not until June 30th, 2020 that the regulation on the collection of contact data was specified and expanded to the effect that the contact data was specifically defined as a name, home address and a telephone number. After the HmbBfDI pointed out to the legislature from the outset that open lists are also unacceptable, the Senate has fortunately included a corresponding note in the HmbSARS-CoV-2 Containment Ordinance. It now states that it must be ensured that unauthorized third parties do not gain knowledge of the data. The regulation has remained in force to this day.

The HmbBfDI took the numerous complaints and requests for advice as an opportunity to randomly inspect 100 commercial and restaurant businesses in June with regard to the implementation of the contact data collection. The focus was on advising and raising awareness of the local economy in the implementation of contact data processing according to the rules of the GDPR. Sanctions were not yet to be feared at this stage.

During the random check, the HmbBfDI determined that 33% of the checked companies used lists for contact data processing.

I used lists that were lying around openly and accessible to everyone (e.g. lists that were laid out openly on the counter, on the tables or at the entrance).

The number of complaints remained high as the process progressed. The press also reported that many catering establishments have not deviated from the practice of using openly available lists to process contact data.

Our subsequent follow-up inspection proved that in some restaurants the requirements were not implemented contrary to our order, so that it was necessary to impose more extensive measures to enforce the data protection requirements. Fines of between 50 and 100 euros were finally imposed in three cases.

Further fine proceedings were opened against individuals and companies who misused contact data for personal or advertising purposes.

3. District office check: confiscation of data and comparison of the population register

The enforcement of the provisions of the HmbSARS-CoV-2 Containment Ordinance by the health authorities has raised numerous data protection issues.
Of course, when it comes to issuing drastic regulations, the state must ensure that these are also followed. But the rule of law also proves its worth, especially in times of crisis - therefore the enforcement of the regulations in exceptional situations must follow the rule of law guidelines.

The HmbBfDI learned from the press that the Mitte district office on

weekend of 19./20. September 2020 in St. Pauli confiscated contact data lists in various locations and then compared them with the population register. The HmbBfDI took this reporting as an opportunity to examine the facts as part of its own examination procedure.

It was determined that the measures mentioned served the purpose of checking compliance with the requirements of the HmbSARS-CoV 2 Containment Ordinance. The comparison of registration registers in particular should also provide general information as to whether the requirements of the ordinance are being complied with by the citizens or whether fictitious, incorrect or incomplete data has been provided across the board. For this purpose, it was checked how often the information provided matched the addresses stored in the population register. The results generated in this way were only stored statistically and not for individuals. The contact lists themselves were returned to the operators of the locations a few days later.

The legal review of this fact has shown that the comparison of the contact data of those affected with the population register carried out by the Mitte district office was unlawful. The intervention was neither based on the suspicion of an infection nor was it related to fine proceedings that were carried out due to violations of the containment ordinance. At that time, the containment ordinance did not provide for fines for those affected in the event of violations of the disclosure of their data. Measures against operators of restaurants that would have justified a comparison of the contact details with the population register did not exist because there was no obligation to check the correctness of the data. A comparison with the population register was neither suitable nor necessary to prove that the contact details were missing or obviously incorrect.

The legislator took this criticism as an opportunity to issue clearer regulations at the beginning of October, exactly what

nomen are obliged and under which conditions the competent authority may have the contact details of the visitors released. For this reason, the HmbBfDI has refrained from taking formal measures such as a warning in relation to this data processing.

4. Examination of an instruction from the social authorities to send the contact details of infected schoolchildren from the health authorities to the BSB

In fighting the pandemic, there was great potential for conflict in various areas of the school system. In particular, the transmission of data positive ge
tested students from the health authorities
to the Authority for Schools and Vocational Training (BSB) raised complex data protection issues.

The HmbBfDI was informed on October 5th, 2020 that the authorities for work, health, social affairs, family and integration as well as the authorities for science, research, equality and districts all health authorities of the Free and Hanseatic City of Ham
burg on October 6th, 2020, according to § 6 paragraph 1 sentence 1 number 1 letter t of the Infection Protection Act, in addition to the schools, the authorities for school and vocational training also regularly provide data on the name, date of birth and the home address of schoolchildren who tested positive to transfer. In essence, it was about the legality of such data transmission and whether the employees of the health department would behave unlawfully or even make them liable to prosecution under § 203 StGB if they not only regularly sent personal health data to the schools concerned, but also to the submitted BSB.

The HmbBfDI has initiated an examination procedure to examine this issue under data protection law. As part of this, the transmission of data on the name, date of birth and home address of schoolchildren who tested positive was carried out by the health authorities to the authorities for schools and jobs
education found to be lawful in principle.

The lawfulness of the processing of this data by the BSB resulted from Art. 6 Paragraph 1 lit. e GDPR in conjunction with Section 98 HmbSG. The processing of the real names of infected pupils was necessary to fulfill the tasks assigned to the BSB according to § 23 HambSARS-CoV 2-KonsemptionVO. This regulation assigns the BSB and the schools joint tasks of infection control. These tasks were implemented by the BSB by creating model hygiene plans according to § 23 paragraph 1 HambS ARS-CoV-2-EindammingVO. The schools implemented these sample hygiene plans as institutions in accordance with Section 33 of the Infection Protection Act (IfSG) through specific hygiene plans. The content of the hygiene plans was based on the specifications for the design of teaching activities according to § 23 paragraph 2 HambSARS-CoV-2-EindammungsVO, according to which it was to be ensured, for example, that schoolchildren for whom official quarantine was ordered left the school do not enter (§ 23 Paragraph 2 No. 2 last half-sentence HambSARS CoV-2 Containment Ordinance). In order to fulfill this task, it was necessary to know the real names of the pupils concerned ler. The basic decision on the need to collect this data was made by the BSB when setting up hygiene requirements and the school concerned when it came to actually implementing these requirements. The knowledge of the real names was necessary for the affected school to fulfill the obligation under § 23 paragraph 2 HambSARS-CoV-2-EindammingVO, for example to issue concrete house bans against the affected pupils. Even if the BSB mainly gives general specifications through model plans within the scope of Section 23 Paragraph 1 of the HambSARS-CoV-2 Containment Ordinance, as the school supervisory authority it has the monitoring function with regard to compliance with the obligation

from § 23 paragraph 2 HambSARS-CoV-2-EindammingVO, so that the knowledge of the clear names is also necessary for the BSB for this purpose is agile. In individual cases, the BSB, as the school supervisory authority, is obliged to check whether the school has issued house bans and has therefore fulfilled its obligations to protect against infection.

Against this background, the data transmission was not fundamentally objectionable. However, the authorities concerned were once again made aware of the fulfillment of the secondary data protection obligations, in particular the information obligations and the necessary data security measures.

5. Video conferencing systems in school lessons

The closure of Hamburg's schools in the spring of 2020 due to the pandemic involved the use of video conferencing systems and other digital services to conduct distance learning, the use of which in compliance with data protection posed challenges for the schools. Data protection issues are often not taken into account at first, but due to the particular problem, this only resulted in advice from the supervisory authority.

During the corona-related closures of the schools in the spring of 2020, the Authority for Schools and Vocational Training (BSB) and the Hamburg schools were faced with the task of organizing digital distance learning without having already developed a digital strategy or a corresponding concept . As a result, the school mostly developed its own solutions and relied on very different solutions and products without adequately considering data protection issues, which led to numerous submissions and complaints to the Ham

Burgische Commissioner for Data Protection and Freedom of Information (HmbBfDI).

The complaints, which related to the use of very different video conference systems and digital learning aids, were followed up by the HmbBfDI in intensive contact with the official data protection officer of the BSB. Due to the exceptional situation caused by the pandemic, the HmbBfDI pursued a cooperative solution and submitted various offers of cooperation to the BSB and the Senator for Schools and Vocational Education in order to set up an official offer for a video conference system or a corresponding learning platform for conducting distance lessons in data protection to provide legal assistance. While there was intensive cooperation at the working level in the context of complaint processing, the concrete offers of cooperation at a higher level unfortunately remained unanswered. Nevertheless, in the second half of December, the BSB entered into a fundamental planning of uniform regulations for digital school lessons and involved the HmbBfDI.

The development of an official offer of a video conference system or a digital learning platform is necessary in Hamburg not least against the background of the data protection regulations of the Hamburg school law. According to the provision of Section 98 b of the Hamburg Schools Act (HmbSG), only the competent authority is authorized to operate electronic learning portals and pedagogical networks and to use them in the classroom in order to help the schoolgirls and teach students media skills. According to § 98 paragraph 2 HmbSG, the competent authority may only use other bodies outside the public sector in exceptional cases and integrate their digital learning offers and learning content into the school networks. In this case, however, for a special security of the data of the students to ensure. In addition, the data of the students may only be used anonymously, aggregated or pseudonymised.

The requirements could not be met in the complaints pending at the HmbBfDI, so that the processing of the personal data of the students required for the use of video conference systems and other digital learning aids does not apply to the area-specific and thus conclusive regulation of § 98 b HmbSG could be supported as a legal basis in connection with Section 6 (1) sentence 1 lit. e General Data Protection Regulation.

As a result, the data protection officer of the BSB, by advising the schools, ensured that the processing of personal data of the students when using video conference systems or other digital learning materials that did not meet the requirements of § 98b HmbSG only with the consent of the pupils or their parents took place and could therefore be based on the legal basis of Article 6 Paragraph 1 Clause 1 Letter a GDPR. This made prior information about the type and scope of data processing necessary. In the school sector, it was important to ensure that consent could actually be given voluntarily, so that comparable and appropriate teaching materials had to be made available as an alternative to teaching via a digital service.

For the data protection framework that must be observed when using video conferencing systems, reference is also made to the orientation guide (OH) on the use of video conferencing systems published by the conference of independent data protection authorities of the federal and state governments (DSK) on October 23, 2020, which is also contained therein for the school sector, abstractly the legal one Requirements for the construction, operation and maintenance of video conferencing systems defined, referenced (see II 10).

The use of video conferencing systems by commercial providers, who often in a non-transparent way collect the data from the students concerned, but

also processed by teachers for their own purposes, makes it difficult in practice to give informed consent as a legal basis. In addition, the voluntary use of video conferencing systems in schools is fundamentally questionable: Especially when schools are closed, there is high pressure on everyone involved to use alternative communication channels and to encourage their use

place to agree. In this respect, there is little room for consent solutions that make it possible to avoid the requirements of Section 98b SchulG.

It is to be welcomed that the school authorities, taking these concerns into account, are striving for comprehensive and uniform regulations for digital teaching across the board for all Hamburg schools. A regulation based on Section 98 of the Schools Act is intended to enable live streaming of school lessons for special reasons in the future, so that the associated encroachment on the privacy of those affected is placed on a clear parliamentary law regulation.

The HmbBfDI advocates a sustainable anchoring of the protection of the informational self-determination of all those involved in digital learning and advises those involved in the search for a modern solution that takes due account of the privacy of those affected.

6. IFB and Nect app exam

The first wave of the Covid-19 pandemic not only put the healthcare system under enormous pressure, but also many sectors of the economy. The governments therefore promised quick and unbureaucratic payment of emergency aid. However, their implementation has exposed various data protection weaknesses.

Like other federal states, Hamburg has been targeted by fraudsters who attempt to exploit the lack of data security measures by applying for payments with forged or tapped data. There was also a need for readjustment here.

In the Free and Hanseatic City of Hamburg, immediate aid was paid out by the Investment and Development Bank Hamburg (IFB). After uncovering phishing attacks, the IFB began to use an app provided by Nect GmbH to identify applicants, which was supposed to take over the identification process. In this way, Nect GmbH processed data from applicants, for which it relied significantly on consent as the legal basis.

The app carried out a largely automated check of the applicant's identity and authenticity. It thus replaces the use of employees who, in the online process, e.g. B. had to recognize the correct identity of applicants by means of a video call by showing an identification document. The app, on the other hand, had to be presented with the ID document using the cell phone camera. In addition, by repeating a short text provided by the app, it was ensured that it was a real person. Biometric data was processed as part of the app in order to be able to carry out the desired authenticity check, which was based on the corresponding consent of the applicants.

The HmbBfDI learned about this matter through various complaints
behavior and initiated an examination. Since the processing of personal data in the course of authentication by the app was based on consent, it was questionable whether this could actually have been given voluntarily. The applicants could not benefit from the promised immediate aid without authentication by Nect GmbH. It was to produce a corresponding voluntariness of the consent

therefore required that alternatives to the authentication process operated by Nect GmbH were created.

With these concerns, the HmbBfDI turned to the provider of the App and to the IFB. The provider was asked to answer a catalog of questions from which no deficiencies could be identified with regard to the formal requirements such as earmarking, storage periods and data protection impact assessment. With regard to the fundamental question of a relevant legal basis, the IFB took up the concerns of the HmbBfDI and took the request as an opportunity to create voluntariness by setting up other alternatives to identify oneself as an applicant. procedure back.

Its establishment ultimately made it possible for all people who, for various reasons, could not use the Nect app to also apply for emergency aid. With this pleasing result, the process could be closed here.

7. Corona Warn App

With the development of the Corona Warn App, the Federal Government has broken new ground, both in terms of its open development model and its data protection-friendly functionality. The Hamburg Commissioner for Data Protection and Freedom of Information critically monitored its creation.

In the search for a social approach to the upcoming Covid-19 pandemic at the beginning of the year, a number of technical solutions for tracking infection chains and avoiding further infections from people who were already infected were discussed.

Among the first ideas were some approaches that were problematic from a data protection perspective. Including in particular those who

rely on the collection of location and other personal data for tracking contacts and a central storage and evaluation of this information. However, projects were quickly formed that pursued a trustworthy approach that was compatible with data protection law, such as e.g

PEPP-PT or DP-3T, the design of which was later implemented by Apple and Google in an unprecedented joint project in the form of a contact tracing protocol. The Corona Warn App (CWA), which was developed by T-Systems and SAP and ultimately opted for by the federal government, enables contacts to be tracked in a data protection-friendly manner while maintaining the principles of decentralized storage and voluntariness.

The Hamburg Commissioner for Data Protection and Freedom of Information accompanied the public debate and the development of the CWA for months and expressly welcomes the implementation of a decentralized system for recording contacts. The fact that the Corona Warn App has now been downloaded by more than 24 million people (as of December 18, 2020) is quite a success. Large parts of the population would certainly not have confidence in the data protection compliance of the app if all data were recorded centrally on a server operated by the federal government stood. Another important reason was the open source development of the CWA. Public source code enables independent bodies and the technically savvy public to form their own opinion of the app and its data processing, as well as to get involved, report bugs and suggest new features. All of this has taken place in the development of the CWA and should be an example for future public sector software developments.

The recent discussion about an app solution that should tie in with Southeast Asian solutions and possibly be based on a decentralized, non-voluntary model should not end up jeopardizing this trust. Despite all the concerns about the pandemic that is still spreading and the massives

Ultimate personal and social consequences, it must not be forgotten that a tracking app that records all movement data centrally by no means guarantees a more successful fight against the virus. The associated interventions in the right to informational self-determination could shake the population's trust in the CWA and thus undermine its functionality.

If the voluntariness were questioned, it would ultimately also remain questionable what a solution should look like in which people are checked to see whether they actually leave their place of residence with their mobile phones or simply leave them at home.

The CWA certainly has room for improvement, and in particular the lack of connection between many test laboratories and their infrastructure needs to be optimised. The app should also enable cluster recognition and provide users with the function of a contact diary, with which they can record their encounters. In connection with other measures, such as the possibility of more frequent comparison of the collected IDs with the server, clearer statements about contact encounters and a more precise risk determination are possible.

8. Working from home

In addition to increased technical and organizational measures when handling personal data, working from home always requires a home office agreement in advance.

Working in the home office is not only for employees

Employees face a major challenge, but also employers, since they remain responsible for the processing of personal data by their employees even when working from home.

Before work is shifted to the home office, the following should be done

Points to be observed from a data protection point of view:

ÿ Suitability of the activity for the home office

Employers should always ask themselves whether the activity is suitable for working from home. In this regard, the type of personal data to be processed is of great relevance. The more sensitive the personal data is, the less suitable it is to process it in the home office. For example, if it is data according to Article 9 GDPR (e.g. health data), social data or employee data, particular caution is required.

ÿ Home office agreement

Working from home requires an express agreement
tion - typically a works agreement from home office - which should contain at least the following content:

ÿ What work may be done from home ÿ Who provides the technical equipment and Internet access (including maintenance and repairs) ÿ Is the use of private hardware and software permitted ÿ Does the workplace have to be specially secured ÿ Regulations on employee data protection during working hours , on the accessibility and completion of a certain proportion of the working time at the workplace.

Since Article 13 of the Basic Law guarantees the inviolability of the home, employers have no general right of access to the homes of employees.

