Machine Translated by Google

ACTIVITY REPORT

PRIVACY

2021

**The Hamburg representative for
Privacy and Freedom of Information**

Hamburg

Machine Translated by Google

Machine Translated by Google

30. Activity report on data protection by the Hamburg Commissioner for Data Protection and Fre

2021

Machine Translated by Google

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

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

Circulation: 750 copies
Front page photo: Martin Schemm, edited by Thomas Krenz
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH Print:
oeding print GmbH

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

---

submitted in April 2022
Thomas Fuchs (editorial
deadline: December 31, 2021)

Machine Translated by Google

INHA LTSV E RZ EICHNIS

Machine Translated by Google

Machine Translated by Google

Machine Translated by Google

1 Introduction

This 30th activity report on data protection 2021 is a special annual report. It documents a year of farewells, transitions and new beginnings: the second and last term of office of the longstanding Hamburg Commissioner for Data Protection and Freedom of Information, Prof. Dr. Johannes Caspar passed away in the spring, Ulrich Kühn shaped the transition for almost six months, and on November 1, after my election by the

Hamburg citizenship took office.

First of all, this constellation requires a word of thanks: To Johannes Caspar for 12 years, in which he shaped the office and made it an international brand. In which he raised public awareness of data protection, its freedom-ensuring function,
has raised its importance for human dignity and the protection of privacy to a new level through a feel for topics and media presence, through high professional expertise and process-related enforcement.

To Ulrich Kühn, his long-time deputy, for the prudent management of the interregnum, which in no way meant a period of standstill, but set its own accent with the first formal warning against a state agency because of the planned use of Zoom.

And last but not least to the employees of the HmbBfDI, who, like
This report impressively shows, at a time that was further characterized by the actual and data protection challenges of the pandemic, consistently standing up for the interests and
Citizens' rights in the area of data protection
to have.

And the number of submissions continues to rise: for the first time we received more than 4,000 written submissions, almost 3,000 of them formal data protection complaints. that documents
how much awareness of their own rights to privacy and digital self-determination has reached the citizens.

Machine Translated by Google

And how much the HmbBfDI is perceived as a contact point for enforcing these rights. Therefore, it remains an important concern to adapt the human and technical resources to these requirements. The independence of the Hamburg Commissioner for Data Protection and Freedom of Information, which is enshrined in the Hamburg Constitution, cannot come into play if the authority cannot be guaranteed to be adequately equipped for its tasks.

This is especially true at a time when the digital transformation is accelerating and is only just beginning in some areas, particularly in the public sector. And so that the tasks of the data protection authorities change and expand, the formative role is added to the supervisory one. But more on that later.

The HmbBfDI has big plans for the future. And I very much hope that our projects will succeed and that they will also reach the citizens - in both senses of the word. At this point, I wish you fruitful reading of this annual report and look forward to your suggestions and reactions.

Thomas Fuchs

Machine Translated by Google

Machine Translated by Google

INTRODUCTION 1.

Machine Translated by Google

1 Introduction

1.1 Europe – data protection is growing together Data protection is European and international, it has always been that way. Nothing crosses borders like data traffic.
Since 2018 there has been a uniform legal framework for this in the EU with the General Data Protection Regulation (GDPR).
And this is currently evolving: With the Digital Services Act (DSA), the Digital Market Act (DMA) and the Data Governance Act (DGA) of the European Commission, the regulation of the digital sector in Europe has reached a new level. The overarching goal of all these projects is clear: a secure digital space should be created in which the basic rights of users will continue to be protected in the future.

The cross-border view is reinforced by the judgments of the European Court of Justice (ECJ), which prohibit data transfer in put the USA under special observation. Due to the finding that the data of European citizens does not enjoy the same protection in the United States as in the EU, since every American technology company has to put up with the American secret services accessing their data, the data protection-compliant use of American Systems and software products problematic.

Even if data protection issues are often initially discussed at European level - and for many people this is probably very abstract - they affect us here in Hamburg every day. For this reason, European and international topics form their own chapter in the activity report for the first time this year.
Even if the HmbBfDI is no longer a member of the European Data Protection Committee (EDSA), it is intensively involved as a country representative in the Social Media Expert Subgroup of the EDSA and, above all, as the authority responsible for Facebook and Google in Germany, has special responsibility.

Machine Translated by Google

Johannes Caspar has rightly pointed out at this point in recent years that the Irish data protection authority does not apply the same standards and determination as we do to others
European data protection supervisory authorities are used to enforcing data protection law. This applies in particular to American companies that have their European headquarters in Ireland. This weakens European data protection in general and it even threatens to fail, Caspar continued. Unfortunately, this finding is

still up to date.

However, this is contrasted positively by the growing number of important decisions by European supervisory authorities that strengthen the application of the GDPR in Europe. The decisions by Austria and France on the statistics program “Google Analytics” by the American company Google LLC or Belgium’s decision on TCF 2.0 are only examples. TCF is 2.0

a technical standard infrastructure of the trade association of the
Online advertising industry (IAB), which is a basis for tracking surfing behavior on the web and thus for personalized advertising. This decision will have far-reaching consequences for the digital advertising industry and may also have a positive effect on the protection of our data when using the Internet. Numerous decisions by the authorities, but also by the member state courts, now fill in the GDPR on the basis of specific cases

Life and thus create additional legal certainty.

The HmbBfDI follows such decisions in its actions. That is why looking at the whole of Europe, and not just at Brussels, is of increasing relevance.

1.2 Germany – Beginning of a national data policy Digitization is entering a new phase. In Germany, not only the last few years have made it clear how much the country has to catch up when it comes to digitization, especially with regard to the public sector. And rightly so, the view widens from the infrastructural requirements to the entire field

of digitization, data use, data access, data security
and privacy.

The coalition agreement of the traffic light government shows the need for action, and this is not least a regulatory one. A data law, a data access law, a research data usage law, a medical data law or an employee data protection law. These are just five examples of a total of 15 bills mentioned in the coalition agreement. There are also plans for a data institute, data rooms, data trustees, data donations...

These projects unite the idea of the progressive process of
Shaping digitization democratically. This is to avoid that only a few large companies have power over the data and that we can only limit the standards they set by evading them, if at all. For example, the non-profit use of data is of particular importance, also as an opportunity for science and research and for the economy

scientific progress.

This changes the role of data protection. The right to privacy
and informational integrity of citizens is at least theoretically implied in these approaches. Data protection must therefore be considered from the outset, and thus part of a new digital architecture
tecture of our society.

This means that the expertise of the data protection authorities should, actually must, be included in all projects and legislative proposals from the outset. And it also means that we as supervisory authorities should provide answers on how legitimate goals can be achieved in a data protection-compliant manner.

This requires a certain rethinking towards formative, constructive data protection. Regulators will ask for that, but it will be worth it.

Machine Translated by Google

1.3 Hamburg – data protection as a civil right

4,000! This mark was exceeded for the first time in 2021. So many
Hamburger:innen turned to the HmbBfDI with a request, mostly with a complaint.

The range of topics is wide: the neighbor's outdoor camera, unsolicited personalized advertising, the use of personal data by insurance companies or energy companies, data protection by employers, the broker's duty to provide information and much more
more.

The complaint and the right to information are civil rights.
They create the opportunity to defend oneself against the unauthorized, non-legitimate use of personal data. It is good that the people of Hamburg make use of this right in large numbers. And that's why it's important that the HmbBfDI can respond to the people of Hamburg in a reasonable amount of time and with high quality. Unfortunately, this is still not the case. The technical and human resources of the authority are not created for this number of procedures. And with all the effort, the number of "old cases" that are not

can be treated promptly, unfortunately too high. Here is unchangeable
There is a need for improvement, for which the HmbBfDI will make very specific suggestions in 2022.

Added to this are the increasing deliberations of the public authorities, which also take up a large part of this report. This
The HmbBfDI is happy to take on this task and is pleased to note that the importance of this task in the run-up to project launches is increasing. Especially since the Senate, with its digital strategy, will rightly continue to push the increasing digitization of city services in the coming years.

1.4 Privacy and Communication

At first glance, data protection is a technical and legal issue – overarched by a complex European legal framework and IT processes that most users can hardly comprehend

can pull. The data protection professionals have it in one
Sphere of expert: inside knowledge made comfortable.

In the political discussion, data protection is often used as an excuse if something doesn't work or shouldn't be done.
And it can often actually be observed that data protection also
meaningful projects or plans prevented. Not because they cannot be implemented legally or technically, but because the fear of doing something wrong means that projects are prematurely abandoned or the hurdles are seen as higher than they actually are

are.

This contributes to an image that sees data protection as a brake on innovation. This image is wrong, but nonetheless it cannot be ignored. False images can also solidify.

For this reason, everyday and understandable communication of data protection issues in a language that people outside the technical and legal sphere can understand is so important.
This is especially true when teaching young people about data protection issues and teaching data and media skills in schools and other educational institutions. Of the

HmbBfDI would like to strengthen trust in data protection and
enable the people of Hamburg to actively exercise their fundamental right to informational self-determination.

Machine Translated by Google

Machine Translated by Google

Machine Translated by Google

2. EXAMS

Machine Translated by Google

2. Exams

2.1 Overview

In the reporting period, the HmbBfDI continued to check the CRIME file Au relia. No similarly profound deficiencies as were found in an examination of the CRIME file “Group and Scene Violence” in the 2016/2017 reporting period could be identified.

As early as November 2020, the HmbBfDI began examining the "Aure lia" file maintained by the State Criminal Police Office 71 (state security) (see TB Data Protection 2020, I 2). This state-owned CRIME file (“Criminal Research and Investigation Management Software”) is used to avert danger, including preventing crime, including extremist and terrorist crimes from the areas of ideologies and politically motivated crime that cannot be assigned. When examining the CRIME file "Group and Scene Violence" in the 2016/2017 reporting period, the HmbBfDI found significant deficits in the management of the file. This ultimately led to a formal complaint being issued against the Ministry of the Interior and Sport (BIS) (cf. TB Data Protection 2016/2017, II 1.2). For this reason, it was now necessary to check whether the Aurelia CRIME file was kept in compliance with data protection regulations. During an on-site appointment to explain the file, the HmbBfDI had a cursory look at its content and subsequently had access security, compliance with storage and deletion periods and logging explained. The HmbBfDI also randomly checked the requirements for storage of individual persons. The test did not lead to any objections.

The processing of personal data by security authorities is not always comprehensible and recognizable for the citizen. Data protection checks of measures taken by the police or the intelligence services are therefore an important part of the work

Machine Translated by Google

by regulators. Already in the coming reporting period
the regular mandatory check of the so-called anti-terrorist file (ATD) and the right-wing extremism file (RED) is due again (cf. on the last check TB Data Protection 2020, I 1). In addition, according to §§ 73, 78 Para. 3 of the Police Data Processing Act (PolDVG) in the area of hazard prevention law, the statutory rotation for checking compliance with the statutory provisions in police measures according to §§ 20 to 31 begins for the first time

and 50 PolDVG. The HmbBfDI is then at a maximum distance of
Two years legally obliged, among other things, to check data processing through the covert use of technical means (§ 20 PolDVG) or electronic surveillance (§ 30 PolDVG).

2. 2 Encrypted e-mail communication for youth welfare offices

After a long preparation process, the encrypted
E-mail communication between youth welfare offices and external bodies in 2022 can be used across the board.

What happened until now:
In October 2017, the HmbBfDI ended email communication with
External bodies are checked by the general social service (ASD) of the youth and family welfare department in the Wandsbek district office. It was found that in all kon

trolled cases not sufficiently encrypted e-mails and
have just been sent with sensitive personal social data of children and young people (cf. 26. TB, II 5).

According to § 78a SGB X, each data-processing social service office is obliged to take the technical measures that are necessary to ensure data protection. For protection

of the sensitive information contained in the emails

Machine Translated by Google
EXAMS

the use of so-called end-to-end encryption is required. Contrary to the legal requirements for data protection-compliant electronic transmission of social data, the checked e-mails were not sufficiently encrypted; end-to-end encryption was not performed. During the examination, the youth welfare office also confirmed that such content can probably be found in almost all files. In the course of the examination, the HmbBfDI asked the social authorities in 2017 to take the necessary measures.

In the 2018 activity report, it was reported that, in agreement between the social authorities, the Senate Chancellery and the HmbBfDI, the "Governikus MultiMessenger (GMM)", which includes S/MIME or GPG encrypted emails

can send and receive (cf. 27. TB, III 3). This IT infrastructure component was developed on behalf of the IT planning council.
It is made available to all authorities and offices in Hamburg by the Senate Chancellery.

After the year 2019 without any significant progress for the treatment

Once the shortage had been resolved, email encryption using the GMM was successfully piloted in a youth welfare office in mid-2020. Everyone involved in the piloting agreed that this piloted solution should now be used in all district youth welfare offices. Despite repeated inquiries from the HmbBfDI in the social authorities, another year passed after the piloting before the social authorities took up this topic again in mid-2021

men has.

The current status:

At the kick-off meeting at the end of October 2021, there was consensus among those involved in the further planning that the rollout process should be led by the newly appointed Chief Digital Officer (CDO) of the district offices. The CDO is that

Machine Translated by Google

State Councilor for the District Administration of the Authority for Science, Research, Equality and Districts (BWFGB) reports directly. A sub-project, which will be managed by the social authorities, will involve the youth welfare organizations. An initial estimate of the further course of the project was communicated to the HmbBfDI in November 2021. The preparatory tasks that still need to be completed for the rollout process are then to be completed by the end of March 2022

be closed. The rollout process is scheduled to end in October 2022

be finished. From this point in time, all youth welfare offices in the districts can then communicate in encrypted form with the youth welfare agencies. Even if 5 years will have passed since the test was carried out, the HmbBfDI is cautiously optimistic that this step will mark the start of greater use of encrypted communication will take place with external parties. It would be a very big development step for the Hamburg administration towards data protection-compliant electronic communication.

3.3 AutoAkte

The use of artificial intelligence in administration offers the opportunity to increase efficiency. When designing, a possible loss of one's own data sovereignty must be prevented.

With the AutoAkte project, the Senate Chancellery is using artificial intelligence to develop technical support for electronic file management. The documents fed into the ELDORADO file management and archiving system are automatically analyzed in five test authorities and used to train an AI system. The extension to most other authorities is planned. An AI model is developed based on text recognition and the accumulation of certain terms. On the basis of this, the software can determine which content can be found in which file.

If a new document is then created, the software suggests files in which, based on the terms used, it is likely that they relate to similar topics. The decision as to which file the document analyzed in this way is to be located is made by the administrative staff. The AutoAkte software is responsible for this decision

Machine Translated by Google
EXAMS

tion is a supporting tool for increasing efficiency. Individual files can be excluded from the analysis due to their sensitive content by entering the file number in the system as

exception is marked.

The AI is trained in a Microsoft Azure cloud. For this purpose, copies of the complete file contents are uploaded to the cloud and stored and analyzed there for a period of a few hours to a few days. The data is stored in encrypted form, but for specific processing in the

Cloud temporarily decrypted. Then the raw data
deleted from the cloud while the trained AI model remains there. The original electronic files remain in the ELDO RADO system hosted at Dataport. The storage in the cloud takes place on servers in the European Economic Area on the basis of an order processing contract with Microsoft. Access by the US parent company is not planned, but technically and factually not excluded.

From the point of view of the Senate Chancellery, there is no actual risk that US security authorities can access file content because the unencrypted storage is likely to be shorter than the assumed processing time for a data request under the US Cloud Act and FISA 702. However, such a risk-based consideration does not correspond to the legal assessment of the European Data Protection Board in its Recommendations 01/2020. In addition, it is only the raw data of the file contents copied to the cloud that are deleted at short notice. The trained AI model, which is permanently available in the cloud, contains a detailed set of rules about which content can be found in which file. The question of whether and which personal findings can be recovered from the AI model without the raw data cannot yet be resolved

finally be assessed.

The examination of the very complex processing procedure is ongoing.
The urgent recommendation of the HmbBfDI, the pilot operation with Echt

Machine Translated by Google

The Senate Chancellery did not follow to pause data until the legal situation is clear.

2.4 Donation advertising with a personalized website The processing of the first and last name for advertising purposes for a personalized website is not what those affected expect - especially if they have no connection to the person responsible and do not receive any information about this data processing

have.

At the end of 2020, the HmbBfDI was dismissed by a complaint drew attention to the fact that an aid organization had sent out a letter containing links to personalized websites – including a first and last name. When the advertising addressees called up the pages, they were called up by name

an existing problem was addressed and suggestions were made to you for possible support both for the organization in combating this problem and for a specific person ("Your godchild suggestion"). A direct response to these suggestions was also possible via the personal websites ("Become my godfather!").

In order to set up the personalized landing pages of the advertising recipients, the responsible body processed their names, which they did not collect from the data subjects themselves, but instead had received from the service provider from which the data records of addressees came from. No information was given when the data was collected; the letter advertising also did not contain any Information. In this, only the address service provider was considered responsible for the advertising broadcast and the possibility of advertising objection to this.

The HmbBfDI has asked the non-profit organization to comment on this special form of advertising and the associated data processing, in particular on the question of the legal basis for the operation of the personalized websites.

Machine Translated by Google
EXAMS

From the written reply and subsequent discussions, it emerged that this was the first advertising campaign in this form, which had been designed in such a way as to increase the response rate and, as a result, the support for the projects funded by the organization raise. Included

were no further than the names of the advertising addressees
information processed. The websites were not indexable and
could not be found via search engines, but only via the specific links given in the letters and the correct spelling of the first and last names. As the legal basis for this data processing, the organization relied on its legitimate own and non-profit interest, Art. 6 (1) lit. f) GDPR. The indications of the HmbBfDI that advertising addressees,

who are or were not related to the aid organization and have not received any information about it, do not expect their names to be used for personalized websites, led to the termination of the campaign and the deletion of the personalized

Websites.

In this matter, the HmbBfDI issued a warning i. s.d. Art. 58 Para. 2 lit. b) GDPR pronounced.

This has become permanent.

2.5 Testing of the video conference systems at the IT service provider Dataport

Together with the data protection supervisory authorities from Schleswig-Holstein, Saxony-Anhalt and Bremen, the HmbBfDI has been testing several software solutions for video conferences at the IT service provider Dataport since mid-2021.

As early as spring 2020, it became apparent that video conferencing services are an essential factor for success in the pandemic

Machine Translated by Google

of decentralized working methods in the pandemic. In the last
Activity report therefore placed a special focus on the requirements for video conferencing services set out by the federal and state data protection supervisory authorities. In doing so, their intended use in sensitive areas was considered (cf.

29. TB II 5 and II 10).

In 2021, the HmbBfDI has focused in particular on the use of such
services in the Hamburg administration (cf. Chapter IV 6 on the Zoom procedure). In addition to those from data protection
From a technical point of view, the HmbBfDI sat down with more transparent and data

protection-friendly alternatives apart. That's how he uses it
HmbBfDI, for example, has been using a platform for the purpose of media education since this year, which is based on the open-source service BigBlueButton (cf. Chapter VII 3). Dataport's completely open-source "Project Phoenix" also represents an alternative to powerful commercial providers, which aims for high transparency and digital sovereignty (cf. https://www.dataport.de/was-wir-bewegen/portfolio/ dphoenixsuite/ and 29th TB IV 1). The dPhoenixSuite includes an audio and

---

Video conferencing module, including modules for creating texts,
spreadsheets and presentations and for e-mail communication. the
Suite is now generally available to all carrier countries and is also being used by Dataport outside of the core carrier countries
Bremen, Hamburg, Saxony-Anhalt and Schleswig-Holstein for the
distributed to the public sector. The module for video communication
on is based on Jitsi Meet, which is also open source, and is supplemented by additional chat and other value-added functionalities.
In view of the fact that all processing steps at Phoenix are controlled by Dataport as a public IT service provider, there is basically the possibility of intensively examining the entire process and, above all, adapting it (or having it) adapted to your own needs

to. The HmbBfDI has therefore with the other data protection supervisory
authorities of the data port carrier countries initiated a joint examination in order to examine the data port video conferencing services more precisely

Machine Translated by Google
EXAMS

investigate. The aim is for the supervisory authorities to carry out a uniform assessment of the audited services. The subject of the test are two products in the context of the Phoenix project,
under the product name dOnline Collaboration 1.0 and 2.0
be distributed, as well as an "existing solution" for implementation
of video conferences based on Cisco with the product name
dvideo communication.

The review started in mid-2021 and has not yet been completed. At this point in time, however, it can already be stated after the first analysis that Dataport was able to provide various documents that are significantly superior to those of other (commercial) providers in terms of scope and informative value. The exam will be held in the course of 2022

closed.

Whether and – if so – to what extent the Cisco-based video conferencing solution differs from the Jitsi-based services and what implications this will have for the responsible bodies that use these services for their individual purposes will be presented in the next activity report at the latest will.

2.6 Coordinated Audit of Media Companies

The first results of the coordinated media check have shown that the consent obtained through the use of cookie banners on the respective websites is mostly ineffective and improvements have to be made.

As part of the coordinated audit (see 29. TB, III 4), the authorities involved, in addition to the HmbBfDI, sent a jointly developed questionnaire to selected persons from mid-August 2020

Machine Translated by Google

media companies in their respective areas of responsibility. A very high number of cookies and third-party services integrated by the providers were found on the media websites checked, which are mainly used for user tracking and advertising financing.

Via the implemented cookie banners, the respective websites usually ask for differentiated consent from the users for the use of cookies and third-party services. However, the majority of these consents are not effective (https://datenschutz-hamburg.de/pressemitteilungen/2021/06/2021-06-30-medienwebsites). In particular, the following deficiencies were identified:

The first time the website is called up, third-party services and cookies that require consent are integrated without the user having had the opportunity to give their consent at all beforehand. Furthermore, there are significant shortcomings with regard to the transparent presentation of the data processing processes. Insufficient or even incorrect information is given about the tracking of user behavior.

In addition, the coordinated review has shown that even if individual user settings are made, wei
Afterwards, numerous cookies and third-party services are actively integrated into the website
remain integrated, which were actually previously rejected by the individual settings of the users. In this context, information on data processing on the basis of a legitimate interest (Article 6 (1) (f) GDPR) is also given as part of the consent dialogues, which also gives the wrong impression that consent can or must also be given to such processing processes .

All consent banners also give users the opportunity to consent to the use of all cookies and third-party service providers directly at the first level

Machine Translated by Google
EXAMS

grant, whereas there is no equally easy way of rejecting user tracking in its entirety or of being able to close the banner without a decision.

The data protection supervisory authorities have, within the framework of the An Adaptation of the "Orientation Guide for Telemedia Providers: Inside" on the question of the simplicity of a rejection option is now clearly positioned (https://www.datenschutzkonferenz-online.de/media/ oh/20211220_oh_telemedien.pdf, p. 17):

"If users cannot simply ignore a request for consent when calling up a telemedia service because this covers the content of the service, the consent is generally not voluntary if the granting of the refusal involves greater effort, e.g. B. to clicks and attention

is. In order to ensure that they can prove effective consent, providers of telemedia must therefore urgently ensure that the options made available are of equal value."

Finally, the designs of the respective consent banners reveal numerous forms of so-called nudging. here
subtly become users unconsciously
Giving consent under pressure, for example by highlighting the button for consent in a much more conspicuous way than the button for rejecting or for individual settings, or by making the refusal of consent unnecessarily complicated or not using the button for settings/options at all clickable button too

recognize is.

Possible supervisory measures against the media companies audited by the HmbBfDI are currently being examined. Here, too, the cooperation between the German supervisory authorities,
who take part in the coordinated examination, a comparable procedure is ensured.

Machine Translated by Google

Machine Translated by Google

Machine Translated by Google

REPORTS 3.

Machine Translated by Google

3. Reports

3.1 Forwarding transparency requests to the LKA

As with all other data processing operations, a legal basis is required for the forwarding or transmission of personal data between two public bodies. Personal data from inquiries about transparency legislation from citizens may therefore not be passed on to security authorities by the agency responsible for providing information without checking it and without the legal requirements being met. If this happens nevertheless, storage by the security authorities is also inadmissible.

In July 2021, an applicant in accordance with section 11 of the Hamburg Transparency Act (HmbTG) asked the Altona district office by email
about time and place of everyone in the area of the district office to this
Information stands registered and approved by the parties at the time
"Alternative for Germany" (AfD); "National Democratic Par
tei Deutschland" (NPD) and Basisdemocratic Party German
country (the basis) in the months of August and September 2021, specifying the respective dates, times and addresses. The responsible specialist office of the district office forwarded this e-mail (including the name and address of the applicant) to the LKA 71 (state security) of the Hamburg police with a request for an assessment of whether the answer to the inquiry would lead to an increased risk for the information stands

could.

The HmbBfDI is of the opinion that the (unsolicited)
Disclosure of the applicant's personal data to the LKA was not justified: The processing of personal data is subject to the principle of purpose limitation (Article 5 (1) (b) GDPR). After that, processing of personal data for purposes other than the original purpose

Machine Translated by Google

only permitted under certain conditions. For public bodies of the Free and Hanseatic City of Hamburg, the admissibility of purpose-changing processing is based on Section 6 of the Hamburg Data Protection Act (HmbDSG). A transfer of personal data from a HmbTG procedure to the LKA could be considered, for example, if the transfer of the applicant's data was to avert a threat to public security (§ 6 Para. 2 No. 1 HmbDSG) or to prosecute criminal offenses or administrative offenses are required (§ 6 Para. 2 No. 2 HmbDSG).

However, these requirements were not met here because the request did not provide any actual indications or information in this regard. A transmission of the data was therefore not justified.

The problem is not new at the HmbBfDI: inquiries about elections
stands of right-wing extremist parties were already in the TB Informati
freedom from freedom 2010/2011, chap. 4.3 (at that time, however, only from the point of view of freedom of information). In TB In
freedom of formation 2016/2017, chap. 4.7, the issue was raised again. At that time, the HmbBfDI was informed that some of the information would be transmitted in a standardized form to the security authorities in order to inform them about the applicant's identity. The HmbBfDI had demanded an end to this practice, which was also promised. The forwarding now in question was apparently not aimed at directing the LKA to the applicant, but rather with the purpose of obtaining an assessment of the risk situation from the LKA. Irrespective of the objective, the forwarding of the complete data of the applicant was not permitted. We sought a conversation with the legal office of the district office, which shared our legal opinion without hesitation based on the clarification that had already taken place in previous years.