If access is expressly desired, effective consent is required for access to the employee's apartment.

ÿ Technical and organizational measures

Dangers in the home office can be different than in the company
Workplace. Employers must determine these in advance and take appropriate technical and organizational measures to ensure the security of the personal data (Art. 32 GDPR).

Suitable measures are

ÿ the employees for data protection in the
Raise awareness of the home office.
This can be achieved through training on data protection.

ÿ keep spatial security in mind.
Is there a separate workplace, separate room, away from the rest of the living area, which can also be locked?
Can telephone calls or video conferences be overheard by unauthorized third parties (especially family members or neighbors) in the vicinity? Can work documents and notebooks that contain personal data be kept locked after work?
It's just that

to store as many documents as is absolutely necessary in the home office. If necessary, an upper limit for documents with personal data must be set for the home office.

ÿ that ensure data security when using IT.
If possible, only technical devices and software provided by the employer should be used. If you use your own devices or software (bring your own device – BYOD), you must ensure that business and private data are kept separate, passwords are secured and different passwords are used for private and business use. Personal data should only be accessed via a secure VPN (Virtual Private Network) connection and be encrypted end-to-end. In the case of call forwarding from the business to the private telephone

fon, it should be ensured that callers outside the organization only see the office number.

If these requirements are met, nothing stands in the way of successful work in the home office.

9. Covid-19 prevention in companies

Companies in all sectors are currently making great efforts to prevent infections on their business premises. The privacy of employees and customers must not be neglected.

Company managements are subject to a duty of care towards employees and a responsibility for the health of their customers and other guests. In order to meet these requirements even during a time when there is an exceptional risk of infection, data collection that was hardly imaginable until recently seems legitimate in many companies. Data protection does not stand in the way of sensible measures. However, the special need for protection of health data must always be taken into account and an appropriate balance sought with the privacy of the people concerned. This demanding task has led to numerous requests for advice from the HmbBfDI.

He also proactively disseminated the results on his website and at online events.

The first questions about health protection arise when entering business premises and business premises. Questioning customers or visitors to shops about symptoms of illness is not permitted, nor is measuring body temperature using thermal imaging cameras or clinical thermometers. The information obtained is health data, de

9 GDPR is only permitted in strictly regulated cases. From the exceptional circumstances comes with the customer

9 (2) (a) GDPR. This must be done voluntarily, so access must not be made dependent on it. Alternatively, guests of the business premises should be informed by setting up or handing out information signs/sheets in the entrance area that they are asked not to enter the company for reasons of safety for employees and other visitors/customers if they have acute respiratory symptoms .

In the case of employees, the collection of health data to contain the pandemic may be justified under Section 26 (3) BDSG and Article 9 (2) (b) GDPR. Recording body temperature and asking about symptoms specific to Covid-19 are at best justified in workplaces with close physical contact or particularly systemically important facilities such as hospitals. In the other companies, employee surveys are possible to a limited extent.

In order to avoid contact with potentially infectious colleagues, it is not objectionable in the pandemic situation if, before entering the workplace, people are asked whether the person concerned is themselves infected with the Covid-19 virus, whether they are in contact with a verifiably infected person or whether they

during the relevant period in one of the Robert Koch Institute

area classified as a risk area.

For example, the open question, in which
country a holiday absence was spent or with which

Persons the person concerned was in contact with. Negative information from the person concerned that the above points do not apply to him is sufficient. As an alternative to the individual query, it can also be requested that employees actively report if they fulfill one of the above points.

With the end of the first lockdown and the gradual return

With the return of employees from the home office in the summer of 2020, the question of protecting risk groups increased. Many employers intend to keep people with increased protection needs working from home longer or to provide them with individual offices. They were faced with the challenge that belonging to a risk group is not immediately recognizable and that there is no obligation to disclose diagnoses or symptoms of illness to employers. From this labor law principle is also

not deviate in the pandemic. However, employees are free to point out previous illnesses of their own accord in order to obtain special protective measures. Employers may call for people to get in touch if necessary and may process the relevant data in this case. When storing the information, special protection must be ensured in accordance with Section 26 (3) sentence 3 BDSG in conjunction with Section 22 (2) BDSG.

Since members of the risk groups do not pose an increased risk to others, it is the responsibility of the respective responsible employee to decide whether it makes sense for them to disclose their data or not.

After all, despite all precautionary measures, is it an infection?
come on among the employees, it may be necessary to warn the colleagues. The identities of employees who have tested positive for Covid-19 must be treated confidentially, insofar as this is possible without endangering the health of others. The fact that a person is a carrier of the virus can be very stigmatizing. Therefore, the disclosure of personal data from people who are proven to be infected or suspected of being infected is for information

only lawfully if knowledge of the identity is necessary for the precautionary measures of the contact persons.

Depending on the group of recipients of the information, a differentiated approach must be taken. Depending on the size of the company, it is usually for most employees and, if necessary, for external parties

be sufficient to know that an unnamed person from a specific department has tested positive. Additional information may be useful, such as which days the person was present, which meetings they attended and which community facilities (e.g. canteen, library) they used. Depending on the size of the department, further differentiation according to subordinate organizational units will be possible within the department. Targeted disclosure of identity may be required for individuals who have had direct contact. This applies, for example, to people who share an office room or to those who are likely to have shaken hands. Admissibility then follows from Section 26 (3) BDSG and Article 9 (2) (b) GDPR.

10. Guidance on video conferencing systems

Video conferences have been an integral part of many people's everyday work since March 2020. There are a few points to consider in order to ensure compliance with data protection law.

With the worldwide spread of the infectious disease CO VID-19, more and more workplaces in companies and authorities in Hamburg were switched to working from home. In addition to questions about secure access to company resources, there was a particularly large number of requests for advice on all aspects of video conferencing systems from a data protection perspective. The market for video conferencing services was already extremely diverse before the pandemic development and offered several software solutions for different usage scenarios. It was always immanent to the requests for advice to the HmbBfDI that those responsible were looking for quick and easy-to-use solutions. Recourse to commercial video conferencing providers was therefore quickly and often without intensive

dealing with data protection issues.

Against this background, the HmbBfDI addressed the most important requirements for such systems in a comprehensive FAQ at the beginning of the pandemic and provided those responsible with a solid roadmap for data protection-compliant use.

After a more detailed technical and legal examination of the respective services, it was found that a large number of providers are constantly making fundamental adjustments to their own services and that a clear statement on the data protection-compliant operation and use of the systems is therefore not easy to make and has long-term validity could be hit. Some services changed relevant technical implementations of their services several times within a very short time. The conference of the independent

On October 23, 2020, the data protection supervisory authorities of the federal and state governments published an orientation guide (OH) on the use of video conference systems (https://datenschutz-hamburg.de/assets/pdf/OH-Videokonferenzsysteme.pdf) so that those responsible have a binding Be able to develop guidelines for the introduction and continued operation of the services for yourself. Of the Accompanying OH video conferencing systems is a checklist that summarizes the requirements in a form that can be operationalized and provides even more clarity. The HmbBfDI was actively involved at all levels in the preparation and was also able to assert Hamburg's positioning to a large extent, so that those responsible across Germany now have uniform requirements that must be met. There was also an increasing desire to legally assess specific data protection services and make recommendations. The HmbBfDI has not yet made any individual assessments in this regard, but has requested the measures that can be derived from the OH video conferencing systems in the course of regulatory inspections and in the context of public projects. This is proving difficult in view of the many offers on the market and the technical innovations that are often implemented at short notice.

The HmbBfDI strives to always communicate to the manufacturers the data protection requirements that it believes need to be implemented. Of course, this also includes basic requirements such as data protection through technology design and data protection-friendly default settings.

For a comparative view of different video conferencing systems, reference is made to the information provided by the Berlin Commissioner for Data Protection and Freedom of Information (https://www. pdf). The HmbBfDI agrees with the results contained therein, but at the same time refers to some technically outdated objects of investigation.

In its judgment of July 16, 2020 (Case C-311/18), the European Court of Justice (ECJ) also made a far-reaching decision on the transfer of personal data to the USA - which also takes place in connection with the use of video conferencing systems. After that, a transfer of personal data to a third country can no longer be based on the so-called Privacy Shield. In principle, however, the existing standard contractual clauses of the European Commission can continue to be used. However, it must be checked in each case whether the rights of those affected by the data processing are regulated in the third country at a level of protection comparable to that of the European Union and whether the standard contractual clauses actually apply sufficiently. For data transfers to the USA, for example, the clauses cannot be used without additional measures

will. This in turn requires additional guarantees (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommenda tions_202001_supp ementarymeasurestransferstools_en.pdf).

TESTS III.

1. Checking of files in the security area

During the reporting period, the HmbBfDI complied with its legal obligation to check the anti-terrorist database (ATD) and right-wing extremism database (RED) at both the Hamburg police and the State Office for the Protection of the Constitution (LfV) in Hamburg. In addition, the Hamburg police began checking the CRIME file "Aurelia".

1.1 Mandatory inspection of the RED and ATD at the LKA and LfV

Both the ATD and the RED are a common standardized central file, each of which is different
Federal security authorities as well as the state criminal investigation offices and
of the constitutional protection authorities of the federal states at the Federal Criminal Police Office. While the ATD serves the purpose of investigating or combating international terrorism related to the Federal Republic of Germany (Section 1 (1) Anti-Terrorism Database Act (ATDG), the RED was used for the purpose of investigating or combating violent right-wing extremism, in particular the prevention and prosecution of created criminal offenses with such a background (§ 1 Para. 1 Right-Wing Extremism File Act (REDG)).

services from the areas mentioned are networked and the information is made mutually accessible for the authorities involved. Both the Hamburg police and the LfV Hamburg are obliged to store personal data collected by them in the file in accordance with the provisions of the respective law (cf. § 2 ATDG or REDG). The authority that entered the data is responsible under data protection law for the data stored in the file, namely for the legality of the collection, the admissibility of the input and the correctness and up-to-dateness of the data (cf. § 9 Para. 1 S. 1 REDG or Section 8 (1) sentence 1 ATDG).

The HmbBfDI has to fall within its area of responsibility

An on-site check of these files was carried out by the security authorities on January 23, 2020 (LfV Hamburg) and on January 24, 2020 (Police Hamburg LKA 7 - State Protection Department). In addition to examining the documentation submitted and the technical framework conditions, the storage of individual people in the files was randomly checked for plausibility and consistency. No deficiencies could be identified at either point, so the audit did not lead to any objections: With regard to both files, it was successfully demonstrated and demonstrated to the HmbBfDI that access to the personal data was adequately secured technically and limited in terms of personnel is. In particular, the focus of the technical review was placed on access and access protection and the authorizations of the clerks were traced. The controlled storages were also technically comprehensible. The randomly viewed storages corresponded to the legal requirements of the ATDG and REDG. The HmbBfDI had the requirements or the reason for the storage explained for each file for approx. 10 percent of the storage. Particular attention was paid to ensuring that the file was actively maintained (e.g. the person responsible can keep an eye on the outcome of the proceedings to be expected during ongoing investigations). It was also checked that in so-called free text fields for data subjects, no personal data is entered into the file by the person responsible, the storage of which is not provided for by law.

Similar to the Federal Commissioner for Data Protection and Freedom of Information (BfDI), the HmbBfDI also comes to the conclusion in the course of its examination that other communication channels and forms of cooperation are likely to be more relevant in practice to the work of the security authorities than the ATD and RED file en (cf. BfDI 28th activity report on data protection, p. 52 ff.). The reason for the examination carried out by the HmbBfDI was the legal requirements, which stipulate that the data stock must be checked by the data protection supervisory authority at least every two years

has taken place. In doing so, the legislature has in turn followed the guidelines of the Federal Constitutional Court (BVerfG, judgment of April 24, 2013 – Az. 1 BVR 1215/07). With regard to these files, the highest German court had ruled that, with regard to the weakly structured individual legal protection, the compensatory function of supervisory control is of particular importance if regular controls at appropriate intervals are involved. (BVerfG loc. cit., para. 217). The audit carried out in January 2020 is already the second audit by the HmbBfDI of the files in question at the state authorities mentioned (cf. on previous audits: activity report on data protection 2014/2015, p. 66 and 2016/17, p .26).

Although the BVerfG emphasizes the particular importance of data protection supervision, especially in the case of data processing that is opaque to the citizen, and expressly warns that this special importance should be taken into account when equipping the supervisory authorities (BVerfG loc Due to the lack of staffing, it was not possible to comply with the statutory inspection requirement every two years. Also in view of the ever-increasing

The number of mandatory audits of files and investigative measures to be carried out on a regular basis in the security sector (cf. Section 73 of the law on data processing by the police) already indicates that the HmbBfDI will have difficulties in future to continue to fulfill the statutory audit obligation at least every two years . It is incomprehensible that, despite clear instructions, there has been no increase in personnel in this area and it contradicts the provisions of the Constitutional Court.

1.2 Checking CRIME file Aurelia

During the reporting period, the HmbBfDI also began examining the “Aurelia” file maintained by State Criminal Police Office 71 (state security). This state-owned CRIME file ("Ciminal Research and Investigation Management Software") is used to avert danger, including the preventive fight against criminal offenses

finally extremist and terrorist offenses from the
Areas of politically motivated crime right, left, as well as foreign ideologies and non-assignable politically motivated crime.

The audit by the HmbBfDI started with a first on-site appointment to view the file at the LKA in November 2020. The focus of the ongoing audit is - in addition to the question of adequate access security and logging - on compliance with the deletion, audit and storage periods . It is of particular interest to the HmbBfDI whether the required individual case checks were carried out when the storage was extended. The stored data must be checked after the specified separation test periods have expired to determine whether the searchable storage of the data is still required. An extension of the storage is only possible if there are special reasons in the individual case (cf. § 35 law on data processing by the police).

During the reporting period, the HmbBfDI began to carry out random checks to determine whether, based on viable justifications, the need for further storage to fulfill the tasks is understandable and plausible.

The reason for this audit was that the HmbBfDI had to identify significant deficits in police data processing when examining the CRIME file “Groups and Scene Violence” in the 2016/2017 reporting period and ultimately also lodged a formal complaint with the Ministry of the Interior and Sport (BIS) (cf. HmbBfDI activity report on data protection 2016/17, p. 23 ff.). As part of the complaint, the HmbBfDI made a number of recommendations to the BIS to ensure that the file(s) will be managed in compliance with data protection in the future.

This implementation must also be checked for the CRIME file, which is now being examined.

The HmbBfDI will report on the outcome of the test in the next activity report.

2. Video surveillance Hansaplatz

Since August 2019, Hansaplatz in St. Georg has been under video surveillance by the Hamburg police. In the 2019 reporting period, the HmbBfDI began an extensive review of the admissibility of video surveillance and largely completed this in the current reporting period.

In its 28th activity report for 2019, the HmbBfDI reported in detail on the HmbBfDI's inspection of the Hamburg police's video surveillance of Hansaplatz in St. Georg, which started on August 1, 2019. After an extensive data protection legal examination, the HmbBfDI comes to the conclusion that there are no indications that the prerequisites for video surveillance of Hansaplatz and the directly adjacent streets by the Hamburg police are not met:

In principle, video surveillance without cause interferes with the fundamental rights of all those affected. These are part of a Vi

deodorant surveillance predominantly passers-by and visitors who do not pose any danger and who do not face any danger.
The use of video cameras by the police for the purpose of your

Statutory fulfillment of tasks therefore requires authorization to intervene in the form of a statutory basis. According to Section 18 (3) of the law on data processing by the police, the police may openly monitor publicly accessible streets, paths and squares by means of image transmission in order to prevent criminal offenses and make image recordings of people insofar as street crimes (so-called serious point of street crime) have been committed and facts justify the assumption that the commission of such crimes can also be expected there in the future (so-called open preventive video surveillance). The HmbBfDI is due to the police in Ham

burg case numbers and situation analysis submitted to the conclusion that the monitored area is such a focus of street crime, ie a publicly accessible location ("streets, paths and squares"), which over a longer period of time is significantly more affected by the so-called street crime than the rest of the city. Both the type, number and density of crimes qualify the area in question as a crime focus in the area of the Free and Hanseatic City of Hamburg. During the on-site inspection, the HmbBfDI focused in particular on the question of whether the Hamburg police actually limited video surveillance to publicly accessible places within the meaning of the standard. According to the case law of the Federal Administrative Court (see judgment on video surveillance of the Reeperbahn, judgment of 25.01.2012 - 6 C 9/11, para. 47), the regulation does not authorize the police to video surveillance of buildings, parts of buildings and areas that are publicly accessible are, but do not belong to publicly accessible streets, paths and squares. Monitoring entrance areas, for example, affects the transition to the private area of the people filmed. In this way, movement and visit profiles of those affected can easily be created (judgment on video surveillance Reeperbahn: OVG Hamburg, judgment of June 22, 2010 - 4 Bf 276/07, para. 136).