It was also reported that the forwarding of the applicant's request for transparency, including the personal data, was a one-time oversight. The data of the claimant at the LKA were deleted. A renewed sensitization of the employees was promised.

3.2 Contact tracing/Luca app

Since the beginning of the corona pandemic, contact tracing has been a crucial means of overcoming the crisis. After it had already been shown in 2020 that openly laid out paper lists led to many people leaving incorrect contact details or correct ones being used by third parties inappropriately (cf. 29 TB, II 2), digital solutions for contact tracing had to be assessed in terms of data protection law in the reporting period . Experiences with analogue contact tracing have clearly shown that data protection is indispensable in order to create the necessary trust in society, with which the effectiveness of contact tracing measures can be guaranteed in the first place.

It was and is important to the HmbBfDI to campaign for data protection-friendly containment of such digital contact tracing systems. Therefore, the HmbBfDI participated in a task force appointed by the conference of data protection officers of the federal and state governments (DSK). Under the direction of Berlin and with the cooperation of Rhineland-Palatinate, Mecklenburg-Western Pomerania, Baden-Württemberg and Hamburg, the members of this task force drew up a statement adopted by the DSK ("Contact tracing in times of the corona pandemic, practical solutions with a high protection of personal data", as of March 26, 2021) as well as a guide for those responsible and developers ("Use of digital services for contact tracing when visiting events, facilities, restaurants and shops to prevent the spread of Covid-19 ", as of April 29, 2021).

Machine Translated by Google

In both documents, the DSK particularly emphasized that digital methods for processing contact and presence
data must be operated in accordance with data protection regulations. Only then
such solutions can be the better alternative to paper lists.

For the use in Hamburg, the HmbBfDI was informed that the Senate had decided to acquire licenses for the Luca app for digital contact tracing, a service of Culture 4life GmbH based in Berlin. The Hamburg health authorities used the application after licensing. The HmbBfDI informed Kasse Hamburg, also with reference to media reports and assessments by independent experts, that there were data protection concerns regarding the use. However, the Senate did not make the licensing dependent on the assessment of the HmbBfDI and did not seek advice in advance.

In the period that followed, there were constructive and cooperative discussions with the Hamburg cash register and the social authorities at the working level. The City of Hamburg hoped that the operators of the system would make improvements in terms of data protection. The HmbBfDI consulted the colleagues at the supervisory authority in Berlin and it became apparent that the hoped-for improvements to the Luca app would take considerably more time. Therefore, the HmbBfDI turned to the Senator for Labour, Health, Social Affairs, Family and Inte

gration and stated that the overall view of the defects that had become known had led to the conclusion that the Luca app was not state-of-the-art and that the major weaknesses could not be eliminated in the near future. Healthy

health authorities would have to be responsible for data protection
ensure that you do not use insecure technical infrastructures.

The HmbBfDI repeatedly referred to the preferable use of the Corona-Warn-App (CWA) from the Robert Koch Institute as a secure and data-saving solution for decentralized contact tracing.

This offers cluster recognition comparable to the Luca app, with which QR codes can also be scanned in facilities. It can warn users of possible contacts without the involvement of the health authorities directly and without any further delay. The 64th HmbSARS-CoV-2 Containment Ordinance did not allow the use of the CWA. The Senate decided against this because the CWA cannot provide any address data required for quarantine orders, but this is mandatory according to § 7 HmbSARS-CoV-2 Containment Ordinance, insofar as the ordinance for the purpose of official contact tracing prescribes the obligation to collect data in a specific area .

The guests, customers and visitors
Nonetheless, the CWA provides visitors with crucial information. Here you have to weigh up: There will undoubtedly be individuals who do not go into isolation despite the warning from their app. Overall, however, the Corona warning app is likely to interrupt more chains of infection, since those affected are informed directly and without a delayed detour via the health authorities.

Against this background, the HmbBfDI asked the senator to consider opening up the use of the CWA for this purpose in Hamburg by amending the HmbSARS-CoV-2 Containment Ordinance.

The Senate initially did not decide to change the HmbSARS-CoV-2 Containment Ordinance.

In the last few months of the reporting period, the pandemic situation has changed to such an extent that it is now necessary to ask about the need to collect contact data across the board. Due to the massive overburdening of the health authorities, contacts are not followed up by the health authorities, or only in isolated cases – for example in nursing homes or hospitals. In this respect, it makes sense, at least in all of them

whose spheres of public life refer to the CWA as probates
to set funds.

Machine Translated by Google

It was not until February 2022 that the 65th Amending Ordinance resolved the area-specific deletion of the obligation to collect contact data.

3.3 School in times of Corona

With the progress of the pandemic and changes in protective measures and teaching concepts, new data protection questions arose constantly, which also had to be answered by the courts.

Even in the second year of the COVID-19 pandemic, this led to school area to an increasing number of submissions to the HmbBfDI, as the pandemic has led to a large number of new processings of personal data from the people involved in school operations came.

Distance learning formats led to data processing using video conferencing systems and digital learning tools. Measures to avoid health risks and to prevent infections have resulted in various data processing situations, including health data, which are subject to the special protection of Art. 9 data

General Protection Regulation (GDPR) and have been the subject of various submissions to the HmbBfDI.

The question of the admissibility of the processing of personal data by the Hamburg schools and the Authority for Schools and Vocational Training (BSB) in the context of pandemic-related protective measures under data protection law came to a head in particular with the question of the admissibility of the compulsory corona testing of the pupils who class group are carried out to. While the test result is indisputably considered a health date

is to be classified within the meaning of Art. 9 GDPR, the question arose as to whether the disclosure of this date to third parties, which is inevitably associated with testing in the classroom, can be permissible under data protection law. This question was decided by the Hamburg Administrative Court in parallel with the examinations carried out here. In its judgment of April 29, 2021 on file number 2 E 1710/21, the administrative court initially stated in principle that the restriction of access to presence offers at the school regulated in Section 23 (1) sentence 3 no through the mandatory participation in a corona test as a necessary protective measure within the meaning of the Infection Protection Act and the resulting data processing operations are compatible with the provisions of the GDPR. According to the administrative court, the self-testing of the students in the class is then permissible if the students are given the opportunity to do this test procedure in the class by presenting a test result from a test with a test provider § 6 para. 1 Sentence 1 of the Coronavirus Test Ordinance in order to avoid disclosing the test result to fellow students. This option had not been granted by BSB's model hygiene plans prior to this court decision. However, the model hygiene plans were adjusted by the BSB as a result of this judgement.

The use of video conference systems was already reported in the 29th activity report of the HmbBfDI (Chapter II 5 there). The "Lernen Hamburg" learning management system created by the authority for schools and vocational training for distance learning was further expanded in 2021. The authority created additional server capacities to meet the growing demand from schools for the use of this system and to enable reliable operation of the system. Since this system was also made available for all vocational schools and was used there, a submission to the HmbBfDI prompted the planned introduction of Microsoft 365 to all vocational schools

Machine Translated by Google

schools in Hamburg by the Hamburg Institute for Vocational Training (HIBB) for a surprise. The HmbBfDI was not involved in the planning of this large-scale project. although it is

at Microsoft 365 by a nationwide data protection law highest

controversial product. As part of a model project for
Use of Microsoft 365 at vocational schools in Baden-Württemberg

Berg, where the local Ministry of Education worked together with the State Commissioner for Data Protection and Freedom of Information, a high data protection risk was identified when using this service (https://www. baden-wuerttemberg.datenschutz.de/lfdi-raet- due to-high-risks-of-data-protection-law-from-the-use-of-the-tested-version-of-microsoft-office-365-at-schools-from/). For this reason, a working group has also been set up at the KMK level, which, with the involvement of the DSK, checks whether MS 365 can be used in schools at all. Our concerns have now been addressed, at least to the extent that the HIBB has initially suspended the nationwide introduction until we have checked the reliable documents that we now have.

3.4 University Amendment Act

After a lengthy coordination process, it was decided to adjust the data protection regulations in Hamburg's higher education law to reflect changes in teaching operations caused by the pandemic.

In higher education, the COVID-19 pandemic made it impossible

Due to the risk of infection and the distance formats required as a result, a change in teaching operations was necessary and presented the Hamburg universities and the Authority for Science, Research, Equality and Districts (BWFGB) with actual, technical and thus also legal challenges.

The digitization of teaching that was driven forward as a result of the use of video conference systems, learning platforms and other digital learning formats raised various data protection issues that were to be resolved by the BWFGB with a legislative project summarized under the title "Digitization of teaching and examinations".

The BWFGB included the HmbBfDI in the discussion, adaptation and amendment of the draft law and its objections were discussed extensively. The rounds of talks, which also included university representatives, showed that the area of tension between pedagogically justified, widely desired data processing powers on the one hand and processing principles to be observed under data protection law, such as legality/proportionality considerations and data minimization aspects on the other hand, was of particular importance.

This area of tension became particularly clear on certain cornerstones, such as the question of the admissibility of recording digital courses and the admissibility of monitoring students in the context of digital exams, including their recording. When digital courses are recorded, audio and video data from students may be recorded, which not only has a personal character, but can also, depending on the format and topic of the course, have particularly personal, sensitive and sensitive content. The same applies to the recording of the video supervision of an online exam, which may capture images of and from the students' most private area, namely their private apartment. This intensity of intervention had to be sufficiently taken into account when formulating legal regulations.

At the end of the voting process, there was a draft to deal with changes in the Hamburg Higher Education Act (HmbHG), in particular in § 111 Para. 2-4 HmbHG and in § 3 of the law

Machine Translated by Google

the impact of the COVID-19 pandemic on higher education,
made.

The regulation in § 111 paragraph 2 HmbHG should now contain a legal basis for the universities to hold digital courses and the personal data required for this

To be allowed to process data of participants.

A regulation for the processing of personal data in the context of digital examinations for video supervision and authentication of the students to be examined was drafted for Section 111 (3) HmbHG. Since video supervision as part of a digital distance examination may represent an intrusive measure because it allows insight into private rooms and thus into the private sphere as a protected area for students, restrictions on this intrusion were included at the objections of the HmbBfDI. In particular, a recording of the video surveillance and an automated evaluation should not be permitted. In addition, participation in a digital exam under video supervision should only be possible on a voluntary basis.

The draft regulation in Section 3 of the Act to Cope with the Effects of the COVID-19 Pandemic in the Higher Education Sector did contain an authorization for the higher education institutions to record online events through image and sound recordings, but through various additions it restricted the further processing of the recording result included. In addition, the inclusion of these powers in this law and its time limit emphasized the exceptional nature of this data processing power due to the pandemic.

The draft law was passed by the middle of the citizenry
sen and as a law from 06/17/2021 on 06/18/2021 in Hamburg
cal Law and Ordinance Gazette No. 43. The result is a legal regulation that makes serious and visible efforts to protect data protection restrictions

to formulate the rights and freedoms of those affected and to

To bring it into line with the requirements of the universities based on practical needs.

3.5 2022 census

The 2022 census is in sight. The HmbBfDI is the lukewarm intensively and critically accompany the preparations and the implementation of the population census and also monitor compliance with the statutory deletion periods after the surveys have been completed.

Under current EU law, member states are required to carry out a population census (census) every ten years. Since the last census took place in 2011, the current census was initially scheduled for 2021. Due to the effects of the corona pandemic and the time-consuming preparation, the census had to be postponed to 2022. The new deadline is May 15, 2022.

The census is used to determine basic data on the population, employment and housing situation as the basis for official statistics. A central task is the statistical determination of the official population figures. The 2022 census is again designed as a register-based population survey. This means that not all citizens are surveyed, but that large amounts of existing data from the state administrative registers, such as the population register, are used as basic information. As a result, the so-called household survey can be limited to a sample of around 10% of the population

will. In addition, at addresses with special areas, the
Residents of dormitories were interviewed. In shared accommodation, the facility managers are obliged to provide information. In the census of buildings and apartments (GWZ), the owners, administrations and others

Machine Translated by Google

persons entitled to dispose of or use all residential buildings or apartments questioned.

The Federal Constitutional Court (BVerfG) confirmed this method as constitutional in its decision of September 19, 2018 (2 BvF 1/15; 2 BvF 2/15) on the norm control applications of the states of Berlin and Hamburg.

For the data protection support of the 2022 census
by the statistics working group of the data protection conference

working group formed, to which the HmbBfDI belongs. As part of its participation in the legislative process for the 2022 Census Preparation Act and the 2022 Census Act, this working group raised data protection concerns and developed proposals for amendments, which, however, were not fully taken into account. Major points of criticism of the Census Act relate to non-anonymous surveys in sensitive special areas, such as prisons, the full census that is still planned for the GWZ, the mandatory survey of membership in a public religious community – especially since the German legislator exceeds the EU requirements here .