The much more intensive interventions resulting from this would then no longer be covered by the standard. The HmbBfDI therefore had to check whether the police had ensured that no house entrances and windows of residential and commercial buildings were monitored by aligning the camera accordingly or using technical "pixelation". From a sufficient unrecognizable ma

The HmbBfDI was able to convince itself of this during an on-site inspection at police station 11 on Steindamm. In addition, random tests were carried out to determine that even when the camera is dragged along and the zoom function is activated, the rendering of identity cannot be circumvented. No outliers or incorrect programming could be detected.

The HmbBfDI currently sees a need for improvement in the implementation

technical and organizational measures as part of the design of the statutory logging obligation. In further talks with the Hamburg police, a solution to an automated, audit-proof logging procedure is to be taken.

3. Windows 10 and updates in the FHH

The configuration options provided by Microsoft when using Windows 10 Enterprise to securely prevent the transmission of telemetry data are not sufficient. Additional measures by those responsible are therefore re

At the end of last year, the data protection conference positioned itself in the form of a test scheme for the use of Windows 10, in which those responsible who are already using Windows 10 or intend to do so are able to independently ensure compliance with the legal requirements of the GDPR in their specific case Check and document (https://www.datenschutzkonferenz-on line.de/media/dskb/20190403_positionierung_windows_10.pdf).
The data protection issues relating to the use of Windows 10 continue to concern all data protection supervisory authorities and the need for advice persists in the reporting period. For this reason, a working group of the data protection conference has carried out further investigations into Windows 10 with regard to the telemetry level security (https://www.datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf). As a result and as consequences for those responsible, it can be stated that to prevent the transmission of personal telemetry data when using the Enterprise Edition, the so-called telemetry level security can be used and by means of contractual, technical or organizational measures - for example by filtering the internet

Net access from Windows 10 systems via an appropriate infrastructure - it must be ensured that no transmission of telemetry data to Microsoft takes place. In addition, the data protection conference agreed that Windows 10 should offer the option of disabling telemetry data processing through configuration in all editions offered. The data protection supervisory authorities will hold further discussions with Microsoft on this and on the laboratory tests carried out by the DSK.

At the same time, the FHH also has news on how to use Windows 10 to report. After the HmbBfDI carried out an examination of the Windows 10 versions of the urban configuration used in the past two years, the Senate assured in its statement on the 28th activity report on data protection that “the examination to switch off unwanted telemetry data and potentially remaining data flows is a regular part of the Check before the respective rollout” of Windows 10 updates and has already been carried out accordingly since the update to version 1809. During this year's citywide update to version 1909, the Senate Chancellery and Dataport were unable to provide such a report. When asked in August 2020, the HmbBfDI was informed that no own telemetry tests had been carried out because the corona crisis tied up all capacities, some of which had a high priority, such as securing the VPN infrastructure. In addition, there was still a lack of dedicated staff in the responsible area at Dataport in August. By the end of the reporting period, the HmbBfDI did not have any further information on this when requested, as to when the appointment and the associated activities will be carried out. In view of the fact that the Senate has assured the permanent inclusion of a telemetry and data flow test, the Senate Chancellery's decision not to suspend the rollout process until such a test has been carried out is problematic. Especially for such critical infrastructures should be off

Sufficient staff are available to meet the legal requirements through technical and organizational measures

to ensure adequate security. This also includes a corresponding check before going live. The Senate Chancellery announced that the current planning now includes the beginning of the tests from the 2009 version.

The HmbBfDI will continue to be in dialogue with the stakeholders involved and will advocate a consistent review of legal data protection issues in the FHH rollout process.

4. Coordinated audit of media companies

As part of a coordinated cross-state audit, the HmbBfDI is involved in the website analysis and legal assessment of the online presence of media companies.

In association with a total of 11 German supervisory authorities, the HmbBfDI wrote to the media companies with the widest reach in its area of responsibility in mid-August and, by sending them a comprehensive, coordinated catalog of questions, asked them to comment on the data flows on the websites operated. The examination focuses on web tracking and the use of cookies and comparable technologies.

As early as March 2019, the conference of the independent federal and state data protection authorities (DSK) adopted the guidelines for telemedia providers (https://www.datenschutzkonferenzonline.de/media/oh/20190405_oh_tmg.pdf). Accordingly, for the integration of third-party service providers on the website, in particular with the help of cookies and other tracking mechanisms that make the behavior of users on the Internet comprehensible, as well as for the creation of user profiles, only consent as a legal basis within the meaning of the DSGVO can be considered. Before such processing, ie before Coo

gravel or information stored on the user's end device is read, informed consent must therefore be obtained in the form of a declaration or other clearly confirming action.

The mere continued use of the offer does not constitute consent in this sense. The European supervisory authorities have recorded this in their consent guidelines (Guidelines 05/2020 on consent under Regulation 2016/679, sections 40, 41, https://edpb.europa .eu/sites/edpb/files/files/file1/edpb_gui delines_202005_consent_en.pdf).

Unfortunately, online media do not always meet these requirements, which means that the basic rights and freedoms of users are violated every time they visit a website.
Furthermore, not only the massive advertising tracking of users is objectionable, but also often the lack of transparency and lack of traceability of the data transfer to the respective integrated advertising service provider.

At the HmbBfDI, all media companies with the

Answering our questionnaire reported back. The evaluation and legal analysis is still ongoing and, like the planning of the audit, is being coordinated nationally. In an industry whose products are regularly used across borders, the supervisory authorities involved should make decisions that are as consistent and harmonized as possible.

5. The data hunger of networked devices

Manufacturers of networked devices often use their Internet connection to access the data of the device users. A sufficient legal basis and often more transparency and obtaining consent are required here.

Many manufacturers of Internet-connected devices (eg
music systems, household robots, video or alarm systems) it can rightly be attested that you have the best interests of your customers in mind - their personal data. These are often collected without their knowledge and without sufficient transparency for those affected and used by the manufacturers, for example, to create profiles, for product improvements or for other purposes.

With smartphones and tablets, users have become accustomed to the operating systems transmitting extensive data about the device owner and their usage behavior to the provider's server.
This concept is also being established for Windows in the area of PCs and notebooks (see III 3). In addition, users are increasingly encouraged to use cloud services, which means that even more personal data ends up in the hands of software providers.

With networked devices, users are usually less aware of such a thirst for data. Nevertheless, device users should always try to retain as much sovereignty as possible over their systems and the data stored there. Information on the so-called self-data protection can be found under exactly this search term in search engines. The website of the Federal Office for
Security in Information Technology (BSI): https://www.bsi-fuer buerger.de/ BSIFB/DE/Empfehlungen/ Recommendationen_node.html

The market for electric vehicles shows the practical difficulties encountered in establishing self-determination via one’s own data. The vehicles of the manufacturer Tesla transmit almost every operation of the driver to the server of the manufacturer.
The exact scope or purpose of the data collection by the vehicles is hardly transparent to the owners and drivers. But not only the drivers are monitored - others too
Drivers in traffic or pedestrians walking past a parked Tesla can be victims of digital capture without your knowledge. A study by the "Netzwerk Datenschutzexpertise" took a closer look at the data streams in Tesla vehicles in 2020 and

came to the conclusion, among other things, that the "sentry mode" function, with which Tesla vehicles are supposed to recognize break-in attempts or parking bumps by other vehicles, is not compatible with European legislation. If the guard mode is activated with a parked Tesla, the vehicle continuously and without cause records the surroundings via the cameras installed on all sides Manufacturer's server in the USA. The study can be downloaded here: https://www.netzwerk datenschutzexpertise.de/sites/default/files/gut_2020tesla.pdf

However, surveillance by networked devices is not only increasing on the street; more and more potential spies are also finding their way into private households. You can typically recognize the corresponding devices by the sales attribute “Smart Home”. In previous activity reports, we have already examined the risks of smart TV sets (TB 25, V 17) or digital language assistants (TB 26, III 6 and TB 28, II 16). Computer-controlled variants of classic household and garden appliances such as robotic vacuum cleaners or lawnmowers, which relieve their owners of everyday work, are now becoming increasingly widespread. Here, too, "smart" models are offered that can be operated and controlled remotely via an app. In the course of their daily "work", some of these devices create detailed floor plans of their owners' apartments or premises internally and transmit them to the manufacturer via the Internet. One should therefore consider whether it is really necessary to grant these devices Internet access via the home WLAN.
After all, this opens the door to the manufacturer and possible third parties
a non-visible digital access door to your own apartment or property.

A further further development of a classic household item also ensured Europe-wide activities at the HmbBfDI in 2020. In concrete terms, these were so-called networked loudspeakers. Unlike classic speakers, for the cable

have to be laid across the apartment, the music signal is transmitted by radio. This also makes it possible to play sound in several rooms or outside areas at the same time, because the loudspeakers are networked with each other via WLAN. An app is used to set up and configure such a system and control the music playback, which can be fed directly from streaming services from the Internet if desired. Many systems can also be connected to voice assistance services such as Amazon's Echo ("Alexa") or Google Home.

While some owners of such speakers welcome the smart connection options, there are others who deliberately do not want to connect their devices to the Internet. At one of

For many years, this was not a problem for leading device manufacturers in this area, because the systems could also be operated without Internet access. However, in 2017, the company changed the terms of service. Since then, the speakers can only be set up and used if a revised data protection declaration is accepted in the configuration app and a user account is created with the manufacturer. Furthermore, the device owners should consent to the configuration and usage data being sent to the manufacturer via the Internet on a regular basis.
This unilateral change in the terms of use annoyed the company's existing customers in particular, since they can now only continue to use their devices, which have been freely usable for years, if they connect them to the Internet and register with the manufacturer to register. Accordingly, several complaints were received by the data protection authorities of the EU, including the HmbBfDI.

The data protection authorities first had to clarify which branch of the manufacturer is the main branch in the EU, as this determines the national supervisory authority with primary responsibility. The task fell to the Dutch data protection authority, which opened a hearing against the manufacturer in 2019. The result was published in December 2019 as the so-called

Draft decision notified to the other EU supervisory authorities. In accordance with the provisions of Art. 60 (4) GDPR, there is then a four-week period to lodge an objection, otherwise the draft would become legally binding as a resolution.

The draft decision of the Dutch Data Protection Authority provided for the manufacturer's requirement for a mandatory User account with the manufacturer is not objectionable and the procedure ren, since there are no data protection objections. Among other things, the company followed the argument that side-contractual obligations such as guaranteeing IT security could only be fulfilled on the basis of known customer accounts

Collection of the relevant user data authorized.

This assessment is not shared by the HmbBfDI and other supervisory authorities, especially in Germany. In practice, numerous manufacturers of computers, smartphones or other networked devices provide evidence that IT security and updates can also be guaranteed without the user setting up an account with the manufacturer.

We therefore lodged an objection to the draft decision at the beginning of 2020 and agreed with our Dutch colleagues in February 2020 that they would start investigating the facts at the manufacturer again. For this purpose, in-depth examination questions were jointly developed. There is currently no new version of the draft resolution from the renewed referral.

We will continue to accompany the process, because the question on which the case is based is of a fundamental nature: It must be clarified whether and to what extent a manufacturer of a networked or smart device still collects data from the

Customers may collect and if so, on what legal basis and to what extent.

6. First procedure under Article 65 GDPR

The first dispute settlement procedure according to the GDPR leads to an unsatisfactory result in specific individual cases as well as on a fundamental level.

In the first case since the GDPR came into existence, the European Data Protection Board (EDPB) has gone through a dispute resolution procedure under Art. 65 GDPR, which was based on a supervisory procedure by the Irish Data Protection Authority (IDPC) against the Twitter International Company. The Hamburg Commissioner for Data Protection and Freedom of Information took responsibility for Germany

national lead supervisory authority has a coordinating role
because Twitter has its German headquarters in Hamburg.

The settlement of the dispute was preceded by a procedure pursuant to Art. 60 GDPR, in which the IDPC, as the lead supervisory authority (LSA), submitted a draft decision to the other supervisory authorities in Europe (CSA) concerned, against which a number of objections were lodged. However, the IDPC did not follow these and instead initiated the coherence procedure.

The initial situation consisted of the notification of a protection violation according to Art. 33 DSGVO by the Twitter International Company (TIC) based in Ireland. In the opinion of the IDPC, this was not submitted properly, and in particular not submitted on time. The breach of protection lay in the fact that, due to a program error, accounts set up as private were nevertheless publicly accessible without the user having to do anything. Almost 90,000 European users were affected over a period of several years. As a result, the IDPC as LSA decided for the missed deadline of Art. 33-Mel

tion to impose a fine in the low six-digit range and submitted a corresponding draft resolution.

With the support of other German supervisory authorities, we have lodged an objection to this draft resolution, essentially addressing the following aspects: ÿ First of all, we consider the role of the Twitter International Company as the controller and Twitter Inc. (based in the USA) as the processor to be assessed for questionable. There is much to be said for joint responsibility according to Art.

26 GDPR, which in turn would have been reflected in the overall assessment of the protection violation. ÿ The object of investigation was unnecessarily narrowed by the IDPC. In addition to violations of Art. 33 GDPR, violations of Art. 5, 25 and 32 GDPR can also be considered. ÿ We consider the amount of the proposed fine to be far too low. This is a major violation and a company with a large annual turnover. The proposed amount therefore does not meet the requirements of Art. 84 GDPR. Specifically, an alternative proposal based on the fine concept of the DSK was submitted.

A total of eight CSAs filed objections, some of which touched on overlapping aspects, but overall covered a broad spectrum. The majority of the objections filed were rejected by the IDPC as inadmissible because they did not meet the “relevant and well-founded” criterion. The IDPC countered the content of the other objections and fully adhered to its draft resolution. In such a case, Art. 65 GDPR provides for a referral by the EDSA, which ultimately issues a decision that is binding for the LSA with a two-thirds majority.

Such a decision in this case was made after an extension of the deadline at the beginning of November 2020. The two-thirds majority stipulated in Art. 65 GDPR was narrowly achieved in the first round of voting. Germany voted against the proposed decision. This position was determined in advance as part of a common position in accordance with § 18 BDSG.
Our rejection had the following reasons:

ÿ Significant parts of the objections from Germany were also considered by the EDPB to be not "relevant and justified" within the meaning of Art. 4 (24) GDPR rejected.

ÿ The remaining points in this procedure saw the EDSA unable to come to a decision. This was mainly due to the fact that the material investigation of the case by the LSA revealed significant gaps.

The plenary session could not bring itself to ask the LSA to carry out a follow-up investigation in order to clarify open questions, such as the roles of the companies. ÿ Only the aspect of the amount of the fine was taken up by the EDPB plenum. Here, abstract reference was made to compliance with Art. 84 GDPR without giving the LSA more specific specifications. Although the plenum was able to bring itself to ask the LSA to increase the fine, the binding resolution does not specify a framework for this.

The result is unsatisfactory in several respects. On the one hand, immense effort was put into reaching a binding decision involving all European supervisory authorities. A total of seven meetings lasting several hours by different working groups of the EDPB were required before a decision that was ultimately of little substance was made in another time-consuming plenary session.

This is very inefficient and should not be repeated in this form will. It is to be expected that many more proceedings under Art. 65 will follow. They are an integral and important part of the common and coherent European data protection enforcement.

On the other hand, this decision stipulated an almost complete determination of the object of investigation by the LSA: If the LSA does not address an obvious violation of the GDPR from the outset, there is no opportunity for the other CSA to deal with these aspects within the framework of the consistency procedure to demand, not least because of the tight deadlines according to Art. 65 DSGVO. You would always be ready

The LSA is instructed to respond cooperatively to such requests as part of the cooperation in accordance with Art. 60 GDPR. If it does not do this or refuses to cooperate altogether, the CSA would also be blocked from the dispute settlement procedure.

In this first procedure, the plenary has decided according to Art. 65 GDPR unnecessarily deprived of the opportunity to take a position on key issues relating to the interpretation and application of the GDPR. The result of the procedure contradicts our understanding of one of the central goals of the GDPR, to create a uniform level of data protection throughout the European Economic Area. This can only succeed if the respective LSA and CSA cooperate and define the essential aspects of cross-border data processing together. The LSA has a special role in this, but by no means the sole determining factor. At the latest in the coherence procedure, going it alone should be prevented and inadequate draft decisions by the LSA rejected by the EDSA. It is therefore only to be hoped that the express request of the EDSA to make the exchange of information between the LSA and CSA as close-meshed and the cooperation as constructive as possible during the cooperation process will be honored in the future.