A new feature of the 2022 census is that for the first time the statistical Administration of the entire database, incumbent on the Federal Office. Therefore, with regard to the cooperation of the statistical offices of the Federal Government and the federal states in the so-called statistical association, a clear and selective regulation of data protection responsibility has been demanded.

In the Census Preparation Act, Section 9a, which was added later, has been criticized. This regulates the transmission of certain data on all persons stored in the German population registers on a specified date to the statistical offices. This should serve to check the transmission channels and the quality of the transmitted data sets and to further develop the programs for carrying out the census. One against this test with real

data at the Federal Constitutional Court was rejected by decision of February 6, 2019 (1 BvQ 4/2019). However, the outcome of the constitutional complaint proceedings is still open.

In the course of the ongoing practical preparations for the implementation of the 2022 census, the HmbBfDI discussed legal and technical data protection issues in several information and consultation meetings with the Statistical Office for Hamburg and Schleswig-Holstein and will continue to do so.

After the planned modernization of the administrative register in Germany, future censuses are to be carried out exclusively on the basis of registers and do not require any surveys of the population. The links required for this

of information from existing and yet to be established
Administrative registers in different areas will pose new challenges for data protection.

3.6 Deletion of application documents

When application documents are to be deleted after an unsuccessful selection process depends largely on whether the posting office is a public or non-public position le is.

During the reporting period, the HmbBfDI received repeated questions from both employers and applicants about the deletion of application documents after the selection process had ended. In the majority of cases, the question of the storage or deletion periods of the application documents arose after the end of an application process

driving

Machine Translated by Google

If the application process ends with a positive selection decision, the application documents must be transferred to the personnel file (if available). If, on the other hand, the application procedure ends with a rejection (so-called negative decision), the application documents of the unsuccessful applicants must be deleted (or returned to the applicant).

Art. 88 Para. 1 GDPR in conjunction with Section 26 BDSG as the legal basis for the processing of applicant data in the non-public area is silent on this. In terms of data protection law, this obligation therefore results from the principles of data minimization and storage limitation. Personal data must therefore be deleted immediately as soon as their knowledge is no longer required to fulfill the purpose of storage. The purpose here is the application process, which ends with the letter of rejection, so that the application documents must be deleted after the letter of rejection has been sent. However, both principles can have a negative effect on both the posting office and the unsuccessful applicants and lead to a lack of evidence, namely when legal claims from the application process are asserted by unsuccessful applicants. It is therefore justifiable under data protection law for the posting body to keep the application documents and/or documentation on the application process for a certain period of time in order to defend itself against legal claims by the unsuccessful applicant. The decisive factor for the length of the period is the period within which legal claims can be lodged by unsuccessful applicants after receipt of a letter of rejection.

The standard used here is six months. This period results from the General Equal Treatment Act (AGG) in the event of a violation of the ban on discrimination.
This period is calculated as follows: According to the AGG, claims for damages or compensation must be made within two months

natsfrist after receipt of the rejection letter (§ 15 paragraph 4 AGG). Only if claims are made against the employer within this period does the three-month period set out in Section 61b (1) of the Labor Court Act begin with the written assertion of the claim against the employer in accordance with Section 15 (4) sentence 1 AGG. As a result, this leads to a retention period of five months plus one month for processing.

However, responsible bodies must not insist on the rigid storage period of six months if the data subject
no later than two months after receipt of the rejection letter, the deletion of their personal data is requested and no claims for damages or compensation have been asserted in the meantime. In these cases, there is no need for further storage and the data must be deleted immediately.

If an employer also wants to store the personal data (e.g. for the purpose of future consideration for other job offers), the opt-out is required

physical and written or electronic information and
Consent of the applicants. Ideally, this should be obtained when the letter of rejection is sent or – depending on the structure of the application process – at the beginning of the application process.

However, the situation is different in the public sector. Here, the legislature has provided for an express and immediate obligation to delete data in the event of unsuccessful application processes in Section 10 (6) HmbDSG. However, sentence 2 contains a limitation of this principle in the event of overriding legitimate interests

the data processing body.

Overriding legitimate interests can also be claims under the AGG. However, there is also the option of submitting application documents for a period longer than six months

Machine Translated by Google

te to save when rejection notifications are not provided with instructions on legal remedies. In these cases, application documents must be stored for at least one year due to the need to provide evidence in the event of potential competitor lawsuits.

During the review of the digitization of the application process and the introduction of the application management system at the FHH (BMS process), the HmbBfDI learned that the FHH regularly stores personal data of unsuccessful applicants for a period of 400 days. A statement then obtained from the Personnel Office revealed that letters of rejection to the unsuccessful applicants at the FHH are usually not provided with instructions on legal remedies, so that at least theoretically any appeals could still be lodged up to a year after the rejection. Therefore, the application data must be kept for at least 400 days (one year + 35 days for processing) after the selection process has been completed.

The storage period is not objectionable in terms of data protection law, because according to § 37 HmbVwVfG there is no obligation to provide administrative files with instructions on legal remedies (RBB) (this is different in federal law according to § 37 paragraph 6. VwVfG, according to which written or electronic administrative files that the subject to challenge, must be provided with an RBB). An obligation to issue an RBB does not result from § 58 VwGO, nor from the rule of law principle of Art. 20 GG, the right to effective legal protection of Art. 19 (4) GG or the principle of equality of Art. 3 GG. There are also no other legal provisions that stipulate such an obligation, so that the authorities issuing the tender are not obliged to provide their – contestable – decisions with an RBB.

Predominant legitimate interests can be multi-level
Application procedures are sometimes too long

lead to storage periods. These long storage periods may be necessary under data protection law and therefore justifiable if
the application process is characterized by special features and several stages of testing. For example, the health requirements of the police are regulated in detail. Applicants who are otherwise suitable may initially fail for reasons that can be remedied (e.g. lack of proof of swimming ability or lack of necessary educational requirements).

In the case of a larger number of repeat applications, it may also be appropriate not to repeat the recruitment process at all stages if a significant number of such
Applications can already be ruled out by resorting to earlier documents, for example if the applicant has been classified as absolutely unsuitable for the police service. Especially with these applicants

However, it should be noted that the storage periods must not be designed as absolute and rigid storage periods, but rather as a review period in order to protect the right to informational self-determination.

Under certain circumstances, applicants classified as absolutely unsuitable may also have constellations that can lead to a different classification in the event of a reassessment. This may affect applicants who identify as
Juveniles or adolescents apply to the police and remain silent about investigations because they cannot assess the risks, consequences and guarantees involved. Long-past “sins of youth” would thus lead to a stigmatization that can last until the age of recruitment (up to the age of 35) has passed. The HmbBfDI drew the Hamburg police's attention to this when examining a complaint. The Hamburg police were able to understand the reasoning of the HmbBfDI and submitted a draft to the HmbBfDI at the end of November, in which the absolute and rigid storage period for absolutely unsuitable applicants was supplemented by a review period.

An interim review period of three is now planned

Machine Translated by Google

years. If the status "absolutely unsuitable" is to continue to be assigned, the reasons that led to longer storage in individual cases must be checked and documented with regard to their continued existence. The relevant processes in the police academy have already been adjusted.

3.7 IT forensics and data protection checks at HmbBfDI

The HmbBfDI has established a standardized procedure for forensic examinations.

In the course of audits and complaints, it must first be determined which data has been stored and processed on a device, such as a smartphone or USB stick. Previously deleted and then reconstructed data can also be of interest for clarifying the facts. With these technical tests by the HmbBfDI, it is of great relevance to obtain meaningful and reliable information about the respective test object, which ultimately has a quality that will stand up in court. The knowledge gained from this forms the basis for the assessment of whether data protection violations have occurred and whether and which sanctions are imposed. In recent years, there has been an increase in such technical tests, which the HmbBfDI has taken as an opportunity for certain parts

to establish rich standardized processes. Special occasion related tests in which storage media were to be evaluated, increasingly represent such an area.

For the previous supervisory practice at the HmbBfDI, evaluations of storage media such as (external) hard drives, USB sticks, SD cards and also memory from smartphones were used to clarify facts within the framework of technical inspections

gene of importance. In order to be able to assess and appreciate such storage media and the personal data stored on them, it is important to define uniform and coordinated analysis processes that are used by external bodies such as courts

– can be understood and evaluated. The HmbBfDI has therefore defined a standardized procedure for the purpose of examining data carriers: First, these data carriers/storage media are backed up without the storage media being changed.

Only then does the analysis follow, which is fully documented.

The procedure is based on the guidelines for IT forensics
Federal Office for Information Security (BSI), with
which ensures completeness, integrity and authenticity. It includes, among other things, the integrity-assured creation of forensic duplicates using so-called WriteBlockers as well as an evaluation based on state-of-the-art tools. As a rule, the programs used have been developed open source in the IT security community. The scope of the examination is always defined at the beginning of the respective review and all steps of this process are documented. The necessary hardware equipment has always been procured in a targeted manner in recent years so that the required resources are available. External training courses enabled the responsible employees to develop the necessary know-how. The HmbBfDI assumes that the described development regarding the necessity of such technical examinations will continue and even increase over the coming years.

It can also be assumed that in the future, in the context of unrelated audits and reports from the responsible bodies about violations of the protection of personal data in accordance with Art.
33 GDPR (Data Breaches) such methodologies by the
HmbBfDI are increasingly used. The exchange with others
On the one hand, the data protection supervisory authorities will be
evaluation throughout Germany and also at European level
uniform and on the other hand through the professional exchange

Machine Translated by Google

also with regard to the quality of data protection checks
lead to added value in supervisory practice.

At this point it should be clearly emphasized that unauthorized access to data that is particularly secured or even the use of backdoors in the context of these technical checks represent a clear limit and were never planned. On the contrary, the HmbBfDI has been positioning itself for several years to ensure that IT security gaps are to be closed as quickly as possible so that everyone can be sure that their personal data is only made accessible to them and to expressly authorized persons. As part of the above checks, there is always a trade-off between the interventions to be carried out – sometimes with private end devices – and the data protection that is in the room

legal violation.

3.8 Complaints from the organization NOYB

In August 2021, several complaints were filed by the non-governmental organization NOYB about the use of "dark patterns" and "nudging" in cookie banners. Other complaints were directed against the use of "payment models" on media websites.

3.8.1 Complaints about “dark patterns” and “nudging” NOYB has lodged
422 complaints against website operators. The subject of the complaints is the use of consent banners, which, in NOYB's opinion, improperly influence users when they give their consent to tracking. As part of its area of responsibility, the HmbBfDI examines five of these complaints.

From the point of view of many operators of telemedia, personal data is only of interest if this data can be used commercially

are. Data processing for the – usually cross-device – tracking of the individual behavior of users (tracking) is an important factor in competition, for example to be able to display personalized advertising. However, before personal data is processed for the purpose of user tracking on websites or in mobile apps, it is imperative that the respective operators obtain prior consent from the users.

In order to achieve the highest possible rate of consent, attempts are therefore increasingly being made to increase the rate at which consent is given by using questionable mechanisms such as "nudging" or the use of "dark patterns".

These terms can include graphical designs of user interfaces and other mechanisms with which de
divide the behavior of users into a specific
direction should be steered.

Graphically implemented control effects are referred to as nudging (to nudge = to nudge) in the context of cookie banner design. Such “nudges” are used to direct users towards one of various options when making their decision.

If “dark patterns” are used, users and Nut
Furthermore, they may be tempted to take actions that do not correspond to their true interests and may even run counter to them. Such decisions that are contrary to interests are achieved, for example, by creating user interfaces that ignore user preferences. This can be done, among other things, with insufficient information about the cookies used, incorrect designations of cookie functions, pre-selected ticks in the settings or confusing colors in selection fields.

Machine Translated by Google

A clear distinction between the two methods is not possible and also not necessary, since both methods are legally different
consider the question of the effectiveness of the consent obtained
meeting.

In the complaints submitted to the HmbBfDI, NOYB claims that deceptive cookie banners are used in this sense, which do not meet the data protection requirements for “voluntary consent given for a specific individual case, in an informed manner and unequivocally”.

The object of the complaints is the use of "dark patterns" in the form of missing or hidden rejection radio
functions on the first level of the cookie banner. As another off
designing the illegal controls through "dark patterns" or "nudgings", the complaints contain information about misleading button colors for the various options in the banner. Accept buttons are clearly highlighted in color and typeface. In contrast, the buttons for rejecting are only kept in low-contrast colors and also from the continuous text

hardly distinguishable.

The 422 NOYB complaints followed a Union-wide review of websites. Accordingly, the responsibility for reviewing the alleged GDPR violations falls within the competence of different European supervisory authorities (cf.

29TB, IV 6). Since the complaints are identical in content
The European Data Protection Board (EDPB) set up a task force for this topic. This is intended to ensure the best possible, harmonized approach to the processing of complaints by the relevant supervisory authorities. The development of coordinated processes is still ongoing.

3.8.2 NOYB complaints against subscription models

Other complaints from the organization NOYB concern the websites of the seven largest news magazines. Two of these complaints fall within the competence of the HmbBfDI.

In terms of content, the complaints deal with so-called “subscription models” or “payment models” on media websites.