Furthermore, the interpretation of the dispute settlement procedure must not result in the lead authority being able to determine the scope of investigation of violations of the GDPR itself. With its decision in the present procedure, the EDPB disempowers itself and relinquishes independent control of the decision to the lead authority. If this is the standard by which future decisions in the dispute resolution procedure will be reviewed by the EDPB, uniform application of the GDPR in the EU will fall by the wayside. It would then be up to the lead authority to shorten related issues in such a way that there is actually no longer any need for a common procedure at EU level. In this respect, it is necessary to revise the view expressed in the decision of the EDPB for future procedures.

REPORTS IV.

1. Digital sovereignty, developments in the FHH, GAIA-X

Digital sovereignty is becoming increasingly important in political and economic decision-making processes. It can be observed that decision-makers are slowly rethinking and that dependencies and the associated risks are also becoming tangible in practice with a view to decisions such as the ECJ judgment on Schrems II.

Many institutions recognize the risks that arise from dependencies on external service providers, proprietary software systems and cloud applications. Software update cycles are dictated in particular by the manufacturers of operating systems and widespread office applications. The individual users have no control and have to

add dependencies. Implications of an economic nature represent a risk, as do IT security and data protection aspects. For example, the change from on-premise - i.e. self-operated software instances - to increased cloud use

This means that the processes and data flows of the applications are becoming opaque and, for the most part, no longer verifiable for the company's own IT and even more so for the individual user. Contractual guarantees may not go far enough and conflict with the legal requirements of other countries. In order to gain more control over one's own data, a rethink is taking place at several decision-making levels, which can be summarized under the keyword of digital sovereignty.

At the European level, for example, the GAIA-X project has been promoted for a year with the patronage of France and Germany. An architectural standard for a decentralized and federated infrastructure is to be created on which the behavior of different platforms can be regulated. The main focus is on data and its real-time use, the basic usage regulations for this and the data

portability between platforms. Shortly before the activity report went to press, it was reported that Google, Amazon AWS and Palantir would be involved in the launch of GAIA-X. If this is the case, there would be a fear that GAIA-X could by no means be a sovereign European platform, but be dependent on large IT companies from the United States.

The focus group on digital sovereignty of the Federal Ministry for Economic Affairs and Energy defines the term as a partial aspect of general sovereignty and includes self-determination in the digital world. The necessary components are trustworthiness of communication, control over data flows and opportunities for self-determined action. Affected persons can then act digitally confidently if they have comprehensive digital education. According to the assessment of the focus group, the associated build-up of skills also has a positive impact on the economic, scientific and political requirements of digital sovereignty.

In the Free and Hanseatic City of Hamburg, too, the red-green Senate, which has been in office since June 10, 2020, agreed specific measures in the “Strengthening digital sovereignty of the state” section of the coalition agreement that are to be advanced in the legislative period. In particular, “disproportionate dependencies on external consultants and service providers” should be avoided will. The use of open source software products is regarded as a key factor in the transparency and openness of the technologies used, in order to enable verifiability, which is not possible with market-dominant cloud providers without considerable effort.

The Hamburg Commissioner for Data Protection and Freedom of Information expressly welcomes the declarations of intent described and calls on the Senate to do its utmost to adhere to the existing ones Developments within the city, at the municipal IT service provider Dataport and in transnational working groups

participate. He and his speakers are always available to offer advice and will be happy to contribute their expertise to future projects.

There are already concrete developments. With the Phoenix project, Dataport has been offering an office software application since this year that is operated entirely on the basis of open source software components and is available to the Dataport carrier countries for initial tests and in some cases already productively.

According to the coalition agreement, the citizenship administration should first test the Phoenix project as soon as the experiences in the pioneering state of Schleswig-Holstein have been positive.

2. New measure modules of the standard data protection model version 2.0b

Since November 6, 2019, version 2.0 of the Standard Data Protection Model (SDM) published by the Conference of Independent Federal and State Data Protection Authorities (DSK) has offered a fundamentally revised version that now fully covers the legal requirements of the GDPR and with the help of the Guarantee goals systematized.

Since autumn 2020, the reference measures catalogue, which is part of the SDM, has been expanded to include four new modules. The catalog can be used to check for each individual processing whether the legally required "target" of measures corresponds to the "actual" of measures available on site. The SDM and the reference measures catalog also provide a basis for planning and carrying out the data protection-specific certification (Art. 42 GDPR) promoted by the GDPR and the data protection impact assessment required in certain cases (Art. 35 GDPR). The legal requirements of the GDPR

the protection goals are implemented through detailed descriptions within the catalog of reference measures and thus support the transformation of abstract legal requirements

into concrete and directly implementable technical and organizational measures.

In the four new modules of the catalogue, the SDM sub-working group addressed the topics of “storing”, “separating”, “correcting” and “restricting processing” and handed them over to the technology working group for approval. Since this year, the Hamburg Commissioner for Data Protection and Freedom of Information has also been actively involved in the UAG SDM and, together with other supervisory authorities, is responsible for the further development of the modules. The focus here is clearly on the topics that are of overarching relevance in supervisory practice and will therefore support a large number of those responsible and implementing people in their daily work.

Users in practice are always called upon to communicate comments, suggestions for improvement and criticism and thus to contribute to the further development of methods and measures.
The HmbBfDI will continue to work to ensure that the interpretation of the GDPR and the associated requirement for technical and organizational measures are based on a uniform standard. The Standard Data Protection Model sub-working group is doing its part.

3. Digitization of administration - with OZG, eIDAS, service account and Online ID function

Some data protection improvements were anchored. At the same time, the access protection to the service accounts of the FHH still contains a serious defect.

The specifications for the digitization of the administration are formulated in a nutshell in the Online Access Act (OZG). According to this, the federal and state governments are obliged to also offer their administrative services electronically via administrative portals by the end of 2022 at the latest. This means that more than 500 administrative services nationwide must be given digital access. In order for citizens to have easy access if they want to use a service in another federal state, the federal and state governments are also obliged to link their administrative portals to form a portal network. To prepare and coordinate this upcoming nationwide digitization task, the IT Planning Council set up the "eID Strategy" project group, in which the HmbBfDI has long been a representative of the data protection supervisory authorities, in particular for the

technical and organizational questions of data protection is an advisory member.

In the reporting period, the “Guide with recommendations for assigning confidence levels” was updated. Based on the sensitivity of the data processed in the administrative service and the threats and potential damage, a procedure model is described in the handout to assign administrative services to the three different trust levels “low”, “substantial” and “high”.

These three levels are specified throughout the EU in the underlying eIDAS regulation. With these different levels, the technical guidelines of the Federal Office for Safety

In information technology (BSI), there are in particular specific requirements and technical procedures for the “identification” processes of those affected and for the “authentication” of those affected. An example: According to the relevant Technical Guideline TR-03107-1 of the BSI, you can only achieve the lower level of trust with an authentication method that is based solely on user ID and password. Although this

In the German and English versions of the eIDAS regulation, this level was clearly designated as “Nieder” or “low”.

referred to as "normal" in the handout as well as in the technical guidelines. Even if the specification of a user ID and password as the sole basis for authentication is very widespread, the frequent reports about the misuse of access data and hacking into web portals also show very drastically that with these features only the level "low" can be achieved. A higher level can only be achieved with a so-called 2-factor authentication. A second factor is used in the authentication process, eg a software certificate or, for the “high” trust level, a hardware factor, such as the online ID function of the ID card. To the data subject and the person responsible for

The HmbBfDI has advocated adopting the terminology from the EU regulation in order to transparently show the administrative services to be digitized that the low level of trust in user IDs and passwords. The "wording" and the integration of secure means of authentication belong together. This has also been taken up in the handout.

Unfortunately, this update is still missing in the technical guidelines of the BSI, although two guidelines, TR-03160-1 and -2, were also discussed intensively in the eID strategy project group.

The TR-03160-1 of the BSI also stipulates features that must at least be stored in the service accounts with which those affected can access the digital administration services via the administration portals. The legal basis here is also the eIDAS regulation and the OZG.
Especially when the means for the authentication method is changed, it is important to ensure that unauthorized persons cannot gain access to sensitive personal data by changing. The draft of the Technical Guideline initially provided for a process in which only part of the available data was to be used. However, especially with people who were born in big cities like Hamburg or Berlin, it is not possible to have a high level of trust

It must be ensured that only the maiden name, the date of birth and the place of birth lead to a clear assignment.
From the point of view of the HmbBfDI, not all of the specifications of the eIDAS implementation provisions were initially taken into account to a sufficient extent if the “high” level of trust is to be achieved, which is available in particular with the online identification function of the identity card. Since identity cards are only valid for a limited period of 10 years, they must be renewed when they expire. Here, the suggestion of the data protection supervisory authorities was taken up, with which a change of the identity card is now also possible with a simultaneous change of name and address in the vast majority of cases
can be done online.

In the next step, these uniform nationwide requirements must be implemented in the service accounts of the federal states and the federal government, taking into account the legal and technical requirements. In Hamburg, this essentially took place with the switch to the online service infrastructure (OSI); a digitization platform for public administration. This service portal is available to citizens, organizations and authorities to register or log in to their own service account. Even though OSI is supposed to stand for "open, secure and innovative", the HmbBfDI had to determine during an initial check that the requirements for a high level of trust are not yet being implemented. For example, not all characteristics are stored to ensure the requirements of the eIDAS regulation. Another serious shortcoming is that an existing service account, which the user with the online identification function of his ID card on Ver

trust level "high", can be taken over with just a user ID and password and the online ID function of any other ID card. An example: An unauthorized person logs on at a low level of trust with only a user ID and password. With this first step, there is still no access to sensitive data in the mailbox

require a high level of trust. But with just a few clicks, this unauthorized person can activate any ID card as access authorization at the “high” level of trust for the existing service account and exchange it for the ID card of the authorized user. When the identity card is exchanged in this way, there is currently no comparison of the data from the old and the new identity card. This could result in an unauthorized person using this second step to gain access to sensitive content stored in the service account mailbox. This lack of access protection needs to be addressed immediately before beginning the service account interoperability pilot, which is currently planned for the first quarter of 2021.

4. Program check of a certification program

Since the GDPR came into force, companies and authorities have been able to go through a data protection accreditation process with the participation of the data protection supervisory authorities. The upstream approval process represents the assessment of a certification program.

To prepare for accreditation, the certification body or the program owner must draw up a certification program and have it checked for suitability by the German Accreditation Body (DAkkS) in accordance with DIN EN ISO/IEC 17011 (cf.
DAkkS rule 71 SD 0016). An essential part of the certification program is the certification criteria for the implementation of data protection requirements, which must be approved by the responsible data protection supervisory authority in accordance with Article 57 (1) (n) GDPR in conjunction with Article 42 (5) GDPR (https:/ / www.datenschutzkonferenz-online.

de/media/ah/20180828_ah_DIN17065-Ergaenzungen-full-V10-final_V3_DSK.pdf).

As one of the first data protection supervisory authorities in Germany, the HmbBfDI has submitted an application for approval for such a certification program with regard to products and services in accordance with the GDPR. As part of the procedure, the HmbBfDI is guided by criteria jointly developed by the federal and state supervisory authorities, the publication of which is planned for the beginning of next year. The paper, which is well advanced but not yet finalized, specifies the requirements of the supervisory authorities for certification programs and is intended in particular to ensure a consistent test standard for all German supervisory authorities.

The very extensive documents submitted by the applicant are currently being checked by the HmbBfDI. As soon as the submitted program has been approved, it will be possible to use it within the framework of specific certifications for specific data processing operations. In this way, a higher standard of trust in the area of data can be gradually achieved in the future
protection.

If applicants want to act as certification bodies themselves and issue certificates, they must be additionally accredited by DakkS. According to § 39 BDSG, the accreditation is carried out jointly by the supervisory authorities and the DakkS. The supervisory authorities assume the role of expert appraisal as specialists in the area of data protection accreditation procedures. At the HmbBfDI have several employees and employees
go through assessor training and are trained to work with the DakkS system assessors to authorize them to act as a certification body.

As a rule, authorization is granted after an examination lasting several days at the on-site certification body. In doing so, both

the systematic requirements, such as the presence of sufficiently qualified personnel or the guarantee of objectivity, as well as data protection-specific requirements are assessed. Both the accreditation procedure and the procedure for approving the certification criteria are associated with a considerable amount of testing, for which the 3rd

December 2019 new fee facts with data protection

Fee schedule available (https://datenschutz-hamburg.de/as sets/pdf/DSGebO.pdf).

5. International Traffic after Schrems II

In its groundbreaking judgment, the European Court of Justice called for a fundamental about-face in the practice of third-country transfers. To enforce its requirements, the HmbBfDI is coordinating a nationwide testing campaign.

In its decision of July 6, 2020, the European Court of Justice (ECJ) declared widespread measures for data transmission to third countries to be insufficient. From now on, no personal data may be sent to the USA on the basis of the EU-US Privacy Shield. If official mass surveillance takes place without cause in countries outside the EEA, the standard contractual clauses of the European Union are no longer a suitable basis as long as their protective effect is not supplemented by individually appropriate additional measures. The judgment is very clear in its aim. The court makes it clear that there must be no “business as usual” in international data traffic.

Regarding the question left open in the judgement, which additional measures are possible in order to continue to use the standard contractual clauses

the European Data Protection Board has published the much-noticed Recommendations 01/2020. In it, the Committee spoke out against any risk-based approach. In countries with extensive secret service mass surveillance, it must be expected that even seemingly irrelevant data will be collected by the authorities and linked with other information to form an overall profile.

If personal data is to be transferred to such third countries, it is therefore of great importance that it is completely protected from official use there. In practice, this can usually only be guaranteed through anonymization, effective encryption and, under certain circumstances, pseudonymization. Many previous business models are therefore no longer possible without changing the technical or location-political design.

The ECJ has emphatically recognized the role of the data protection authorities clarified. If they receive corresponding complaints from data subjects, they must “suspend or prohibit” all transfers that are inadmissible according to the standards set out above. There is therefore no leeway for the goal to be achieved when processing complaints. The way in which a suspension of the transfer can be achieved is at the discretion of the relevant competent authority. In the knowledge that a switch from tools that have been used for years and are integrated into the operational process can cause great difficulties for those responsible in individual cases, the HmbBfDI first enters into a dialogue with companies about which a corresponding complaint has been made. If efforts that have already started are shown and convincing concepts for creating a lawful situation are presented, orders by way of ordinance can often be dispensed with. The question of how much time is allowed for changing a service provider or implementing additional protection measures depends on the circumstances of the individual case. Among other things, it can be important whether a service has been established by the person responsible for some time or

only introduced after the ECJ decision. It is also relevant whether the system is essential for the continued existence of a company and whether it is easy to switch to alternative European providers.

In order to avoid market distortions and to give the court's decision broad effect, the HmbBfDI does not limit itself to pursuing individual complaints. On his initiative, the data protection conference

Task force set up to carry out cross-border random sampling. Under the leadership of the HmbBfDI, software services were jointly identified that are widespread in Germany and are typically handled by involving external service providers from third countries. At the beginning of 2021, the participating authorities will approach bodies in their area of responsibility that have reason to believe that they use such services. This is done using jointly developed questionnaires and letters.

The handling of the violations identified should also be coordinated. However, the uniqueness of each case will have to be taken into account individually.

6. 101 complaints from the organization NOYB

In August, the non-governmental organization NOYB filed 101 complaints against companies based in the EU and EEA with the relevant supervisory authorities. Two of these complaints fall within the area of responsibility of the HmbBfDI.

The subject of the complaints is the data transfer by the responsible companies to the USA as a so-called third country by using the Google Analytics or Facebook Connect services

on their websites and thereby transmit personal data to the USA. Until the decision of the ECJ of July 16, 2020, C-311/18 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doc lang=DE&mode=req&dir=&occ=first&part=1, Schrems II), such data transfers could be based on the Privacy Shield. With the above judgment, which declared the corresponding adequacy decision of the EU Commission to be invalid, transmission based on the Privacy Shield is no longer possible and must therefore be discontinued.

The Privacy Shield was declared invalid by the CJEU because, according to the court, US law does not offer a level of protection that is essentially equivalent to that in the EU. US law, to which the ECJ referred in its decision, concerns e.g. B. the intelligence gathering powers according to Section 702 FISA and Executive Order 12 333. (https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_ schrems2.pdf)

At the same time, the ECJ determined that Commission Decision 2010/87/EC on Standard Contractual Clauses (SCC) is still valid in principle. In doing so, the ECJ emphasized the responsibility of the controller and the recipient to assess whether the rights of the data subjects enjoy an equivalent level of protection in the third country as in the Union. Only then can a decision be made as to whether the guarantees from the standard contractual clauses can be implemented in practice and which additional measures can be taken

to ensure a level of protection essentially equivalent to that in the EU. Although Google has publicly announced in the meantime that it will be switching from Privacy Shield to standard contractual clauses, we are currently not aware of any additional measures that would ensure a sufficient level of data protection when transferring data to third countries.

Since NOYB's 101 complaints relate to the responsibility of supervisory authorities in many European countries and due to the fact that the content of the complaints is identical, the European Data Protection Board (EDPB) set up a task force. It is intended to support the supervisory authorities in ensuring that the approach to the entire complaints handling process is as harmonized as possible.

Using a questionnaire developed and agreed by the task force, the companies responsible for the area of responsibility of the HmbBfDI were written to and asked to comment on the transfer of personal data to third countries. No response has been received as the comment period is still running.

7. Google search engine – new jurisdiction of the BGH

Search results in the Google search engine are often the subject of complaints from those affected when Google LLC has refused to be delisted. As part of its responsibility as the supervisory authority, the HmbBfDI examines whether Google LLC should be ordered to be delisted.

If a person concerned submits an application for delisting to Google LLC against a search result for their name and the latter rejects the delisting, a complaint can be lodged with the HmbBfDI. Within the scope of its responsibility (see also IV. 8), the HmbBfDI examines whether the requirements for a delisting claim are met and, if it accepts this, hears Google LLC on the facts. After the company has checked it again, search results are often blocked as a result. If this is not done, the HmbBfDI checks whether the

listing to the company is to be ordered by the authorities.

In its decision, the HmbBfDI takes into account the so-called Right to be forgotten Case law issued in particular by the European Court of Justice (ECJ), the Federal Constitutional Court (BVerfG) and the Federal Court of Justice (BGH) (see also 28. TB IV. 5). In 2020, the BGH gave up the case law it had developed in 2018 - before the GDPR came into force. According to this, a search engine operator only had to list a search result if it was obvious and obvious at first glance
recognizable violation of rights by the person concerned. Rather, according to the BGH, the fundamental rights of the person concerned must be weighed up on an equal footing with those of the content provider, the search engine operator, the users of the search engine and the public (VI ZR 405/18).

For further questions, the BGH appealed to the ECJ as part of a preliminary ruling (VI ZR 476/18). On the one hand, this concerns the question of how to deal with factual claims in search results, the truth of which the person concerned disputes. Here, the ECJ is to clarify whether the search engine operator has to consider whether it would be reasonable for the person concerned to first take action against the content provider and have the untruthfulness of the allegations determined by a court when weighing up fundamental rights. Another question referred is whether, when considering whether photos of those affected may be displayed as preview images in the search engine, the remaining content of the website on which the image is published should also be taken into account.

The HmbBfDI's assessment of complaints against the non-deletion of search results has always been confirmed in previous decisions by the Hamburg Administrative Court (VG) and the Hamburg Higher Administrative Court (OVG). There are currently six lawsuits against the HmbBfDI before the Hamburg Administrative Court

pending - three of them from 2020 - in which the plaintiffs seek to oblige the HmbBfDI to order Google LLC to remove search results (as of December 31, 2020).
Two of the lawsuits filed in 2019 were withdrawn by the plaintiffs. In a seventh pending lawsuit, the plaintiff seeks the issuance of subpoenas against Google relating to (negative) reviews in its company profile displayed on Google. The Administrative Court of Hamburg already rejected a simultaneous application for a temporary injunction against the HmbBfDI due to the lack of urgency.

8. The concept of the "head office" – ambiguity at the expense of the protection of fundamental rights

The definition of "head office" in the General Data Protection Regulation (GDPR) leaves room for interpretation. At the same time, the regulation lacks powerful mechanisms to resolve different legal views between supervisory authorities in a meaningful way. In order to avoid gaps in legal protection, the HmbBfDI must redefine its responsibilities.

The head office of a controller is defined in Art. 4 No. 16 a) GDPR. Accordingly, this is the branch that represents the "head office" of the person responsible, unless the purposes and means of the processing are determined in another branch. What exactly constitutes the "main administration" is not explained further in the legal text. The question therefore arises as to whether the head office can be freely determined by a company. The relevant commentary literature clearly rejects this idea. At the very least, it is necessary for a "head office" that the head office forms an organizational focus of the business. It should with that

find it difficult to relocate key management structures between member states on a regular basis in order to secure supervision from the appropriate authority.

Since the introduction of the GDPR, the HmbBfDI has had to deal with the question of the main office. Although some large technology companies such as Google have their German headquarters in Hamburg, they often have a central administration in other European countries. For this reason, in order to process many complaints, it is necessary to cooperate with other supervisory authorities in accordance with the procedures of the
Art. 60ff. DSGVO is carried out. Cooperation with the Irish supervisory authority, the IDPC, has not yet reached the level that would be desirable for smooth cooperation.

As part of corporate restructuring at the beginning of 2019, Google transferred responsibility for Google services in the European Economic Area – with a few exceptions – to Google Ireland Limited. The areas excluded from this change, which continue to be managed by Google LLC in the USA, have led to difficulties in cooperation between the supervisory authorities. Even before the restructuring, Google LLC declared Google Ireland Limited to be its main office. Based on this working hypothesis, the HmbBfDI has always sought cooperation with the IDPC as the lead supervisory authority.

In the Activity Report Data Protection 2019, the HmbBfDI reported, among other things, on court proceedings before the Hamburg Higher Administrative Court (see 28. TB, IV. 5.). In these proceedings, the court assumed that there were many arguments for the existence of a main office in Ireland - not least because of the submission by Google itself.

However, the IDPC did accept a relevant appeal

rejected since the structural changes in 2019, with the reference that there is no jurisdiction for complaints against Google LLC in Ireland. Other European supervisory authorities have also followed this path and have not recognized the status of Google Ireland Limited as a head office. One of the reasons given for this was that Google Ireland Limited did not adequately control the purposes and means of data processing.

The HmbBfDI not found among the European supervisory authorities. At the same time, there are no mechanisms in the GDPR to make such questions binding on the basis of individual complaints and individual persons responsible

to be clarified by the supervisory authorities. The European Data Protection Committee, which as a body is actually suitable for clarifying fundamental issues, had already refused to deal with "individual cases" in the past.

The HmbBfDI therefore had to deal with the fact that the IDPC, which was deemed responsible, refused to process the complaints with reference to its lack of responsibility. There is a risk of a critical gap in legal protection if all supervisory authorities reject their own responsibility for those affected and refer to a different one. Clarification at the judicial level could at best be carried out by those affected themselves. To make matters worse, they would have to sue the respective supervisory authorities in other European countries to process the complaints - an expensive undertaking, which individuals are often powerless to face.

In order to ensure meaningful processing of disputed complaints

guarantee, the HmbBfDI must also reconsider its position on the question of a main office. It is not in the interests of those affected that complaints are lost in the jungle of responsibilities. The situation must therefore not arise in which a company places itself in the sphere of influence of a supervisory authority

withdraws, but denies any monitoring responsibility. From these points of view, the HmbBfDI will assume that it is responsible for the lack of a main office.

LEGALLY BINDING ORDERS AND FINES

IN.

1. Introduction to the topic of orders and fines

The HmbBfDI has complied with the change in penal practice ordered by the legislature. A fines office was created in the reporting period. Violations were increasingly punished with fines.

With the General Data Protection Regulation (GDPR), the European standard-setter has not only given the supervisory authorities powerful tools to punish violations of data protection regulations with effective fines in the future. Through the overall construction of the GDPR, he has also made it clear that the expectation is placed on supervisory authorities that fines are no longer the exception. Rather, violations should be remedied and punished, which can also be done with fines. After the GDPR came into effect, it still took some time before violations that fell within the scope of the GDPR were ready for a decision at the HmbBfDI. In the meantime, however, this is the case and has fundamentally changed the work of the HmbBfDI. First of all, the fact that the fine was to lose its exceptional character meant that a fine office had to be set up at the HmbBfDI, which is responsible for punishing data protection violations with fines. If the specialist departments have finally clarified a case and they consider the imposition of a fine to be appropriate, the fines are handed over to the fines office (the legal department), which then conducts the necessary hearings and then imposes the fines.

The requirement to change the way the supervisory authorities work was implemented by the HmbBfDI in its day-to-day work and resulted in 25 fine proceedings being opened in 2020 alone. Fines have already been imposed in 18 cases. There are also fines in three cases that were opened in 2019. Only two proceedings have been discontinued, five others are still ongoing. It is therefore to be noted that the

The HmbBfDI implemented the change in penalties that was expected and ordered by the legislature.

The cases on which the individual OWi procedures are based reflect the work of the HmbBfDI very well. At one end of the spectrum, there are simple cases that keep coming up, such as the insufficient data protection-compliant handling of collected contact data in the catering trade according to the HmbSARS-CoV-2 Containment Ordinance or the personally motivated - and therefore Impermissible – querying of data from police databases by police officers. On the other end

The scale includes individual cases that involve massive data protection violations of a considerable extent and are punishable with fines in the millions. Below we provide an overview of some notable cases.

2. H&M

In the case of several hundred employees of the H&M service center in Nuremberg being monitored by the center management, the HmbBfDI was fined approx. 35.3 million euros against H&M Hennes & Mauritz Online Shop AB & Co. KG for violating data protection regulations. The decision is final.

H&M Hennes & Mauritz Online Shop AB & Co. KG based in Hamburg operates a service center in Nuremberg. Since at least 2014, some of the employees have had extensive recordings of their private living conditions. Corresponding notes were saved permanently on a network drive.

After vacation and illness absences - even short ones - the superior team leaders held a so-called Welcome Back Talk. After these talks, in a number of cases not only specific holiday experiences of the employees were

ten, but also symptoms and diagnoses. In addition, some supervisors acquired a wide range of knowledge about the private life of their employees through one-on-one and hallway talks, ranging from rather harmless details to family problems and re
religious confessions was enough. Some of the findings were recorded, stored digitally and could sometimes be read by up to 50 other managers throughout the company. The recordings were sometimes made with a high level of detail and updated over time. In addition to a meticulous evaluation of the individual work performance, the data collected in this way was used, among other things, to obtain a profile of the employees for measures and decisions in the employment relationship. The combination of investigating their private lives and constantly recording what they were doing led to a particularly intensive encroachment on the rights of those affected.

The data collection became known because the notes were accessible company-wide for a few hours as a result of a configuration error in October 2019. After the HmbBfDI was informed about the data collection through press reports, it first ordered the content of the network drive to be completely "frozen" and then demanded its release. The company complied and presented a data set of around 60 gigabytes for evaluation. After analyzing the data, interviews with numerous witnesses confirmed the documented practices.

The discovery of the significant violations has prompted those responsible to take various remedial actions. A comprehensive concept was presented to the HmbBfDI as to how data protection is to be implemented at the Nuremberg location from now on. In dealing with past events, the company management not only expressly apologized to those affected. She also followed the suggestion to unbureaucratically pay the employees a considerable amount of damages.
In this respect, it was an unprecedented commitment to corporate responsibility after a data protection violation.

Other components of the newly introduced data protection concept include a newly appointed data protection coordinator, monthly data protection status updates, increased communication of whistleblower protection and a consistent information concept.

3. Clearview AI

The US company Clearview AI Inc. hit the headlines worldwide at the beginning of 2020 with its facial recognition app. A complaint gave the HmbBfDI reason to open administrative proceedings against the person responsible.

At the beginning of 2020, numerous media reports revealed that Clearview AI Inc., based in New York, had created a huge database in recent years. According to media reports, this should contain billions of photos of faces. With her face recognition app, the person responsible for registered users offers a search engine which, when a face photo is presented, displays all publicly available photos of this person or of people who are biometrically similar to them. This is done in each case including the indication of the source, for example from public profiles in social networks or from images taken from company websites. The search query is triggered by uploading a photo in the app and, by comparing it with a biometric profile, provides a hit list of photos that come closest to the uploaded template. In addition, on its homepage, Clearview AI offers those affected the opportunity to obtain information about the data concerning them or to delete this data from the company database allow. It provides the appropriate forms for this purpose.

Not only the media made the HmbBfDI sit up and take notice, it soon received a complaint from an affected person. This complaint was preceded by information obtained from the person concerned as described above. He actually found photos of himself and others in the information

He suggested that people who appeared similar to the algorithm were hits on his uploaded photo and then turned to the HmbBfDI, assuming that the data processing was unlawful.

On March 19, 2020, the HmbBfDI sent its first letter to the those responsible, which contained a comprehensive catalog of questions. The HmbBfDI wanted to know, among other things, where the responsible party took the data from, for what purpose and whether the data subjects found out in the context of the information which app user had already inquired about them. Although the person responsible responded to this letter in a timely manner, she hardly responded to the questions from the HmbBfDI. She vaguely described the processing operations and also referred to the alleged non-applicability of the GDPR. The HmbBfDI resolutely opposes this view. In this case, the HmbBfDI sees the territorial scope of the GDPR as open to Art. 3 Para. 2 b) GDPR and assumes its own responsibility. Art. 3 Para. 2 b) GDPR opens up a wide area of application. The wording of Art. 3 Para. 2 GDPR only requires the connection of data processing with the circumstances mentioned and thus includes subsequent data processing in the consideration. This involves an observation of their behavior insofar as the users of the app can recognize the private and professional contexts in which a person concerned appears with photos, provided this takes place in the Union.

The intention of the legislature, the high level of protection of data subjects in the Union against data processing, speaks in favor of a broad interpretation to be guaranteed by a responsible person based exclusively in the third country. This protection is necessary here in view of the mass, indiscriminate data processing by Clearview and the factual impossibility of asserting the rights of data subjects in the USA against app users (US American law enforcement authorities, companies, etc.).

In addition, it can be assumed that the data processing for the vast majority of the data covered by the GDPR is unlawful.

Biometric processing falls under the special protection of Art. 9 GDPR. In this case, the data subject will regularly not consent to the processing of biometric data in accordance with Art. 9 (1) GDPR. The photos of those affected may initially have obviously been made public, for example if a profile picture from a social network was deliberately made public, so that the exception of Art. 9 Para. 2 e) GDPR could be considered here. In any case, the subsequent biometric processing of the photos for the creation of the database, which can only take place with the consent of the person concerned, would have to be taken into account.

The second letter from the HmbBfDI of May 26th, 2020 was only evasively answered, so that on August 14th, 2020 he finally issued an information request notification, which provided for a fine of 10,000 euros per question for failure to provide the required information. Clearview AI Inc. has meanwhile adequately addressed the questions. The HmbBfDI is now examining further steps within the scope of its remedial powers.

4. We see

The HmbBfDI already reported on the Videmo process in the last activity report (28th TB 2019, Chapter IV 3). The background to the process is the use of software for automated facials
detection during the investigation into riots in connection with protests against the G20 summit in Hamburg in summer 2017. This software is called Videmo. For their use by the Hamburg police, a database with a growing volume of initially 17 terabytes was created, in which private recordings uploaded to the police by citizens, police video surveillance material and material from public transport and the media - a total of approx 32,000 video and image files (as of August 2018) – have been incorporated.

The HmbBfDI is of the opinion that there is no sufficient legal basis for the use of the software and has therefore vis-à-vis the

Police ordered the deletion of a so-called template database, ie a database containing all the faces in the video surveillance material converted into mathematical models. The deletion order therefore did not relate to the video material itself, but to the large-scale biometric data processing of all, mostly completely uninvolved, persons depicted in the video material. The police brought an action against this and was successful in doing so before the Hamburg Administrative Court.

The HmbBfDI already announced in the last activity report that it intends to appeal against this decision. This was also implemented. The HmbBfDI applied for the approval of the appeal in good time, which was expressly ruled out by the administrative court.

To the surprise of all those involved in the proceedings and also the public, the police complied with the order and deleted the template database. According to the police, this was done for reasons of necessity: there was no longer any need to use the template database.

On the one hand, it is gratifying that the template database has been deleted and that there is no longer any interference with the data protection rights of thousands of irreproachable citizens, for whom the HmbBfDI clearly lacks a suitable legal basis. On the other hand, from the point of view of legal clarity, it is problematic that the police want to end the legal dispute prematurely. She assumes that the OVG Hamburg should not allow the appeal and that the judgment of the first instance would thus be unassailable. This would mean that it would no longer be possible for the OVG to review the order in court.

The fundamental questions that this case raises for the practice of the investigating authorities and for the protection of masses of uninvolved persons would ultimately remain open for the future.

To the regret of the HmbBfDI, however, the OVG Hamburg did not come to a decision in the reporting period, although the first instance

Judgment was made in November 2019. As a result, the procedural question of allowing the appeal has remained undecided so far.

This situation is unsatisfactory for everyone involved. The police have obtained a successful verdict which they do not know whether it will stand. The HmbBfDI is confronted with statements from the Hamburg Administrative Court after it is not allowed to check whether there is a legal basis for sovereign data processing at all. Years later, thousands of citizens are still unclear as to whether their biometric data was processed correctly or not.

The HmbBfDI hopes to be able to report on a clarifying factual decision in the next activity report.