These models represent a business model that the user
the choice between users and users of a website, either in the
Consent to the setting and reading of cookies or comparable technologies (unrestricted)
or as part of a subscription
ments for the data protection-friendly variant of the provider
to count. By general consent, users allow
and users to the operators of the media websites and their Mar
ketingpartnern a comprehensive - often cross-site - tracking of their usage behavior (tracking). User profiles that are created through such tracking in turn serve as the basis for personalized advertising.

With the complaints submitted, NOYB opposes the business model of so-called pure subscriptions. When they are used, there is already a lack of real freedom of choice as to whether users want to disclose their personal data or not

Not.

If you do not want to give your consent to tracking, it would arise
considerable effort. In terms of time, effort would have to be made
will complete the subscription. From a financial point of view, there were sometimes high burdens due to disproportionately high prices. As a result, users who do not have sufficient financial resources, for example, only have the opportunity to "sell" their data if they want to gain access to the websites

ten.

Machine Translated by Google

The violation of the requirements of the GDPR therefore lies in the fact that there is no truly voluntary consent to tracking.

Since the complaints affected various website operators fen are for which different German supervisory authorities are responsible, was discussed within the framework of the conference of the independent data protection supervisory authorities of the federal and state governments (DSK) founded the sub-working group "Subscription Models", in which the HmbBfDI participates. This is intended to create a uniform complaints office be guaranteed.

The HmbBfDI shares the assumption developed in this forum that "Subscription models" in which users have the choice have to either accept the consent to the use of cookies and comparable technologies or to use the websites with a fee-based "subscription contract" (e.g. subscription contract), are not excluded from the outset by data protection regulations. However, the prerequisite for this is that users have a real choice and that their consent to tracking is actually given voluntarily.

Regarding the question of the voluntary granting of consent the EDPB explains:

"The controller could argue that their organization offers data subjects a real choice when choosing between a service that includes consent to the use of personal data for additional purposes and a ***comparable service offered by the same controller that does not include consent to the use of data for additional purposes .*** *As long as it is possible for the controller to perform the contract or provide the services that are the subject of the contract without having to consent to the other or additional data use in question, this means that there are no longer any conditions attached*

te service is. ***However, the two services must really be of equal value." (Guidelines*** *05/2020 on consent in accordance with Ordinance 2016/679, Rn. 37, https:// edpb.europa.eu/ sites/ default/ files/ files/ file1/ edpb_guidelines_202005_consent_de.pdf)*

Other questions, such as whether consent can be given in such a general way, as is currently the case via the consent button function for pure offers, are also being voted on, as is the question of which comparative standard can be used in the assessment whether the payment option is a suitable alternative to consent.

3.9 Adaptation of the advertising guidance

The extremely practical guide to direct advertising was presented as a draft resolution to the DSK after extensive revision.

After the data protection conference (DSK) on November 7, 2018 had already published an "Orientation guide from the supervisory authorities on the processing of personal data for the purposes of direct advertising under the applicability of the General Data Protection Regulation (GDPR)", the guideline is currently being adapted following a decision by the DSK, which the working group of the DSK " Advertising and address trading" was transferred.

As a member of the "Advertising and Address Trading" working group, the HmbBfDI was extensively involved in the revision and updating of this guide. The practical relevance of the topic of direct mail in relation to compliance with data protection regulations and the need to update the guide can be seen from the large number of requests received by the HmbBfDI in the area of advertising

Machine Translated by Google

difficult to understand. It was therefore all the more important to provide those involved in the direct mail business with an updated technical application guide in order to be able to prevent the constantly growing number of complaints.

As part of the coordination among the supervisory authorities on
Adaptation of the orientation guide revealed the complexity of the
Themes arising in particular from the structure of the business
field "direct mail" in which to an advertising measure
often different responsible bodies work together.

An advertising company often does not have the information for one
The personal data of possible addressees necessary for the advertising measure and is therefore dependent on another company that acts as a seller or lessor of address databases
operated. The assessment of the responsibility of the individual actors under data protection law must therefore take into account very different factual aspects, e.g. whether only the address dealer actually has knowledge of the personal data of the

advertising addressees in detail and what role the advertise

companies in relation to the selection of personal data to be used. The assignment of the act
the companies on the different responsibilities

The GDPR thus represents a task that requires a complex and complex legal examination in order to fulfill the roles as an independently responsible body, as a processor

Art. 28 GDPR or as jointly responsible bodies in the sense
ne of Art. 26 GDPR. In front of this behind

For this reason, as part of the coordination between the supervisory authorities on the adjustment of the orientation guide, it was decided to devote separate consultation to the topic of address trading in order to avoid overloading and confusing the orientation guide on direct mail.

This created space to deal with further complex questions within the framework of the orientation aid, which arise, for example, from the different ways of direct advertising or the different

to be able to deal with advertising material in the case of direct mail in the form of letter mail, advertising by e-mail or as a sales call.
Since very different data categories are processed for the individual advertising media, the orientation guide with regard to the admissibility of the processing was about a clear and understandable presentation of the admissibility requirements for individual processing scenarios.

As a result, an orientation guide has been created that clearly presents the requirements for data protection-compliant processing of personal data by advertising companies, insofar as these act as independently responsible bodies without the involvement of third parties. At the time of going to press, the adjustment of the content of the "Guidelines for the supervisory authorities on the processing of personal data for direct marketing purposes under the General Data Protection Regulation (GDPR)" had been completed, but the formal resolution and publication by the DSK was still pending .

3.10 Google search engine

The HmbBfDI can ask Google to list search results from the Google search engine and arrange them. This occurs when those affected have asked Google LLC to list detrimental search results and the search engine operator wrongly fails to do so.

If an affected person provides Google LLC with sufficiently specific and comprehensible reasons that their personal rights are unjustifiably impaired by a specific search result, Google LLC is obliged to remove the search result from search queries relating to the person.

Machine Translated by Google

As a rule, Google LLC recognizes a violation of rights and lists the search result. In the reporting period, however, the HmbBfDI ordered Google LLC to delist search results in two cases.

In one case, when the complainant's name was entered, decisions of an EU court on a case that the complainant had brought against his employer were displayed in the search engine results. The European Court published the decisions from 2012 and 2013 without anonymizing the plaintiff's name. The HmbBfDI initially saw no violation of Art. 17 (1) GDPR by Google LLC in the display of search results, but revised this decision and ordered Google LLC to be delisted in the case of a name-based search. The court decision contained information that the complainant had sued his employer and because of which circumstances arising from the employment relationship, and how the court took these circumstances into account in its decision. This information was likely to hinder the complainant's future job search, for example. This particular because they are by mere name

plaintiff's search were displayed in the search results. Google LLC immediately followed the order of the HmbBfDI
come.

It has been German case law for decades that court judgments may only be published anonymously. The European Court of Justice (ECJ) only changed its practice of publishing decisions without anonymizing the names of the persons involved after the GDPR came into force in 2018
changes in preliminary ruling procedures. For court decisions published in the past without anonymization and still available on the Internet, there is therefore the possibility of finding them via a name search of the person concerned
to exclude a process party in the search engine.

Another order against Google LLC during the reporting period relates to the display of a job-related report about a complainant in the search results on his behalf.
The report concerns a job change by the complainant in 2009, and a photograph of him issued by his employer was also published. The order is not legally binding, but has been challenged in court by Google LLC.
Therefore, the Administrative Court (VG) Hamburg has to decide whether the search results should be listed.

Not only orders of the HmbBfDI against Google LLC, but also decisions of the HmbBfDI not to issue an order can be challenged in court (see also Chapter IV 7). The Hamburg Administrative Court ruled in June 2021 that complainants have a legally enforceable right to a decision by the supervisory authority that is free of discretionary errors regarding intervention (judgment of June 1, 2021, 17 K 2977/19). This

This view is now held by the majority of case law. The question is already before the ECJ for a preliminary decision (see VG Wiesbaden, decision of August 31, 2021, 6 K 226/21.WI). In this particular case, however, the court ruled that
a right to issue an order against which Google LLC does not exist. The plaintiff, who previously worked as a private agent, objects, among other things, to a search result in which a copy of one of his camouflage passports is shown. The VG Hamburg, like the HmbBfDI, could not see any interest in secrecy in the information on the previous camouflage identity of the plaintiff. Rather, it saw the public interest in the person of the plaintiff as overriding. The plaintiff has applied for leave to appeal.

Another proceeding, in which the plaintiff requests that Google LLC delete a search result, is still pending before the Hamburg Administrative Court. In this case, the court may have to decide whether the sub-pages linked in the source (so-called deep links) on which photos of the plaintiff are shown should also be taken into account for the delisting claim.

Machine Translated by Google

Two further proceedings pending before the Hamburg Administrative Court concern (partly former) plaintiffs working for the AfD. Here, the VG will deal with the question of whether a purely municipal activity for the AfD as a citizens' representative may emerge from a search result or whether a search result should contain a nine-year prison sentence in addition to the activity of the plaintiff for the AfD because of in the 90s offenses committed may be mentioned.

3.11 Accreditation for Privacy Certifications

According to Art. 42 and 43 GDPR, companies that issue certifications in the area of the General Data Protection Regulation must be checked and approved. In Germany, this is done by the German accreditation body together with the competent supervisory authority.

In the Activity Report on Data Protection 2020, the HmbBfDI reported that a company from Hamburg has developed a program for the certification of data processing processes in accordance with the GDPR and has applied for accreditation for this from the German Accreditation Body (DAkkS) (see 29. TB, IV 4). Accreditation is necessary before data processing based on such a program can be certified as compliant with the GDPR. The issuing organization must also be formally assessed and approved for certification.

Determining suitability for certification is called accreditation, derived from the Latin word *“accredere” – “give faith”.*

The DAkkS accredits as a government agency in German

land in a variety of areas and activities, e.g. in technical processes, laboratories or services. Here she bets

own or external experts, who regularly have to prove their competence to the DAkkS. For the area of data protection, the GDPR sees a close integration of data protection

supervisory authorities.

Since applications for accreditation not only the HmbBfDI, but a
A number of supervisory authorities have been raised at the level of the confe
close cooperation between the independent data protection supervisory authorities of the federal and state governments (DSK). The questions of practical cooperation with the DAkkS as well as the guarantee of a uniform level of testing are important

as well as the exchange between the accrediting authorities.

In this context, the HmbBfDI has contributed to the catalog of criteria, with which a uniform test standard for accreditation
ments and program reviews. (Download at https://datenschutzkonferenz-online.de/media/ah/DSK_Application Note_Zertification Criteria.pdf).

On this basis, the HmbBfDI checked and evaluated the application documents for the Hamburg company's program.
The necessary adjustments and renewed checks were well advanced at the time of going to press, but not yet complete. The technical assessment by the HmbBfDI is followed by a referral at European level before a formal accreditation can finally be granted by the DAkkS.

A GDPR accreditation procedure is a complex process for everyone involved. On the one hand, this is because the process is new and requires a lot of fundamental preparatory work. In addition, it is a powerful tool

with which considerable effects can be achieved on the market.
An accredited program can be used by the applicant company itself or by third parties to check and certify corresponding data processing processes for GDPR compliance. That of the European regulation

Machine Translated by Google

The moment of self-regulation desired by the donor can only unfold if this is done at a high professional level and without material conflicts with the supervisory authorities.

Machine Translated by Google

Machine Translated by Google

4. FINES, ORDERS, COURT PROCEEDINGS

Machine Translated by Google

4. Fines, Orders, Legal Proceedings

4.1 Fine Hamburg energy supply companies

The HmbBfDI has imposed a fine of 901,388.84 euros on a Hamburg energy supplier. The fine notice is final.

Between August 2018 and around December 2019, the energy supplier routinely checked contract inquiries from new customers to see whether they were showing what was known as “switch behavior”. Change-suspicious behavior was considered to be that one and the same customer had already concluded two contracts for the same metering point or received bonus payments of more than 500 euros. In order to determine such change-suspicious behavior, master, contract and billing data as well as payment information were checked to see whether the customer was already a contractual partner. If such change-conspicuous behavior was detected, no contracts were concluded.

Within the application form for electricity supply, customers were only informed that any bonus could only be granted if the customer did not report immediately before delivery

was supplied with electricity at the delivery point in question.
Elsewhere, too, such as in the data protection declaration in particular, there were no specific references from which customers could conclude that contract inquiries were checked using the procedure described above.

Such a comparison was made in around 500,000 cases without the
data subjects have been adequately informed and thus un

Third violation of the transparency obligations according to Art. 5 Para. 1 lit. a), 12 and 13 DSGVO. After that, personal data must
processed in a manner that is comprehensible to the data subject

be killed This presupposes that the responsible body

Machine Translated by Google

Collection of personal data provides the information specified in Art. 12, 13 GDPR. The information requirements also include stating the purposes of the processing (Art.

13 Paragraph 1 lit. c) GDPR). After that, the data comparisons actually carried out should have been disclosed.

Due to the large number of cases and the systematic violations, the initiation of fine proceedings was indicated. When determining the specific amount of the fine, it was taken into account that the violation was not very serious from a qualitative point of view, but was classified as a violation of moderate severity from a quantitative point of view.