5. Police inquiries: overview of the procedures

During the reporting period, the HmbBfDI completed a total of eight administrative offense proceedings (OWi proceedings) against police officers who had unlawfully processed data.

In two cases police officers had data from them

Ads used to establish contact with the person filing the complaint, which was aimed at initiating a private relationship.
This problem is known from other federal states and is not limited to the police.

Misconduct of this kind sometimes also occurs with the Corona contact details. With regard to the police, there is the special feature that they act with sovereign powers and the complainants therefore felt particularly harassed. The HmbBfDI has punished this with fines of 300 to 400 euros. There were also cases in which the complainants initially started contacting

agreed and only then about the behavior of the police

Temporary officers complained when the relationship did not meet their expectations. In these cases we have refrained from prosecution.

In another case, a total of three police officers took photos of an official presentation that contained personal data and shared them in a WhatsApp group. This was illegal and the HmbBfDI also imposed fines of 300 to 400 euros.

In three other cases, police officers are closed

data queries from police databases were carried out for various private purposes. It was about queries about ex-partners and neighbors. The cases differ in terms of

the frequency of data queries and were fined between 400 and 600 euros.

All of these cases were reported to the HmbBfDI by the police

permanent position brought to the display. Among other things, there were also notifications of the initiation of an OWi procedure with regard to so-called self-interrogations, ie the retrieval of one's own data from police databases. This is not permitted and constitutes a violation of police service regulations, but it is not a violation of data protection law.

The victim of a data protection breach can never be the same as the perpetrator. Also in the case of violations within the framework of a service

There is no possibility of sanctions under data protection law if we act. If a police officer processes data for official purposes for which he is not authorized, he or she is not acting as a private individual. The GDPR then does not apply, and according to Section 24 (3) HmbDSG there is no possibility of imposing fines on authorities and public bodies for the actions of authorities. However, this does not mean that such violations go unpunished. In this case, the police officers can, within the framework of Dis

be held responsible for disciplinary proceedings.

In all cases, the police officers have the

Fines accepted and no appeal lodged. Following the OWi procedure, the HmbBfDI sends the files to the Dis

disciplinary office of the police, which then decides on the basis of the investigations by the HmbBfDI and the fines imposed whether there is still a so-called disciplinary backlog. If the fine does not adequately sanction what has happened from a service and disciplinary point of view, the police can impose a disciplinary measure following the fine, which can be, for example, a reprimand, another fine, a reduction in salary, a demotion or, in the worst case This can even lead to removal from the civil service.

6. File storage of a clinic in Büren – patient data protection with significant gaps

According to the Hamburg courts, the storage of patient files in a former hospital does not constitute data processing. This has prevented the HmbBfDI from enforcing effective protective measures for a comprehensive file archive. It is uncertain how this gap in legal protection will be closed.

A hospital operating company in Büren (NRW) filed for bankruptcy in April 2010, and the clinic was closed in October of the same year. In 2011, the insolvency administrator returned the hospital property to a real estate company that is a 100% subsidiary of the hospital group, which also owned the hospital operating company in Büren. After the cessation of operations in the clinic, the treatment documentation (patient files) kept in paper form remained in two basement rooms that were also originally intended for storing the files. The hospital building was empty in the period that followed and was temporarily

looked after by different caretakers.

In May 2020, a Youtuber entered the former hospital building, including the two file rooms in the basement, and came across the patient files that had been left behind. The video published about this caused a wide response in the media and complaints about data protection from former patients. The HmbBfDI immediately tried to get the Hamburg-based parent company to back up the patient files appropriately. This failed not least because of the refusal attitude of the clinic group. The latter merely replied by pointing out that the HmbBfDI had no local responsibility from his point of view.

As a result, the HmbBfDI issued an order with which the real estate company was instructed to adequately secure the documents and to ensure the fulfillment of data protection claims for information. The order was declared immediately enforceable, while the real estate company sought legal protection from the Hamburg Administrative Court.

The court granted the application by decision of July 30, 2020 (17 E 2756/20). In justification, it essentially stated that the term "processing" according to the definition contained in Art. 4 No. 2 GDPR refers to any process or series of processes in connection with personal data, such as collection, recording, storage, etc. The mere Presence of files in the building

decomplex does not fall under the requirements of the term data processing. The term “process” indicates that processing does not describe a state, but an action, i.e. the change in a state. Processing requires the transition from one state to another.

The HmbBfDI considers this legal opinion to be problematic. It withdraws the personal data in the form of patient files from data protection law because the previous processor went bankrupt.

As a result, this leads to a state of irresponsibility under data protection law in the sense that there is no longer a person responsible and inquiries from former patients come to nothing.
They simply no longer need to be answered.

Since the VG Hamburg has broken new legal ground with this legal opinion, the HmbBfDI lodged a complaint with the OVG Hamburg. However, with a decision of October 15, 2020 (5 Bs 152/20), the OVG Hamburg confirmed the opinion of the administrative court.
The decision does not contain any noteworthy considerations of its own, but follows the statements of the Hamburg Administrative Court.

Even if this legal opinion is regrettable from the point of view of the HmbBfDI and tears gaps in protection for the fundamental right to data protection that are difficult to justify, it was clear that the HmbBfDI could not assert its opposing view, since a further complaint is not provided for by law. The HmbBfDI therefore lifted the order and informed the city of Büren that the courts were preventing them from enforcing data protection requirements.

The decisions of the Hamburg administrative courts were critically discussed in the legal trade press. It remains to be seen whether this view will prevail. In any case, this would be a not insignificant step backwards for the protection of personal data and the rights of patients.

7. Illegal Video Surveillance of employees

Video surveillance of employees without suspicion is not permitted. The HmbBfDI sanctions such violations with a fine. The assessment of the fine is based on the principle of proportionality. In one case, the special circumstances of the corona pandemic were taken into account.

A company operates several restaurants in Hamburg. Six video surveillance cameras were installed and in operation in one of these branches. The camera images were recorded in real time
drawn and stored for 72 hours. Management stated that the purpose was to prevent theft. According to the findings of the HmbBfDI, half of the cameras were primarily used to monitor the employees. This happened on an unacceptable scale.

These three cameras have the front during business hours
filmed the sales area as well as the kitchen and cold storage of the branch.
The cold storage was only partially recorded. Any thefts could hardly have been solved with the documented camera setting. All that was recorded was who entered the cold storage room and when. Even the suitability of this documentation for investigating or preventing property crimes seems questionable, since goods have to be constantly removed from a refrigerated warehouse during operation. Above all, there have been no thefts of goods since the company took over the branch. The recording was much more preventive. It may have had a certain deterrent effect. However, it had to be taken into account that not only the cold store was recorded, but also other areas of the company in which employees stayed permanently.

The encroachment on the rights of employees associated with the recording was significant. This applies even more to the other two cameras that recorded the kitchen and the sales area. It was simply not clear what legitimate purpose the recording should serve. The kitchen area, which under normal circumstances is used exclusively by employees, was filmed. These were recorded completely in their daily work without any reason for this. The company did not report regular misconduct by employees, nor were there any indications of other matters worthy of protection. The employees got colder in the kitchen and in the preparation area

Meals are constantly monitored without being able to escape at least part of the video recording. According to the case law of the Federal Labor Court, permanent, suspicion-independent video surveillance of employees is disproportionate and therefore inadmissible (BAG, decision of 29.6.2004 - 1 ABR 21/03, para. 23, BAG, judgment of 28.3.2019 - 8 AZR 421/17, paragraph 39). The video surveillance seriously interfered with the general personal rights of employees. These were subjected to constant monitoring pressure.

For the HmbBfDI, the imposition of a fine therefore seemed inevitable. However, when calculating the fine, it was not just the fact that the company had shown itself to be cooperative that had to be taken into account. In addition, the company's sales had almost halved as a result of the corona pandemic
a negative result was expected for the financial year. Under these circumstances, the fine was to be calculated moderately. Last but not least, the imposition of the fine was intended to protect employees. It would not have been in their interest to impose a fine that would have put the company at risk of insolvency. The HmbBfDI has therefore decided on a fine of 3,000 euros. This has been accepted by the company.

8. Location information in images from a fetish portal

If a photo upload function is provided online on the website, the metadata such as GPS data must be cleaned up. Otherwise, in a sensitive context, this metadata could be used by unauthorized third parties with malicious intent.

The HmbBfDI has a fine against a company

issued, which operates an online marketplace for used underwear in particular. The shop is aimed at customers who are interested in purchasing underwear that has been worn for different lengths of time and has a correspondingly intense odor.

The company advertises that it guarantees 100% anonymity.

The reason for opening the fine proceedings was a tip from a concerned citizen who provided the HmbBfDI with numerous GPS coordinates of users of the platform.

A check revealed that the residual information or metadata in the uploaded photos had not been cleaned up.
As a result, the data could be entered into any map service and the exact location at which the photo was taken could be determined. Sometimes there was additional height information in the images
noted, which allow a rough statement about the floor inhabited at the moment of recording.

The number of persons affected amounted to during the control period approx. 760 women between 18 and 50 years. On the amateur recording men, those affected are shown in their underwear. The face is also visible in some photos.

The person responsible is obliged to be able to prove that he has taken suitable technical and organizational measures to protect against data protection violations, measured against the risk (Articles 24 and 32 GDPR). In addition, Art. 25 GDPR requires data protection to be taken into account through data protection-friendly technology design ("privacy by design") and default settings ("privacy by default"). In addition to the sensitivity of the processing, the benchmark for the appropriate level of protection of the measures to be taken is also the state of the art.

An upload function for images has been standard in current web technologies for years. The platform has the service

specifically in the fact that registered users take photos of underwear and the like. can upload. Mostly were used to take the photos Smartphones or other mobile devices or digital cameras are used. It is often a standard setting that the camera apps of the smartphones or GPS modules of the cameras save not only the actual image but also additional information in the image file, the so-called Exchangeable Image File Format (EXIF data).
Using this EXIF data, a fairly precise localization is possible, which can be associated with a high security and confidentiality risk. This type of information has been used in more and more devices with optical sensors since the standard was first published in 1995 and can now be found in virtually all smartphones and tablets with cameras and digital camera systems. This EXIF data can contain various metadata, including the GPS data (location information) in the image file.

As a specification of the state of the art for the field of Data security is provided by the Federal Office for Security in the In information technology (BSI) has the IT baseline protection compendium ready. There, general "standard requirements" are recorded that correspond to the state of the art. According to the findings of the BSI and the conviction of the HmbBfDI, the cleaning of EXIF data as residual information in a photo upload is also one of the standard requirements for online shop platforms that provide a photo upload. According to this, all uploaded images must be completely stripped of their metadata before the images are available to the actual service and can be viewed publicly.

Some of this GPS data is personal data within the meaning of Art. 4 No. 1 Alt. 2 GDPR. For personal reference, it is sufficient if the person concerned can be identified, i.e. if a relationship can be established between the information and the person through a number of further processing steps or through additional knowledge. at

Due to the large number of non-cleansed photos with location data, it was possible to identify several affected persons with relatively little effort within the framework of a random sample. Entering the coordinates and additional research using search engines enabled the data subject to be identified. In one case, in addition to the residential address, additional information such as the cell phone number could also be accessed.

Due to the contextually sexual orientation of the platform alone, there were high risks of possible stalking or discrimination, which could have led to physical – for example through the feared violent crimes – but also to material (dismissal) or immaterial damage (damage to reputation, discrimination). . The latter was to be feared if, for example, it was made public that a person concerned had offered their underwear, which they had worn for weeks and therefore had a strong smell, for sale on a platform by providing their address and, if applicable, their name.

Finally, the data was transmitted or disclosed without authorization, which also constitutes a violation of Article 6(1) in conjunction with Article 5(1)(a) GDPR. Disclosure represents processing within the meaning of Art. 4 No. 2 GDPR, for which a concrete legal basis was required. Decisive for a disclosure to a third party is the notification, which is the case with an image upload on the Internet, if a third party actually retrieves this data.
In the present case, numerous GPS data were retrieved, at least by the whistleblower himself. The cause of the described handling of metadata was a misconfigured add-on of the content management system used.

The defect has been remedied so that the metadata is now automatically cleaned up by the system. The HmbBfDI imposed a small fine in view of the company's low turnover. No appeal was lodged against the fine and the fine was paid.

9. Lack of agreement after Article 26 GDPR

If several companies belonging to the same group of companies run a customer database, they are jointly responsible for the processing. This requires an agreement in accordance with Art. 26 GDPR. The lack of such an agreement was sanctioned with a fine.

A company that offers adult education courses is affiliated with several other companies with similar affiliations
offered to the same parent company. The later complainant had booked and attended a course with one of the companies, but had not paid the course fees incurred.
Some time later he registered for a course at another company in the group and was rejected there. The reason he was given was that he still had arrears with the company whose courses he had already attended. In response to his complaint, the HmbBfDI examined the companies
and discovered that these companies used a common database. When a customer books a course, it is listed in the database under a single customer number from that point on. The administrations of the affiliated companies can use the customer number to see whether and in which other courses of the affiliated companies the customer has already taken part and whether there are arrears with affiliated companies.

It is questionable whether such a procedure is permissible, after all, the GDPR does not recognize any corporate privilege according to which data can be freely exchanged between companies in a corporate group. However, it is undisputed that the management of a joint customer database by several legally independent companies leads to joint responsibility in accordance with Article 26 GDPR.

Pursuant to Art. 26 (2) GDPR, this requires an agreement that duly reflects the respective actual functions and relationships of the jointly responsible persons towards data subjects. However, there was no such thing, which is why the HmbBfDI imposed a fine of 13,000 euros.

10. "Private" Third Party Recordings

The creation of photos and videos of strangers falls within the scope of the GDPR. The household exception of Art. 2 Para. 2 lit c) GDPR does not apply, since it is not an exclusively personal activity.
Recordings made illegally can be sanctioned with a fine.

Recordings that private individuals take with their mobile phones or digital cameras on the street of strangers to whom they have no connection represent a much larger part of the work of the HmbBfDI than was to be expected. It always comes
again that people film each other. Even if the filmed person does not agree, this can be justified because there is a legitimate interest, for example if there is a dispute with threats on the street after a traffic accident. Then the making of records is related to the leave and is often also permissible. If, on the other hand, there is no contact whatsoever between the filming person and the person being filmed, and if the recordings are specifically about the person being filmed, i.e. if this person is not just an accessory to a street scene, for example, then the taking of recordings is not permitted. The motivation for such recordings, about which complaints are submitted to the HmbBfDI, is often of a sexual nature.

In the reporting period, the HmbBfDI had various such
Follow up complaints: So had a taxi driver on the street

photographed young people who were strangers to him and saved these recordings in a folder that had a very high proportion of pornographic recordings. In another case, a man is said to be on a district festival specifically filmed children who were there with their parents to celebrate. In the Wohlerspark in Altona, a man secretly filmed young women who were sunbathing there, lightly dressed. In the Europapassage, a man followed a family and continuously and purposefully filmed the family's underage daughter. Complaints keep coming in because women are filmed in their private parts under their skirts. In the summer of 2020, legislators declared “upskirting” a criminal offense under Section 184k of the Criminal Code. According to this norm, however, no offenses can be punished that were committed before the change in the law came into effect.

These cases are regularly referred to the HmbBfDI by the police and the Hamburg public prosecutor's office. The success of the measure often depends on the investigative work of the police. If they reacted quickly, secured the instrument used in the crime and, above all, the recordings made with it, such cases can usually be closed with fines. In one case, the defender of the film maker objected that the HmbBfDI was not allowed to impose a fine on this. The making of such recordings is an "exclusively personal or family activity" which according to Art. 2 Para. 2 lit c) GDPR does not fall within the scope of data protection law. Since the HmbBfDI had to obtain a judicial confirmation of the confiscation of the mobile phone by the police anyway, this was a good opportunity to have this question clarified in court.

As was to be expected, the responsible investigating judge of the AG Hamburg did not follow the argumentation of the defense counsel. In a decision of July 3, 2020 (163 Gs 656/20), the court stated with pleasing clarity: "The person concerned understands this regulation [meaning the household exception according to Art. 2 Para. 2 lit c) DSGVO] clearly wrong, if he were to conclude

that he is free at any time to arbitrarily take photographs of people he doesn't know in public." Strangers who move around in public could not be "pulled" into the private sphere of the person by taking photographs for personal purposes. who takes such photos.

The applicability of data protection law does not result automatically to an inadmissibility of filming. However, such recordings, which are based on sexual motivation, lack a legal basis. The recordings are then illegal and the HmbBfDI punishes this accordingly.

WE. CONSULTATIONS AND PRIVACY COMMUNICATION

1. Mail encryption at General Social Service

The pilot for the general social service was successfully carried out in the summer of 2020. However, the further introduction process for comprehensive use in the ASD is still open.