In addition, it was a first violation by the company
mens and there has been extensive cooperation with the supervisory authority.

4.2 Fine due to defective TOM in healthcare

When processing patient health data, companies must take appropriate technical and organizational measures (TOM) to adequately protect this data. Inadequate implementation of TOM can result in severe fines.

During the reporting period, the HmbBfDI carried out fine proceedings against a Hamburg-based company that operates in the healthcare sector.

On the one hand, the company had failed to take suitable technical and organizational measures (TOM) to ensure a level of protection appropriate to the risk when employees of the company sent doctor's letters (transfer documents for communication between treating doctors). As a result, several doctor's letters were sent to a

sent to a person who, although pursuing a medical profession, was not the doctor treating these patients further. the

Rather, doctor's letters were intended for a general practitioner of the same name. To make matters worse, the company in Ver

in the past, the unauthorized recipient was informed several times about the incorrect delivery. According to their instructions, the company had provided the address satin with a blocking notice in the data processing system used. However, it failed to ensure through organizational and technical measures that the blocking notice is also adopted for software updates. After an update, the blocking notice was not adopted and the recipient again received doctor's letters about people who were not her patients. Of the

Wrong mailing was therefore due to the missing blocking notice and a failure to select the addressee by the company's employees with the necessary care. This represents a violation of the obligation of Art. 32 Para. 1 GDPR.

Even if the recipient who was incorrectly addressed was himself subject to professional secrecy and the risk of damaging use of the transmitted data can therefore be classified as rather low

the risk to the rights and freedoms of certain natural persons

When processing personal data in doctor's letters, the consequences are so significant that the data must be effectively protected.

It is expected human error that

Employees in hectic everyday life do not always exercise the necessary care when selecting addressees for doctor's letters. Appropriate technical protective measures, such as setting up a blocking notice, must therefore also be taken and it must be ensured that these technical protective measures are adopted when data processing systems are updated.

On the other hand, the company had it at a location for ei

a period of more than one year by implementing and using a logging function for reading

Access to patient data in the used

Machine Translated by Google

information system to ensure appropriate security in the processing of patient data and, in particular, to ensure and prove the long-term confidentiality of the systems and services in connection with the processing. As a result, it was not possible to trace which employees had read access to patient data.

In the case of sensitive data such as health data, in order to protect against unauthorized or unlawful processing, in addition to precautions such as access restrictions and data encryption, suitable measures are also required to subsequently check and determine whether and when personal data was processed. Logging of reading access is particularly necessary in order to ensure that the data specified in Art. 32 (1) b) GDPR

GVO to ensure the integrity of the data stored in the information system. Ensuring the requirements of Art.
32 GDPR, the person responsible has, if required, pursuant to Art. 24 para.
1 GDPR to be proven. A proof from the company there
It was not possible to say who accessed certain patient data at what time, although in one case there were concrete indications of unauthorized reading access. The company thus breached

32 para. 1 GDPR.

The HmbBfDI has imposed a fine in the low six-digit range for these violations. When assessing the fine, it was taken into account as a mitigating factor that this was a first violation by the company and that there was extensive cooperation with the supervisory authority to remedy the violations. The fact that

that the processed data is health data
acted. Thus, special types of personal data have been processed, which by their very nature are sensitive and
subject to special protection under the provisions of the GDPR
gen.

Machine Translated by Google

The company accepted the fine and waived an appeal.

4.3 Two fine proceedings against energy suppliers

In the reporting period, the HmbBfDI issued two fines, each amounting to EUR 12,500.00, against two energy suppliers based in Hamburg. The decisions are legally binding.

The background to the administrative offense proceedings was the outsourcing of the heating energy division of a large German energy supplier and the subsequent sale of the outsourced division. Customers who were affected by the transfer were informed about the transfer of their electricity supply contracts and were given the right to object.

In the event of a declared objection, no personal data of the customer should be passed on to the new company
be transmitted.

Despite duly declared objection by customers
Customers migrated to a relevant extent
electricity supply contracts to the purchaser of the heating energy savings
te. As a result, customer data was also in the cases to the new Un
transmitted to companies in which the data subjects had duly declared a corresponding objection. The causes were errors in the processing of the objections by the contract processor used by the selling company. Due to the large number of violations, fine proceedings against

initiate the companies.

When determining the amount of the respective fines, particular attention was paid to the fact that these were first-time violations and

Machine Translated by Google

extensive cooperation with the supervisory authority has taken place.

4.4 Fine for making videos of strangers' children and young women in shopping malls

The HmbBfDI has imposed the highest fine on a private person since the GDPR came into force for the illegal production of videos by third parties. However, there is no threat of an end to street photography!

In its last activity report, the HmbBfDI already reported on several cases in which private individuals took pictures of strangers on the street with a mobile phone or a digital camera with whom they had no connection (cf. 29. TB 2019, Chapter V 10). In this reporting period, too, the HmbBfDI had to initiate a corresponding fine procedure

execute.

The HmbBfDI received the process from the Hamburg public prosecutor's office to examine any administrative offenses committed by the creator of the videos under the GDPR. On a day in August 2020, a passer-by in a shopping center noticed a man who was covertly hitting young, scantily clad girls
filmed. The passer-by alerted a security officer
service of the mall about his observation. The security service employee then called the police.
During a search of the backpack, the police found a digital camera and eight memory cards. These were seized by the local police.

The seized memory cards contained a total of
156 video files created between 2013 and 2020
the. An evaluation of the video material showed that people

Machine Translated by Google

who were in Hamburg on public roads or paths and in shopping centers were deliberately and secretly filmed and the video files were saved on SD cards they took with them.

The recordings mainly showed young, female people in skimpy clothing. Some of the females captured appeared to be under the age of 14. In many cases, the focus of the recordings was on the buttocks/abdomen of those filmed. In several cases, the creator approached the people filmed to within a few centimeters and followed them with the camera through downtown Hamburg for up to 38 minutes. He purposefully overtook those filmed so that he could film them again as they passed. He also positioned himself in front of the exits of shops to see people leaving the shop

to be able to film again.

The creator of the videos processed the personal data of the young women and girls he filmed, although he was not permitted to do so either by the effective consent of those filmed or by law. The so-called household exception according to Art. 2 Para. 2 lit c) GDPR for the exercise of exclusively personal or family activities does not apply here. The HmbBfDI received a fine in 13 cases due to a violation of Article 83 Paragraph 5 Letter a) in conjunction with Article 5 Paragraph 1 Letter a), Article 6 Paragraph 1 GDPR

fine of EUR 5,000 imposed. When assessing the fine, it was taken into account that the young women and girls in these cases were being followed over a long period of time and secretly filmed at various locations. Furthermore, the creator at least accepted the fact that the persons recorded were also children. This was also taken into account. Children are given special protection by the legal system. They in particular must be able to rely on appropriate protection, as they are often not yet able to adequately differentiate between the private sphere and the social sphere and therefore do not consistently behave in a way that is appropriate to the respective sphere. The creator of the videos accepted the fine and did not appeal.

Machine Translated by Google

The decision of the HmbBfDI to punish such cases with a fine does not mean the end of street photography. Concerns expressed by photographers on social media after the publication of the 2020 activity report are unfounded. The cases pursued by the HmbBfDI are not related to street photography. These are recordings and videos of scantily clad women and children

which is secretly and apparently exclusively for sexual purposes

motifs were made. The recordings are not artistic
shear value and they should probably not under any understanding

fall under the collective term of street photography. The legal assessment of the HmbBfDI in the field of street photography is recorded in a note that is published on the HmbBfDI homepage: https://datenschutz-hamburg.de/assets/pdf/Vermerk_ Fotografie_DSGVO.pdf. According to this, the collection of data for the purpose of street photography is in most cases above Art. 6 Para. 1 lit. f)

GDPR allowed.

4.5 Fine for Disclosure of Illness
a customer advisor

Because the health data of an employee was disclosed to the customer base in violation of data protection, the HmbB fDI imposed a fine of EUR 10,100 on a car dealership from Hamburg. The decision is final.

The HmbBfDI has imposed a fine of EUR 10,110 because a nationwide car dealership group has informed the customer base of its branch outside of Hamburg that the reason for the restructuring there is the absence of the previous sales manager due to illness. The exact time when the incapacity to work began and the notification

that the situation will continue indefinitely
more than 3000 regular customers at this location

transmitted. This notification led to a particularly intensive encroachment on the rights of those affected and put a considerable strain on the employment relationship that existed at the time of the notification. Since there was no legal basis for this transfer of personal health data, it should not have been done. The company has taken precautions to avoid such a case

not repeated.

So how do you communicate restructuring in the company?
data protection compliant?
A change of personnel in the company needs to be communicated.

Employees, but also business partners and customers want to be informed about a new appointment if Kon
tact exists. Open communication should provide clarity

and prevent rumours. But how much clarity is needed and
allowed under data protection law? Belongs to a neutral and factual

Does communication also include the naming of reasons for absence due to illness?

When it comes to announcing new employees with intensive customer contact, current and new contact persons can usually be named to customers.

In the event of a temporary vacancy, the reasons for the absence should not be communicated to the outside world, much less if particularly sensitive data is involved. If there is no consent from the previous employee, there is no justification for the transmission of the state of health, which affects the core of the private sphere, due to the stricter necessity standard in employee data protection - with the exception of exceptional cases regulated by law. Customers can also be given sufficient information without notifying them that they are absent due to illness. Mentioning these reasons is important for establishing a bond with the new contact person in the company

also not required. When it comes to data protection in customer service

Machine Translated by Google

are also personal through appropriate precautions
employee data to be taken into account.

4.6 Warning regarding the intended use of the video conferencing software Zoom

In 2021, the HmbBfDI issued a formal warning to the Senate Chancellery of the Free and Hanseatic City of Hamburg in accordance with Article 58 (2) (a) GDPR. This related to the planned use of the video conferencing software Zoom. The Hm bBfDI came to the conclusion that a data protection-compliant use of the software is currently not possible due to the "Schrems II" decision of the European Court of Justice (ECJ). The warning is attacked by the Senate Chancellery before the Hamburg Administrative Court.

In 2021, the HmbBfDI spoke to the Senate Chancellery

The decision of the ECJ in the case of Facebook Ireland and Schrems (judgment of July 16, 2020, C-311/18), better known as
"Schrems II" had and still has important effects on data protection assessments throughout the European Union. Like all supervisory authorities, the HmbBfDI has the end
ECJ guidance for data protection reviews in the area of the Hanseatic City of Hamburg. At the same time, the HmbBfDI carries out numerous tests relating to this subject (see Chapters V 2.1 and V 2.2).

Third country transfer of personal data when using Zoom

A large amount of personal data is generated when using Zoom. When setting up a Zoom account, this may include a real name, a profile photo, an email address, telephone numbers or
Payment data fall. Some of this information is mandatory if, for example, it is planned to participate in an end-to-en
participate in a de-encrypted video conference. It was up to

Machine Translated by Google

Conclusion of the investigations by the HmbBfDI not recognizable, which is why there are special requirements for the profile information for better encrypted conferences. When using Zoom, the management and thus the associated data processing of the user accounts set up is always carried out by Zoom Video Communications, Inc., based in the USA.

In concrete use, a large amount of conference content is generated as personal data: audio and video transmissions, chat histories and associated meeting content. The use of end-to-end encryption, which is only available with restrictions, can ensure that this data is not disclosed to Zoom Video Communications, Inc.

Metadata is also created, ie communications are logged and user behavior when using the software and information about the hardware used is collected. This data is increasingly enriching the nut

zer account with more information and are available to the Zoom Vi deo Communications, Inc.

So since it can not be prevented when using zoom
data must flow to Zoom Video Communications, Inc
special precautions are taken to protect the data.
This necessity is a direct result of the “Schrems II” decision of the ECJ. In the opinion of the HmbBfDI, Zoom's end-to-end encryption function alone is not suitable for guaranteeing the necessary protection. Even if this function were used optimally, ie used in every meeting without exception, the profile data would remain, which is not covered by this

can become.

For administration during use, there is also the option of only specifying data centers within the European Union as processing locations. Such an agreement is intended to prevent personal data from being

Machine Translated by Google

technically transferred to computer systems in the USA.
However, responsibility for these systems remains with the US-based company. For this reason, according to the assessment of
HmbBfDI also achieved no effective protection. The HmbBfDI
follows an administrative court decision by the French Conseil d'État. Since the GDPR is one euro
If there is a European regulation that aims to standardize the application of the law throughout the European Union, decisions from other member states must also be observed, at least as long as there is no clear line in German case law, or even another ECJ decision.

The French Conseil d'État decided that due to the US law, the "Cloud Act", § 2713 Chapter 121, a location agreement is not sufficient to achieve the necessary protection. The “Cloud Act” enables US intelligence services to extract data from US companies

request, even if they are stored exclusively in cloud systems outside the USA. The separation of companies
headquarters and location of the data is therefore considered insufficient
view protective measures. The HmbBfDI therefore came to the Er
result that the use of Zoom leads to a transfer of personal data to a third country without this data being adequately protected.