The communication between the General Social Service (ASD) and the external bodies continues to run without content encryption of the sometimes highly sensitive data of the children and young people cared for. But there is at least one intermediate step in the plan to achieve data protection-compliant transmission. In a conversation between the management of the social authority and the HmbBfDI in January 2020, ver
agreed to carry out a pilot in the ASD with the technology that was already being considered in 2018, the so-called Governikus MultiMessenger (GMM).

function mailboxes there are stored in the GMM. On the other hand, two external bodies have also implemented their certificates there as an example. In the summer of 2020, the piloting of mail encryption in an ASD office was successfully completed. At the end of August 2020, the steering group for this pilot project unanimously voted in favor of starting the roll-out with the technology used.

The piloting showed that it was important to burden the administration with the necessary technical processes as little as possible. Dataport carried out these necessary preparatory tasks on behalf of the pilot. The guidelines for ASD employees are also to be improved on the basis of experience from the pilot project. The long-announced integration of address books in the GMM in 2021 can also contribute to increasing user-friendliness.

At the same time, experience from the pilot showed that the external bodies also needed more information. In particular, handouts can be used for this, such as how the external bodies can save the certificates in the GMM and in their own mail systems and which processes in mail traffic with the ASD will change
the. By providing information to the external bodies at an early stage, they can adapt to the necessary adjustments to the IT systems, possibly with the involvement of their IT service provider.

Despite the clear vote from the steering group for piloting, the social security authority was not able to complete its internal need for clarification for a roll-out project for mail encryption at the ASD by the time this activity report went to press. Whether and how the roll-out will continue in 2021 is still open three years after the examination of the HmbBfDI in the ASD of the Wandsbek district office.

2. Aid Digital

*The billing process for benefit data via the "Digital Subsidy" includes the processing of sensitive employee health data to a large extent. Regarding the according
Art. 32 Para. 1 GDPR no agreement has yet been reached with the ZPD.*

While the processing processes of the central aid office of the Free and Hanseatic City of Hamburg (FHH) at the Center for Personnel Services (ZPD) are already largely digital, those entitled to aid have so far only been able to submit their applications and the associated documents (such as doctor and medication bills) by means of a written application . This should change. In addition to the classic written application, those entitled to aid should not only be given the opportunity to submit their application for aid to the ZPD digitally, but via

You can also use the same portal to submit reimbursement applications to your private health insurance company (PKV). The project "Beihilfe Digital" was used for this purpose, which the HmbBfDI has been supporting since the end of 2018.

In cooperation with ZPD, Dataport, CompuGroup Medical Mobile GmbH (CGM) and the provider MGS Meine Gesundheit Services GmbH (MGS), its app “My medical bill”, which is already used by some private health insurers, was adapted accordingly. The use of these systems is based on separate usage agreements with MGS and CGM. Use is voluntary for those entitled to assistance.

Those entitled to benefits can take pictures of their medical bills and other receipts with their smartphones, upload them to the app and, in the future, send them to their PKV (if they are an affiliated partner) and to their benefits office. Transmission between the connected partners is encrypted for transport, and the app provider does not have access to the uploaded invoices.

Users can retrieve and manage the uploaded receipts without any time limit. Delivery of notifications via the app is planned for a later expansion stage.

The HmbBfDI has pointed out from the beginning that particularly if the user and thus also potential attackers can access the submitted data or if feedback/notices are to be sent to the user in this way, an identification appropriate to the high level of protection cation and authentication process is to be provided.

There is an agreement with the ZPD that the data of employees, pension recipients and their relatives, which is processed as part of the processing of benefits, is subject to a high level of protection.

The ZPD's current solution provides for the user to create a user account when registering online for the "My doctor's bill" app by providing a user name (valid e-mail address). The user access ("CGM LIFE Key") required for use and the user account ("CGM LIFE Account") are in turn offered by CGM and set up during online registration.

In the further registration process, the beneficiary will be asked to enter his personnel number and his date of birth for identification. If the comparison of the data entered matches the personnel master data stored at the ZPD, a letter with a personal activation code is sent to the employee's private postal address currently stored at the ZPD.

The second authentication factor is the use of an authenticator app (TOTP procedure; time-limited one-time passwords) that the user can freely select. After installing the app and receiving the code letter, the user can complete the registration by entering the code. Authentication then takes place each time you log on to the app with the access data user ID and password and a one-time password generated by the authenticator app to the ZPD.

While the data protection documents submitted to the HmbBfDI also presented the planned integration of the online ID function of the electronic ID card and the prospect of the process going live in March 2020 was announced for the end of 2020, implementation has not yet taken place has taken place and is no longer intended by the ZPD.

Articles 32 and 25 GDPR determine which technical measures are required for data security, including the authentication of users. The state of the art is to be considered here
view. The HmbBfDI already sent the ZPD in May 2020 in a

informed in a detailed statement that due to the high risks, an authentication process using a hardware token – such as the new ID card or other RFID-enabled cards – is required. This is the only way to ensure that the extensively processed health data is sufficiently safe from an accident
rightful retrieval are protected. The continued use of the procedure currently provided by the ZPD using one-time passwords would only be possible for a period up to the end of 2022
concretely named prerequisites: On the one hand, this includes taking concrete steps to immediately implement an authentication process using a hardware token. On the other hand, the users must be informed about the remaining risks of the procedure with the one-time passwords
and agree to such a solution.

With the Patient Data Protection Act of October 14, 2020, which was heavily criticized by the data protection supervisory authorities, the federal legislature has also standardized the access conditions with which those affected can access their sensitive health data. These are redefined in § 336 SGB V. The comprehensive implementation of § 336 SGB V will shape the state of the art in an area that is comparable in content to the aid app.
The new regulation allows those affected to access their health data under certain circumstances by means of a soft
waretokens, like a one-time password. At the same time, however, it makes it clear that the option of a hardware token must be offered and that the person concerned has a right to choose. In addition, § 336 SGB V nF expressly states that the person concerned must be informed of the special features of access if access is not secured by a hardware token. The person concerned must expressly agree to this solution in advance if he or she wishes to use it.

The HmbBfDI will continue to advocate for a secure solution for the assistance app, where those affected can choose between the two authentication methods.

3. Video Conferencing Systems during the apprenticeship

The use of video conferencing systems to conduct courses and to monitor students writing exams entails various data protection problems and should be carefully considered by the responsible bodies.

Due to the restrictions in public life caused by the SARS-CoV-2 virus, face-to-face courses at public and private universities were only possible to a limited extent, so that courses were held with the help of digital video conference systems and some exams were taken digitally by the students at their private ones terminals were written at home.

The subsequent questions to the Hamburg Commissioner for Data Protection and Freedom of Information regarding the processing of the students' personal data used in this context showed in particular the importance of the information obligations under Articles 12 and 13 of the General Data Protection Regulation (GDPR) or under Article 4 No. 11 GDPR (as the basis for consent).

The Bucerius Law School (BLS), for example, had the final exams of the spring trimester written by the students in the form of distance exams in the period from March 16, 2020 to March 31, 2020.

In order to prevent attempts at deception, the use of the digital video conferencing service of Zoom Inc. (Zoom) was stipulated for the writing of distance exams. The BLS used Zoom as so-called "software as a service", so that the video conference service was used via the Zoom servers. In order to take part in the video conferences, the participants had to go through a registration process.

run, whereby it was left open for the students to register for the video conference for the exam via an app to be installed by the service provider Zoom or via its website.

The data protection required under Articles 12 and 13 GDPR
The university did not initially give the students any information. It

Due to a lack of information, the nature and scope of the processing of their personal data in the context of video surveillance during the exam remained unclear for the students. In particular, it was not clear which data was processed exactly, where this data was stored and which functions of the video conference service were to be used. It should be borne in mind that at that time Zoom had functions such as so-called attention tracking, which raised serious doubts about the admissibility of the associated processing of special categories of personal data pursuant to Art.

Art. 9 GDPR brought with it. There was also a recording function, although it was not clear to the students, due to a lack of sufficient information, whether a recording should be made by the BLS and where this recording should be saved. It was also unclear whether adequate organizational and technical measures had been taken to prevent the use of these additional functions.

The BLS also gave no indication of configuration options to protect privacy, such as the use of filters to make the private background unrecognizable in the video image.

The students saw each other through the use of video technology

an insight into their private rooms and thus into their privacy, without being able to foresee the type and scope of the data processing and the existence of appropriate technical protective measures. This example shows: The use of digital technologies through initially unmanageable functions without which he

required information according to Art. 12 and 13 GDPR makes data processing a black box process. Transparency and information are essential for those affected to protect their basic rights and not just a mere formalism.

By intervention of the HmbBfDI were in the course of further theft
surphase issued data protection notices for the first time, but these were incomplete compared to the content requirements of Art. 13 Para. 1 and 2 GDPR. It explained in a fragmentary way about the processing of image and sound data, the purposes pursued and a lack of storage. Only after further complaints did the BLS finally issue another revised version of the data protection information to the students.

Comparable problems were also found when using digital ones
Video conferencing services in the individual departments of the university
tät Hamburg to hold courses. A lack of data protection notices also led to inquiries from students at the HmbBfDI.

A lack of information from the students made the existence of a legal basis for the processing of their personal data appear doubtful. Both the BLS and the university

Hamburg also relied on consent in accordance with Art. 6 Paragraph 1 Sentence 1 No. 1 GDPR as the legal basis for the processing of student data. According to Art. 4 No. 11 DSGVO, it is mandatory to clarify the type and scope of data processing, since only then can a declaration of consent be given "in an informed manner", which was not the case in the present cases.

Further open data protection issues remained, such as the existence of joint responsibility according to Art.
26 GDPR with regard to metadata processing during the use of a digital service by the students or when they register for a video conference via the homepage of a provider of the digital service used. The subsequent question of the suitability of the digital services commissioned by the universities as processors could not be resolved either.

The BLS, for example, has refrained from monitoring exams via Zoom, and to the knowledge of the HmbBfDI continues to use this service to hold courses. Here it will have to be examined to what extent the decision of the European Court of Justice

of July 16, 2020 (Case C-311/18, Schrems II) can have an impact on the data protection-compliant use of Zoom at the BLS.

The problem of the existence of a joint responsibility according to Art. 26 GDPR in relation to the processing of metadata of students and the transmission of personal data of students to processors in third countries within the meaning of Art. 44 et seq to set a self-operated authority for data protection-compliant teaching.

With a so-called “on-premise” solution, video conferencing services can be operated by the universities on their own servers, provided the service provider actually offers this solution, so that a connection to a third country within the meaning of Art. 44 et seq. GDPR can be ruled out. The registration processes for a video conference can also be designed in this way in such a way that the students do not necessarily have to go to the homepage of a service provider to register and can thus avoid the collection and transfer of their metadata. The entire area of the use of video conferencing systems in university teaching should in future be given clear legal regulations that create structures that are as uniform and legally secure as possible for students, lecturers, but also for the responsible bodies.

4. Representation of countries' regulators at EU level

In the current reporting year, the HmbBfDI held the position of state representative on the European Data Protection Board. This role resulted in a number of additional responsibilities.

Confirmed by the conference of the independent supervisory authorities of the federal and state governments (DSK), the HmbBfDI continued to be the second representative in the EDSA alongside the BfDI. More than two and a half years since the GDPR came into force, there is still none

This state representative is formally elected by the Bundesrat, as provided for in Section 17 of the Federal Data Protection Act.

Due to Corona, the frequency of meetings of the EDPB increased significantly. In some cases, virtual meetings took place on a weekly basis via the European Parliament's video conference infrastructure, which could be used for this purpose. The Schrems II decision of the ECJ and the abolition of the Privacy Shield (see IV 6) and the first decision of the EDPB according to Art. 65 GDPR (see III 6) brought the committee additional items on the agenda.

At a total of 27 meetings in 2020, ten public guidelines and a number of other papers, some of which were internal, were approved. Germany, with its large number of supervisory
authorities heavily involved. The Hamburg Commissioner for Data Protection and Freedom of Information alone contributed to the achievement of the following results through collaboration or leadership: ÿ Guidelines 08/2020 on the targeting of social media users (main rapporteur together with ULD in the Social Media Subgroup) ÿ Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 (support for the country representative in the Enforcement Subgroup) ÿ Internal Document "EDPB Guidance on its plenary minutes" (main rapporteur together with the Secretariat of the EDPB) ÿ Internal Document on how to deal with complaints relating to data protection infringements started before the entry into application of GDPR that continue after 25 May 2018 (Principal rapporteur)

In addition, further guidelines are being worked on with the participation of the HmbBfDI.

In addition to the routine tasks such as preparing meetings with the other country colleagues and writing reports, these activities have taken up considerable resources. It's not just about doing justice to our self-image as an authority with a strong European connection. Rather, only active participation enables content control and pre

ment of the results, which is only possible to a very limited extent in the last step of the formal decision-making in the EDPB plenary.

The HmbBfDI has represented the data protection supervisory authorities of the countries at European level since 2015. Until 2018, representation took place at the level of the predecessor body, the so-called Art. 29 Working Group, and then within the framework of the European Data Protection Board. The latter was created by the General Data Protection Regulation as an independent EU legal body with its own rights and obligations. Many hopes associated with the implementation of the EDPB have not been fulfilled since then. The body, which consists of the supervisory authorities of all member states and the European Data Protection Supervisor, is cumbersome and has so far not done justice to its task as a decision-making body for questions of legal enforcement in cross-border data processing. The reasons for this are manifold and can ultimately be traced back to legislative deficits or misjudgments.

Essential questions, such as a pan-European concept of fines or a speedy determination of the main offices of data processing companies, are still open. In the future, the body will only be able to fulfill its tasks effectively if priorities are set more clearly and national interests are taken back to a greater extent when the authorities involved make decisions related to law enforcement.

5. Press and Public Relations

The year 2020 brought a new record in terms of the number of press inquiries - the HmbBfDI received around 400 corresponding entries. This high was due in particular to data protection aspects relating to Corona, but also to issues such as the ECJ judgment on Schrems II or the fine proceedings against H&M.

The trend, which has been observed for a long time, of a constantly increasing number of inquiries from the press and the media on a wide variety of data protection topics continues unabated. In the report In 2020, the main reason for this is the corona pandemic. Numerous inquiries addressed the recording of Corona guest lists, the misuse of the data and the use of video communication systems in the education sector due to the pandemic. Furthermore, the ECJ judgment in the Schrems II proceedings with the suspension of the Privacy Shield and the fine proceedings of the HmbBfDI against H&M were responsible for numerous press inquiries.

Other important topics included the case of unsecured patient files from a former hospital in Büren and a notice of access to information against the US company Clearview AI, a provider of a facial recognition app. As in previous years, the HmbBfDI has received numerous inquiries from foreign media about such cross-border topics.

With regard to local Hamburg data protection issues, the above-mentioned fine proceedings against H&M, which also attracted international attention, should be mentioned in the first place. Furthermore, there were new developments with regard to the administrative court proceedings on VIDEMO regarding the issue of the admission of an appeal and the deletion of the biometric database. Finally, the topic of data Hamburg police computer mentioned without official reason.

On the occasion of the second anniversary of the GDPR, statistical inquiries about the number of complaints, data breaches and sanctions reached the HmbBfDI again. In addition, the media was interested in the GDPR evaluation report of the EU Commission and for fundamental questions about cross-border data processing and the consistency procedure in the European Data Protection Board.

In the 2020 reporting period, the HmbBfDI received a total of 398 press inquiries, which is around 20% more than in 2019 (332).

On average, around 33 inquiries per month were processed in the 2020 reporting year.

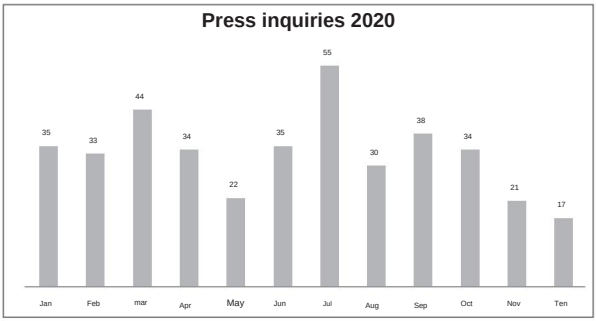


Fig. 1: Monthly press inquiries in 2020 marked as “special events”

As Fig. 1 shows, July stands out with a peak in inquiries for the recording of the Corona guest lists and the ECJ decision on Schrems II. With regard to the two Internet companies Facebook and Google, it can be said that inquiries have fallen significantly, from around 26% of the total number of inquiries in 2019 to just around 8% in 2020. Of the two companies, Facebook (5%) ahead of Google (3%).