A warning to the Senate Chancellery The HmbBfDI is a
supervisory authority with regard to public bodies in Hamburg, but is also particularly obliged to provide advice. It is an important concern of the HmbBfDI to ensure this advisory activity towards public authorities

liable to fulfill. After hearing about plans to use Zoom, he
had been driving, he was therefore very keen to express his fundamental concerns about its use at an early stage and to point out that the market already offers numerous alternatives,
which can be used in accordance with data protection regulations.
Unfortunately, the HmbBfDI was not able to assert itself with these concerns, so that

Finally, by way of a formal procedure, a warning was issued in accordance with Article 58 (2) (a) GDPR. With this
a supervisory authority may have been a responsible body before that
indicate that planned data processing is likely to violate the GDPR. The HmbBfDI saw these requirements as given by the planned introduction of the software as a supplement to existing video conferencing solutions.

The HmbBfDI regrets that this step – and with it the transition from advice to supervision – was ultimately necessary. Ultimately, however, the protection of personal data must be guaranteed against imminent violations of the law.

The Senate Chancellery is now having the HmbBfDI's warning checked by the Hamburg Administrative Court. The HmbBfDI sees this as an opportunity to ask a German court important questions in connection with the transfer of personal data to third countries when using video conferencing systems

to clarify. In this respect, it is a matter of principle
national and European importance.

4.7 Overview of Legal Proceedings

The HmbBfDI was also involved in legal proceedings in the reporting period. Proceedings that were pending prior to the reporting period were continued.

For example, the proceedings regarding the “Vi demo” face recognition software used by the police at the G20 summit in Hamburg in 2017 were continued (see the description in the TB Data Protection 2020, Chapter V 4). As a reminder: In the absence of a legal basis, the HmbBfDI ordered the deletion of the biometric database. Complaint against this before the Administrative Court

Machine Translated by Google

Hamburg was initially successful. Against this, the HmbBfDI has filed an application for admission of the appeal. This is to be decided by the Hamburg Higher Administrative Court. The outcome of the decision is particularly uncertain because the Hamburg police have meanwhile deleted the disputed database and thus in principle complied with the original order of the HmbBfDI. Nevertheless, from the point of view of the HmbBfDI, there is an urgent need for the open legal questions to be clarified by a higher court in order to create legal certainty for future use of comparable data processing systems for the security bodies of the FHH and - ideally - to address the problem area of biometric face recognition to the legislature

hand over.

In addition, the HmbBfDI was faced with complaints from citizens that the responsible authorities had to intervene. One focus is court proceedings involving a delisting claim against Google LLC. according to Art. 17 GDPR, i.e. they track a listing of search results within the Google search.

Here, the Hamburg Administrative Court strengthened the rights of citizens in a judgment that is not yet final. It has determined that there is a fundamental right to the HmbBfDI examining complaints as to whether Google LLC. by indexing search results, or the processing of the personal data of data subjects contained therein, violates the GDPR. In the event that the HmbBfDI determines such a violation, the person concerned is entitled to a decision free of discretionary errors with regard to the adoption of remedial measures in accordance with Article 58 (2) GDPR,

in particular a ban on processing.

However, citizens have exercised their rights under Art. 78 GDPR in other constellations as well and had the HmbBfDI's decisions reviewed by a court. affected person

Machine Translated by Google

are making more and more use of the effective instruments which the GDPR provides to confidently protect their personal rights. A lawsuit was filed against the HmbBfDI's decision not to take action in a case relating to employee data protection: A former employee contacted the HmbBfDI because she felt she was being monitored by her employer. In fact, the employee had improperly used the company car made available to her for private purposes. In addition, the hourly billing showed significant irregularities. The employer made video recordings of the private use of the company car, which the employer promised to delete as part of a labor law settlement. The Hamburg Administrative Court upheld the HmbBfDI's decision not to take action, as the surveillance measures were justified.

In another case, a plaintiff requested that an e-mail provider be issued with an order obliging it to delete an e-mail account. The HmbBfDI had previously refused to take action because the plaintiff had not sufficiently demonstrated her account ownership. The Administrative Court of Hamburg dismissed the lawsuit and ruled that the supervisory authority was under no obligation to conduct extensive, factual investigations of its own in the event of incomplete or unclear information, in particular in the very own sphere of complainants, in order to clarify the matter.

If incomplete or unclear information is not completed or clarified even when requested by the supervisory authority, although this is possible and reasonable, there is no objection if the supervisory authority does not independently conduct its own “out of the blue” investigations, but bases the facts on the facts presented Evaluate information and evaluate unclear or incomplete information to the detriment of complainants.

In contrast, the HmbBfDI only negotiated an objection to an imposed fine. The subject of this was a fine

Machine Translated by Google

due to unlawful e-mail advertising in 10 cases. During the course of the hearing, the objection was limited to the amount of the fine.
The majority of the fines imposed by the HmbBfDI were accepted by the addressees and they refrained from objecting.

Machine Translated by Google

Machine Translated by Google

CROSS-BORDER ISSUES 5.

Machine Translated by Google

5. Cross-border issues

5.1 European Activities 5.1.1 Emergency Procedure Facebook

In the spring of 2021, the HmbBfDI issued a cease-and-desist order against Facebook by way of what is known as an emergency procedure in accordance with Art. 66 (1) GDPR and subsequently Art. 66 para. 2 GDPR requests the European Data Protection Board for a binding decision.

On May 10, 2021, the HmbBfDI issued a cease-and-desist order against Facebook Ireland Limited, in which it instructed those responsible not to carry out certain processing without a legal basis. This arrangement was in accordance with the Aus

acceptance provision of Art. 66 Para. 1 GDPR exclusively for the Territory of the Federal Republic of Germany and only valid for a period of three months. It is now permanent.

The background to the order was the updated terms of use and the new data protection guidelines from WhatsApp, which users have been confronted with since the beginning of 2021. WhatsApp users were asked to agree to the new regulations by mid-May 2021 at the latest, otherwise they would not have been able to continue using WhatsApp in a meaningful way. The WhatsApp provisions that are the subject of the proceedings provided for extensive pas say, with which the person responsible, WhatsApp Ireland Limited, granted itself the right to process user data with other Face

book company to share. See Facebook's privacy policy also a general cross-company use and evaluation of data from affiliated companies.

The HmbBfDI saw the danger in the new wording that WhatsApp with the new regulations in addition to the existing exchange options with Facebook for the Pro areas

Machine Translated by Google

Product improvement, analysis, network/security, further processing options for marketing purposes and direct advertising in the future
creates and thus Facebook even more extensive data processing
gene across the different services. In our opinion, such use by Facebook would only be possible if WhatsApp users had explicitly consented to it.

The de facto acceptance of the terms of use without alternative does not replace consent under data protection law.

The HmbBfDI is responsible for Facebook in Germany, as the German branch of Facebook is based in Hamburg.
However, Facebook's European headquarters are in Ireland. The rules of jurisdiction in Art. 55, 56 GDPR and the cooperation procedure according to Art. 60 ff.

GDPR stipulates that primarily the lead supervisory authority
de, in this case the Irish Data Protection Commission (IDPC for short),
acts under supervisory law. That was not the case here, so the HmbBfDI assumed there was an urgent need for action and took interim measures.

Deviating from the regular procedure of cooperation and coherence according to Art. 60, 64, 65 GDPR, the HmbBfDI as affected
On the basis of Art. 66 Para. 1 DSGVO provisional measures against Facebook Ireland Ltd. take action to protect the rights and freedoms of German users.

Due to the time and space limitations of the temporary injunction, the HmbBfDI decided, in addition to the measures mentioned above, to request a binding decision from the European Data Protection Board (EDPB), which, according to Art.

66 Para. 2 GDPR can extend or even supplement an emergency order according to Para. 1, for example by extending the order to the entire EU area or by final measures.

The EDPB has extensive powers: While Art.
66 para. 1 GDPR provides clear guidelines for the scope of application

ger measures (limited in time and space), there are no such specifications for the scope of final measures
according to Art. 66 Para. 2 GDPR. The EDPB decides in such cases
cases instead of the lead supervisor, whether it is about the
limited scope and period of time, further, definitive measures are required. The EDPB has no competence to rule on the legality of the interim measures taken by the authority concerned. This is a matter for the national courts. Both

Procedures according to Art. 66 Para. 1 and Para. 2 GDPR are therefore self
constant types of procedures with different requirements and objectives and can also be designed very differently in the result.

For the EDPB, it was the first emergency procedure under Art.
66 para. 2 GDPR. Based on the evidence provided, the EDPB concluded that Facebook Ireland Limited with
There is a high probability that user data has already been processed by WhatsApp as a (joint) controller for the common purpose of the security and integrity of WhatsApp and the other Facebook companies and for the common purpose of improving the products of the Facebook companies. However, given some inconsistencies, ambiguities and uncertainties identified in WhatsApp's user information on the one hand and in some of Facebook Ireland Limited's written commitments and WhatsApp's written submissions on the other hand, the EDPB concluded that it was unable to is to establish with certainty what processing is actually being carried out and how. Therefore, he decided that the prerequisite

requirements for proving the existence of an infringement and an urgency were not met.

The EDPB therefore decided not to take any definitive measures against Facebook Ireland Limited in this case. However, he stressed the high probability of violations, especially in Hin
view of the security and integrity of WhatsApp Ireland Limited

Machine Translated by Google

and the other Facebook companies and with regard to the
Improving Facebook Company Products.

The EDPB also considered that this matter warrants further investigations quickly. In particular, it should be checked whether the Facebook companies carry out processing in practice that involves merging or comparing WhatsApp user data with their own data sets, which is not least facilitated by the use of unique identifiers. For this reason, the EDPB requested the IDPC to conduct an investigation as a matter of priority as to whether or not such processing activities are taking place and, if so, to determine whether they have a proper legal basis pursuant to Article 5(1)(a) and Article 6(1) 1 GDPR.

The EDPB also asked the IDPC to review the role of Facebook Ire
land Limited, i.e. whether Facebook is acting as processor or as (joint) controller in relation to these processing operations. The results of these investigations are still pending.

The first emergency procedure under Art. 66 (2) GDPR touched on a number of questions to which the EDPB has not yet found conclusive answers. For example, it remains unclear what specific requirements are to be placed on the evidence to be submitted in an emergency procedure under Art. 66 (2) GDPR if an affected person is otherwise not responsible

leading authority without extensive investigative powers
EDPB asked for a binding decision. These and more
The EDPB is likely to ask questions in a new or updated guideline on the urgency procedure under Art. 66 GDPR
respond.

5.1.2 Objections to draft resolutions pursuant to Art. 60 GDPR

One of the tasks of the supervisory authorities concerned is to examine the draft resolutions of the lead supervisory authorities. If necessary, objections according to Art. 60 para. 4 GDPR. During the reporting period, the HmbBfDI, as the supervisory authority concerned, coordinated a joint appeal by the German supervisory authorities against draft resolutions by the Irish Data Protection Commission, with different outcomes.

The number of enforcement procedures in the EU has increased overall over the reporting period. Nevertheless, even four years after the introduction of the GDPR, there are only a few draft decisions on substantial measures against powerful IT companies such as Facebook or Twitter, which have their European headquarters in Ireland and are active across borders in the EU and EEA.

It was all the more important for the HmbBfDI, as the national supervisory authority responsible and affected, to examine the long-awaited draft decisions of the Irish Data Protection Commission (IDPC for short). In almost all draft decisions of the IDPC, he came to the conclusion that a relevant and justified objection was required in order to ensure an equally high level of protection in enforcement and a uniform application of the GDPR in Europe.

The filing of an objection is regulated in Art. 4 No. 24, Art. 60 Para. 3 and 4 GDPR. According to this, the lead supervisory authority must submit a draft decision to the supervisory authorities concerned, against which they can raise a relevant and justified objection within a period of four weeks. the

Machine Translated by Google

In Art. 60 Para. 5 GDPR, the objection period is even reduced to two weeks if the lead supervisory authority submits a
submitted a draft decision that was then not yet capable of consensus.

After receiving a relevant and reasoned objection, the lead supervisory authority has two options: it can follow the relevant and reasoned objection and submit a correspondingly revised draft, or it can submit the matter within the framework of the consistency procedure pursuant to Article 65 (1) lit. a GDPR before the EDPB. It is then incumbent upon the Committee to make a binding determination as to whether the appeal is relevant and well founded, and if so, to rule on all of the issues that are the subject of the appeal.

The individual steps and requirements for filing an objection are only roughly defined in Art. 4 No. 24 GDPR. For this reason, the European Data Protection Board (EDPB) adopted comprehensive guidelines on the relevant and justified objection in the reporting period, which the HmbBfDI helped to create together with other German supervisory authorities.

For German supervisory authorities, the filing of an objection pursuant to Art. 60 (4) GDPR entails special challenges under national law: In principle, every supervisory authority is entitled to object if the requirements of Art. 4 No. 22

GDPR as the supervisory authority concerned and as such
to lodge a formal objection. On the other hand, according to § 18 Para. 1 BDSG, cooperation between the supervisory authorities of the federal and state governments in matters of the European Union as well as early involvement and coordination among the supervisory authorities is required. According to Section 19 (2) BDSG, the lead supervisory authority within Germany has a prominent role if there is a German branch, as only they process the relevant complaints.