With a view to the local origin of the inquiring media, it can again be stated that by far the most inquiries come from national media. Inquiries from foreign media increased significantly in 2020 due to topics that were also perceived internationally, such as the H&M fine, the ECJ decision on Schrems II or questions about the EDPB, as the following table shows:

Press inquiries...	2019	2020
regional media: national	75	107
media:	212	219
foreign media:	45	72
In total:	332	398

Table 1: Press inquiries to the HmbBfDI 2019 and 2020

Apart from this Activity Report Data Protection 2020, there were no further publications in the print area in the reporting year. The Internet offer of the HmbBfDI is constantly being further developed. In the reporting period, the HmbBfDI has 25 press releases lungs published.

In addition, the Hamburg data protection officer and some employees of the authority again gave lectures and presentations on aspects of the GDPR and various topics of data protection and took part in rounds of talks or panel discussions. Due to Corona, these events mostly took place as video conferences. As part of the data protection and media competence promotion of the HmbBfDI, there was also participation in numerous corresponding events (see VI 6 for details).

6. Media education

Promoting data protection skills is also one of the core tasks of data protection authorities, because young people's ability to protect themselves against possible risks in the digital world must be strengthened. Data protection is not just law enforcement and the enactment of fines and administrative orders.

On February 11, 2020, Safer Internet Day took place under the motto "Together for a better Internet". Together with other partners (Hamburg/Schleswig-Holstein media authority (MA HSH), Hamburg police, Blinde Kuh eV association and Hamburg books halls), the HmbBfDI took part in a day of action on the subject of “Internet security and data protection”. A wide range of information could be offered through close cooperation between the various institutions. The HmbBfDI informed large and small visitors how playful a safe

and still create a password that is easy to remember.

At the beginning of 2020, the range of information offered by the HmbBfDI was also expanded. The website https://datenschutzhamburg.de/medienbildung now contains extensive media education information for children and young people, parents and those with legal guardianship, as well as educators. The HmbBfDI constantly provides new information there and gives tips and tricks for safe use of the internet.

The corona pandemic has relentlessly shown that many German schools are lagging behind when it comes to digitization. There is often a lack of a functioning digital school infrastructure, the appropriate teaching-learning concepts and up-to-date training for prospective teachers. Even if funds are drained from the Digital Pact School and schools in Hamburg are equipped with digital devices, there is still a lot to be done. This backlog was clearly noticeable at the beginning of this year during the corona-related closures of the schools. Since there was neither a strategy nor a corresponding concept for exclusively digital distance learning, many schools used various solutions and products without sufficiently considering data protection issues. This led to numerous submissions and complaints to the HmbBfDI (see Chapter II 5.

"Video conferencing systems in school lessons").

The highly emotional debate on e-schooling reached a climax with the (false) report that the HmbBfDI would ban Skype for distance learning. As early as 2019, the HmbBfDI called for a contact point for pedagogical staff, but also for head teachers, where they can get advice, information, further training and security (preferably locally) on legal issues. Alternatively, it would be conceivable for the responsible body to make more information material and guidelines available in order to reduce uncertainties.

In addition, it became clear that even more had to be invested in teaching and further training opportunities for teachers. A recent study shows that only 40 percent of all current teacher training students feel well prepared for the digital challenges of their later everyday work (https://studitemps.de/magazin/frauen-fuehlen-sich-durch-studium-weni ger-gut -prepared-for-digitization-as-men-%e2%80%92-brandenburg-universities-are-pioneers/). It is therefore important that media education and the associated basic legal knowledge are already integrated into the training of prospective teachers, but of course also of educators and other educational professionals. The demands that the HmbBfDI already formulated in its last activity report for the education system (cf. 28th TB 2019, Chapter V 11) are therefore by no means losing their importance and topicality.

Nevertheless, it must be acknowledged at this point that some demands - partly due to the massive pressure to digitize - could be implemented this year. For example, funds were released that will further advance the expansion of the digital (school) infrastructure and equipping the teachers with digital devices. The latter is also to be welcomed from a data protection point of view. The Hamburger Medienpass is also being revised and updated. The mandatory modular teaching units on digitization also include a module on the subject of “social media and data protection”.

At the beginning of the year, the HmbBfDI was also able to hold workshops at schools and other educational institutions. The aim of these workshops is to reduce any uncertainties and to promote the skills of the participants in relation to handling personal data and privacy. Media education is considered one of the key disciplines in an increasingly complex mediatized world ("Media education as a key discipline in a mediatized world. Perspectives from theory, empiricism and practice" in MedienPädagogik volume 37). Fostering these 21-century skills (More

more here: https://www.oecd.org/site/educeri21st/40756908.pdf) is essential for educators, but also for children and young people. Only with this knowledge can children and young people be prepared for the world of tomorrow. Of course, many workshops and training courses by schools and institutions of open child and youth work (OKJA) were also canceled at the HmbBfDI due to the corona-related restrictions. This development is completely understandable. It is nevertheless important, even after the pandemic, not to return to the status quo ante, but also to teach media skills in school. Happily, since the end of this year, the HmbBfDI has been receiving an increasing number of inquiries about data protection workshops and training courses.

For the promotion of data protection competence in schools, the HmbBfDI supported the production of the FWU school film project “Data protection – rules and rights in the online world” as specialist advice. The school film is aimed at young people and explains the social relevance of data protection for the target group. The HmbBfDI also created in cooperation with a didactic

Specialist advisor for learning materials tailored to the film. The film, including the accompanying materials, will be freely accessible from next year in all school libraries in the federal states that have a cooperation with the FWU.

In order to impart the diverse "21-century skills", an institutional opening of schools with extracurricular learning venues and institutions is essential. Open child and youth work can also be one of these places of learning. Together with the Eimsbüttel district office, the HmbBfDI has therefore launched a project that supports educators in designing their own media competence projects that are practical and target group-oriented. At the end of the project period, various tried and tested project concepts are available, which can then be passed on to other institutions.

Together with the school authority, the authority for culture and Me

dien (BKM), the authority for work, health, social affairs, family and integration (social authority), the Hamburg media network and other partners, a draft of a monitoring system and a fund for the Promotion of media skills developed. With the Media Competence Fund, a program is available through which media education projects can be funded. It is now a matter of showing political will, recognizing the importance of media education and providing the fund with the appropriate financial resources. The same also applies to media competence measures that have already been established.

Parents are regarded as the most important supporters of children's learning ("Learning at home" by the Telekom Foundation from 2020, page 40). It is therefore essential to invest more and more in media education for parents. "ElternMedienLotse" is an established media education measure. "ElternMedienLotse" is a measure funded by the school and social authorities, in which adults are trained to organize media education parents' evenings. It could be argued that this is a classic task for teachers represent teachers. However, many teachers do not currently have the appropriate qualifications to inform parents about new, constantly changing media phenomena and to advise them on media-pedagogical issues (see: E-Government Monitor 2020 – Digital services of general interest – Education). The sponsor of the "ElternMedienLotse" measure, the non-profit Hamburg citizen and training channel TIDE, will revise the "ElternMedienLotse" concept in 2021 with a view to the great relevance of media-pedagogical work with parents.

In the future, the training should be modular and current media events and developments should be integrated in a targeted manner. The HmbBfDI will accompany TIDE in this process and provide content-related support for issues relating to data protection. This process requires financial planning security that extends beyond one-year periods in order to make offers reliable and effective. The HmbBfDI is committed to this.

VII. INFORMATION ON PUBLIC ACTIVITIES

1. Facts and figures

The incoming numbers at the HmbBfDI were not only consistently high in 2020, but in some cases new highs were reached again. So have the HmbBfDI in the reporting period

raum reached a total of 3,900 written submissions, which is 261 more than in 2019 and 2,281 (minus IFG submissions) more than in 2017 before the GDPR came into force. The HmbBfDI understands the term “written receipts” to mean, in particular, written data protection complaints and requests for advice, but also requests for information addressed to the HmbBfDI as the person responsible within the meaning of the GDPR or as the body responsible for providing information under the Hamburg Transparency Act (HmbTG) and requests for advice on freedom of information. Since the exact specification is made by the responsible specialist consultants, it always takes a certain amount of time before all inputs have been statistically evaluated. This is the reason why at the time this activity report went to press, only 3,698 (around 95%) of the entries had been evaluated. The figures listed below are extrapolations made for better comparability.

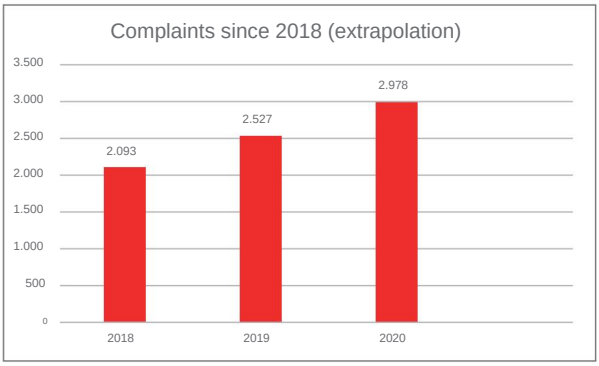
1.1 Complaints and Advice

Complaints under data protection law are in writing and in writing

78 GDPR ("the right to an effective legal remedy against a supervisory authority") applies. Around 76% of the written receipts in 2020 are complaints about data protection law. In the

Extrapolating this means that a total of 2,978 complaints, ie around 8 complaints per day, were submitted to the HmbBfDI. This means that the already very high number of complaints from the

The previous year has already been significantly exceeded and, also after further statistical evaluation, a new all-time high is marked:



Advice on data protection law is written and verbal information that is given to the responsible departments, the persons concerned and the authorities on request. In the reporting period, an extrapolated 358 citizens (previous year: 415), 143 responsible bodies in the private sector (181) and 17 times authorities (20) were advised by the HmbBfDI, so a total of 518 written consultations were carried out. This value is thus significantly below the value of the previous year (617).

In addition, 634 telephone consultations were carried out this year (persons affected: 524; responsible bodies: 100; authorities: 10). A total of 1,152 legal data protection consultations were carried out, which is also significantly fewer than the 1,446 consultations carried out in the previous year.

In the reporting period, the significantly increased number of complaints is offset by the equally significant decrease in the number of consultations. It remains to be seen whether a trend emerges here.

1.2 Obligation to report according to Art. 33 GDPR

According to Art. 33 GDPR, the person responsible is the supervisory authority de to make a notification immediately and if possible within 72 hours after becoming aware of the breach of the protection of personal data if the breach is likely to pose a risk to the rights and freedoms of the affected persons. The most well-known violation of the protection of personal data is the hacker attack, which often exposes weaknesses in data security. Even though in 2020 the main reasons for personal data breaches were mostly less spectacular and often related to human error (262 times e-mails and postal items were sent to the wrong addressee, which is close to the level of the previous year - 275 - corresponds), it is striking that the number of reported hacker attacks has more than doubled from 74 to 156. This is a worrying development that will continue to be monitored. Accordingly, the total number of reports of personal data breaches has increased significantly from 611 (28. TB VI 1.3) to 686.

1.3 Remedial Actions

In the reporting period, the HmbBfDI again from its ver

Various options for remedying violations of data protection law (Article 58 (2) GDPR) have been made use of. Specifically, the following measures were taken in 2020:

measure	Legal basis Article	Number 2020
Warnings	58 paragraph 2 lit	1
Warnings	Art 58 Abs. 2 lit. b	5
Instructions and Art 58 (2) lit. c – g orders and j Fines Art 58 (2) lit. i		2
		22
revocation of certifications	Art 58 Abs. 2 lit. h	0

1.4 European Procedures

If a complaint or similar has been received, it can be entered into the European Commission's Internal Market Information System (IMI) as a European procedure if it can be assumed that citizens of other EU countries are also affected by the alleged data protection violation are. lead

The supervisory authority in whose area of responsibility the person responsible has his European main branch is then responsible; all other supervisory authorities can report as being affected in the procedure.

European procedure	Number 2020
procedure with concern	10
Lead-managed proceedings	2
Further proceedings acc. Chapter VII DSGVO (Art. 60 ff)	Are not recorded statistically.

1.5 Opinions in legislative procedures

The HmbBfDI is to be supplied with Senate printed matter during the voting procedure insofar as data protection issues are affected ('Guideline for the Participation of the HmbBfDI' in the version of July 24, 2019). During the reporting period, the HmbBfDI was involved in 61 so-called printed matter votes, 34 of which dealt with legislative and regulatory projects (including the conclusion of international treaties).

2. Allocation of tasks (status: 01/01/2021)

The Hamburg Commissioner for Data Protection and Freedom of Information

Ludwig-Erhard-Str. 22 (7th floor), 20459 Hamburg
Tel.: 040/42854-4040

Fax: 040/42854-4000

E-Mail: mailbox@datenschutz.hamburg.de

Internet-Address: www.datenschutz-hamburg.de

Head of department: Prof. Dr. Johannes Caspar
deputy: Ulrich Kuehn
antechamber: Heidi Niemann

Representative for the budget, personnel and organizational management, Presidential affairs, corporate duties
Arne Gerhard

Budget management, planning and management, reporting, Controlling, basic questions of fee law
Robert Flechsig

Press and public relations, IT management, website of the HmbBfDI
Martin Schemm

Education and training, administration, travel expenses, fees and fines, building matters and procurement
Rolf Nentwig

antechamber, office
Heidi Niemann

Processing of the registry
Frau Vukšiÿ

Processing of the registry, information according to Art. 15 GDPR Ipek Sari

Promotion of data protection competence and media education, public relations
Alina Feustel

Basic questions GDPR, BDSG, HmbDSG and HmbTG, representation of the HmbBfDI in court proceedings Dr. Christopher Schnabel

Basic questions about sanctions and record keeping, case-by-case processing
Cornelia Goecke

Basic questions HmbVwVfG, VwGO, VwZG, labor, service and disciplinary law
Richard Heyer

Basic questions Art. 58 GDPR, individual case processing Steffen Sundermann

district and parliamentary affairs, parties and factions, Elections and referendums, economic administration, environment, churches
Eva Verena Scheffler

Passport, identity card and registration system, civil status system, statistics, Archiving, public construction and housing
Uta Cranold

Police, public prosecutor's office, courts, penal system, constitutional protection, fire brigade, notaries, immigration authorities
Anna-Lena Greve

Health and social services, research
Arne Brest

Public transport (especially local public transport), eGovernment (Smart City), supply and disposal, freedom of information
Swantje Wallbraun

Schools and universities, housing industry, geodata, finance and taxation
Alexander Schierman

Accreditation and certification, organization of the representation of the countries in the EDPB
Ulrich Kuehn

Search engines (especially Google, NorthData), apps, telecommunications
Felix Wagner

Apps, Internet of Things, technical and organizational advice and Testing, accreditation and certification
Mr. Schneider

ePrivacy, Tracking, Cookies, Press and Broadcasting, Accreditation and Certification
Katja Weber

Social networks (esp. Facebook, XING, Twitter), interdisciplinary case management Simon Hoffmann

Smart devices (especially voice assistants), development of test tools, technical development of the authority's website

Roland Schilling

Search engines (esp. Google)

Dr. A.S. Let's Come Together

European affairs, accreditation and certification
Frau Jacobson

Interdisciplinary case processing
Amina Merkel

Basic technical issues in eGovernment, technical organizational advice and testing . Sebastian Wirth

Basic technical questions in biometrics, video surveillance, Configuration and operation of the test laboratory, technical organizational advice and testing
Eike Mücke

Technical and organizational advice and testing
Jutta Nadler

Basic technical questions for networks and mobile devices, Configuration and operation of the test laboratory, technical organizational advice and testing
Robert Maka

International data traffic, fundamental issues in the economy, agriculture, trade unions Dr. Jens Ambrock

Clubs, sports, tax consultants and auditors, foundations
Heike Wolters

Employee data protection, banking, gastronomy
Oksan Karakus

Advertising and address trading, logistics, transport (excluding public transport)
Sabine Siekmann

Commercial services, industry, lawyers (excl notaries), private security services and detective agencies, market polling
Pauline Matters

Trade (stationary), insurance industry, video surveillance (non-public bodies)
Bianka Albers-Rosemann

Credit agencies, mail order and online trade, debt collection, culture, education (excluding schools and universities)
Behrang Raji

Interdisciplinary case processing
Viola Büchl

Interdisciplinary case processing
Eggert Thode

FROM

Edition: 800 copies
Front page photo: Thomas Krenz

Layout & printing: Druckerei Siepmann GmbH, Hamburg

Publisher:
The Hamburg Commissioner for Data Protection and Freedom of Information
Ludwig-Erhard-Strasse 22
20459 Hamburg

Tel.: 040/428 54 40 40 (office)
Fax: 040/428 54 40 00 Web:
datenschutz-hamburg.de E-Mail:
mailbox@datenschutz.hamburg.de

The Hamburg representative for Privacy and Freedom of Information

Hamburg