Even if a common position within the meaning of Section 18 (1) BDSG does not yet have to be reached for an objection under Article 60 (4) GDPR, German supervisory authorities have recognized the need for a joint and coordinated approach at the European level and are under one immense time pressure,

exchange views on the submitted draft resolution and jointly file a relevant and reasoned objection. The lead supervisory authority within Germany takes over

the coordination between the supervisory authorities concerned
the. This coordination task applies as long as she intends to raise an objection herself.

Since the HmbBfDI, due to a German branch of Facebook in Hamburg, has the domestic leadership in draft decisions affecting Facebook or Instagram within the meaning of Section 19 (2) BDSG, it had several times in the reporting period

task of coordinating a joint appeal.

Two objections by the HmbBfDI primarily concerned the interpretation of the legal basis for data processing in accordance with Art.
6 Paragraph 1 lit. b GDPR, which the HmbBfDI as incorrect and not in
in line with the guidelines that the EDPB drafted. In all previous objections to the draft decisions of the IDPC, the calculation method and the assessment of the amount of the fine were also criticized. So far, the IDPC has not commented on whether they follow these joint objections. If this is not the case, these objections will also be submitted to a consistency procedure before the EDPB in accordance with Article 65(1)(a) GDPR

Need to become.

In the spring of 2021, the HmbBfDI was also intensively involved in an objection lodged by the BfDI against the IDPC's draft decision regarding WhatsApp's then new data protection declaration. Here the BfDI is in the coordinating role within Germany, since WhatsApp as a telecommunications service is assigned to its area of responsibility

Machine Translated by Google

is. Due to the connection with other services of Facebook
or meta group, these cases also have one for the HmbBfDI
high relevance. Among other things, he argued against the IDPC's assessment of the so-called lossy hashing process and spoke out in favor of evaluating the hash value used as personally identifiable data. The EDPB confirmed this view in its binding decision, which had to be taken into account and implemented accordingly by the IDPC.

The critical examination of draft decisions by leading supervisory authorities at global providers with a large user base in Germany is an important element in guaranteeing one of the central claims of the GDPR: the establishment of a uniform and high level of data protection in the European Union. About the supervisory measures taken by the lead authorities
is therefore not decided independently of the other authorities concerned and ultimately collectively. This also applies in the opposite case if the HmbBfDI or another German supervisory
authority has primary responsibility for cross-border processing.

5.1.3 European Data Protection Board

A new state representative was elected by the Bundesrat
European Data Protection Committee and thus relieves the HmbBfDI in this role.

Pursuant to Section 17 of the Federal Data Protection Act (BDSG), the Federal Council is responsible for electing the deputy of the joint representative in the European Data Protection Board (EDSA).
He did this in the reporting year and elected the Bavarian state data protection officer to this function at his 1006th meeting. This ends a long phase during which the Län

Machine Translated by Google

the representative was not occupied by a legally stipulated election, but by appointment by the data protection conference (DSK). The HmbBfDI, which has been in this role at the request of the DSK since October 2015, at that time still in the European predecessor body, which perceived the so-called Article 29 group, was thus ent loaded.

Representing the interests of the federal states and representing their areas of responsibility in the EDSA is an important addition to the work of the Federal Commissioner as a joint representative. Due to the fact that data protection supervision is organized on a federal basis in Germany, close coordination between the state data protection officers is important. The preparatory conferences and feedback on results from the EDSA organized by the HmbBfDI until mid-2021 will be continued by the Bavarian colleagues.

This gives the HmbBfDI more scope for work on the content on European level. This makes it possible to deal with a growing number of statements on draft decisions (see Chapter V 1.2) and to take on additional tasks as part of the country representation in the Social Media Expert Subgroup of the EDPB.

The HmbBfDI continued and intensified its tasks in this regard during the reporting period. In addition to the ongoing ED SA mandate on the subject of "dark patterns", the HmbBfDI took over the main reporting on the use of social networks by public authorities in July 2021. This takes into account the ECJ case law "Wirtschaftsakademie" in the matter of Facebook fan pages and the special role model function as well as the tasks of the public authorities. In addition, those affected have higher expectations of transparency and secure data processing from public bodies than from private bodies that use social networks. With the new work package, the Social Media Expert Subgroup wants to provide guidance on practical precautions that public authorities can take to ensure compliance with the

Machine Translated by Google

to ensure legislation. This also includes clarifying whether and if so, how they can use social media in a way
which is compliant with the GDPR.

5.1.4 EDSA guidelines for cooperation in the one-stop shop Mechanism

Only if strong regulation of dominant IT companies succeeds will the GDPR effectively fulfill its intended purpose. This goal is jeopardized by a concentration of responsibilities in Member States in which only manageable results are achieved. The HmbBfDI has successfully campaigned in the European Data Protection Board (EDSA) for comprehensive opportunities for the other supervisory authorities to exert influence

puts.

When enforcing GDPR requirements at cross-border
progressive cases comes to the lead authority at the place of
headquarters of the person responsible for a key position.
Only this data protection authority can take supervisory measures with Au
enacted. This is where the success of the harmonized data protection law introduced four years ago will be decided. Ironically, the IT companies with global market power have mostly settled their European headquarters in the same EU member states.

It is therefore of Union-wide importance that effective supervision is exercised there. The legislator has taken this into account in the form of the cooperation procedure in accordance with Art. 60 GDPR. The lead supervisory authority then has to coordinate the processing of cross-border cases with the other authorities concerned in other Member States. Under certain circumstances, they can force the lead authority to initiate examination procedures and also veto the results.

In practice, the enforcement of rights against internationa

Machine Translated by Google

not satisfactory for large corporations for two reasons. On the one hand, the GDPR does not have a time limit for the completion of test procedures. As a result, even four years after the introduction of the GDPR, there are only a few draft decisions on substantial measures against IT groups with significant market power. On the other hand, there have so far been differences of opinion as to the cases in which the cooperation procedure of Art. 60 GDPR applies, so that the lead authorities can be forced to take action. This has always been undisputed for complaints in which a data subject claims that their own rights have been violated. Less clear-cut cases, however, concerned e.g

wise media reports or information from whistleblowers

about planned business models with customer data, for which it was not yet known whether they had already been implemented. Corresponding information, which the HmbBfDI and other authorities concerned made known to the respective lead supervisory authorities, were sometimes not followed up there consistently. Since the decision not to initiate investigations was not reported back in the draft decision either, the other authorities had no means of enforcing an investigation by means of an objection.

To clarify the internal procedures, the HmbBfDI was one of the rapporteurs for several comprehensive internal papers by the EDPB.
This initially affects a document on cooperation under Art. 60 GDPR that is still being processed, parts of which are
Paragraphs 1 and 3 in March 2021 by the EDPB Plenary with only one

dissenting votes were accepted. The previous negotiations in the EDPB had shown that never before had an issue been so hotly contested in the committee.

In these procedural guidelines, the EDPB advocated a broad scope of the cooperation procedure. All cross-border cases where there is a lead and at least one affected supervisory authority are

accordingly to be treated in accordance with Art. 60 GDPR. This includes next

Machine Translated by Google

Constellations with withdrawn by the person concerned
Complaint also explicitly those in which the national procedure
law does not provide for a conclusion by means of a resolution. Also
Media reports or information from whistleblowers that do not
Complaints within the meaning of Art. 77 GDPR trigger the cooperation procedure if they are specific and substantiated. Not
In the EDPB's opinion, it is usually sufficient if a less detailed newspaper article is forwarded without comment. In this respect, further classification explanations are required from the sending authority. However, it is not necessary for the supervisory authority concerned to present proof that the data processing described in the newspaper article actually takes place or that it can even name the specific data subjects. Finally, it is the task of the lead authority to determine within the framework of the procedure pursuant to Art. 60 GDPR,

whether there is a violation. Whether and to what extent the lead authority initiates investigations is initially decided at its own discretion in such cases that are not complaints. Once the cooperation procedure has been opened, it has the decision not to act, but to submit it to the other authorities concerned, who can veto it. If the objection is not remedied, the EDPB can then, if necessary, enforce an examination procedure by the lead authority.

With all procedural autonomy, the EDPB emphasizes the primacy of Union law and the duty of all supervisory authorities to ensure the practical effectiveness of the GDPR. This also includes a high degree of communication and transparency. The EDPB has the requirements for early and comprehensive information

exchange according to Art. 60 Para. 1 and 2 DSGVO specified and also
The form, content and scope of the draft decisions in charge of the authorities are described in such a way that the authorities concerned can optimally contribute to the processing of the case.

In addition to the unanimously adopted Internal EDPB Document 02/2021 on obligations when processing complaints, the EDPB

Machine Translated by Google

passed another internal document on the practical implementation of the so-called amicable settlement (Internal EDPB Document 06/2021 on on the practical implementation of amicable settlements), for which the HmbBfDI was also the rapporteur.

The internal EDPB Document 06/2021 describes practical implementation options for amicable settlements when processing cross-border cases, taking into account the one-stop shop mechanism (OSS for short). According to the general understanding, an amicable settlement represents an alternative approach to dispute resolution. So if a complaint about an alleged violation of the GDPR, in particular about the rights of the data subjects, is submitted to the supervisory authority, the supervisory authority concerned can also file this complaint

Consent of the data subject Process faster as part of an amicable settlement and resolve the case in favor of the data subjects without the need for a formal remedial action vis-à-vis the controller or processor. That

The document is intended for both those affected and those

lead supervisory authorities, since the instrument of amicable settlement can be used at any stage of the complaints processing, depending on national procedural rules. An amicable agreement can be found, for example, in recital 131 GDPR, which is primarily aimed at cases with effects in a member state, or in some national procedural regulations. How the individual steps can look like in the context of the one-stop shop is explained in the document in a practical manner using case studies.

The focus of the case description is on the characteristics of the cases (ie relatively simple complaints about the rights of the persons concerned

person) who are particularly suitable for an amicable settlement.

In addition, the legal consequences, including acceptance

a draft decision of the lead supervisory authority

by affected or informed authorities, explained in more detail.

Machine Translated by Google

5.2 International Traffic

5.2.1 Third country transfer when using tracking

Through the use of cookies and similar technologies, the usage behavior of visitors to a website can be tracked across devices. With such tracking, personal data is often transmitted to third countries without the data transfer meeting data protection requirements. Within the scope of its competence, the HmbBfDI can order the suspension of such third-country transfers.

Providers of telemedia use cookies or comparable technologies (e.g. on a website or in apps) so that personal data of the users can also be obtained and processed.

The providers integrated by the website operators are often companies that are based outside of the
European Union (i.e. in a third country). This is currently particularly problematic when it comes to transmission to the USA, since the European Commission has not made any adequacy decision for such a transmission. In July 2020, the European Court of Justice declared the unhindered flow of data between the EU and the USA to be invalid in its decision on "Schrems II" (ECJ, file number: C-311/18). (https://curia.europa.eu/juris/liste.jsf?language=en&num=C-311/18). If personal data is therefore transmitted to third countries during tracking, in particular through the use of cookies, without the data protection regulations
If the requirements of the GDPR are met, a complaint can be lodged with the HmbBfDI.

As part of the processing of complaints about a transfer to a third country through the use of tracking technologies, the

Machine Translated by Google

HmbBfDI informs the website operators about the type and scope of the third-country transfer. You will be given the opportunity to provide the necessary evidence that the requirements – suitable guarantees, such as e.g. B. Standard data protection clauses, or in the event of an exception for certain cases pursuant to Art. 49 GDPR - to a lawful data transfer to a third country are fulfilled.

The conference of independent data protection supervisory authorities has decided on the transfer of personal data to third countries
federal and state governments (DSK) also as part of the revision
ten guidance for telemedia providers in December 2021. In particular, consent in connection with web tracking cannot be based on Article 49 (1) lit.

DSGVO are supported (https://www.datenschutzkonferenz-on line.de/media/oh/ 20211220_oh_telemedien.pdf, p. 32):

"It should be noted that the mere conclusion of standard data protection theft such as the standard contractual clauses adopted by the EU Commission are not sufficient. In addition, it must be checked on a case-by-case basis whether the law or practice of the third country is governed by the standard contractual clauses guarantee protection and whether additional measures need to be taken to maintain this level of protection.
The European Data Protection Board has published detailed instructions on how to proceed with the necessary examination.48 However, it is often not possible to take adequate additional measures, especially in connection with the integration of third-party content and the use of tracking services. In this case, the affected services must not be used, i.e. they must not be integrated into the website. Personal data that is processed in connection with the regular tracking of user behavior on the website or in apps cannot be transmitted to a third country on the basis of consent in accordance with Article 49 (1) (a) GDPR. The scope and regularity of such transfers regularly contradict the character of Art. 49 GDPR as an exception and the requirements of Art. 44 Sentence 2 GDPR."

Machine Translated by Google

If there is a transfer to a third country when tracking technologies are used and if those responsible cannot prove that the additional protective measures required for this are taken, this is a case
an illegal data transfer. According to the requirements of the Schrems II decision, the HmbBfDI has to suspend or prohibit the transmission (see 29. TB, Chapter IV 5).

5.2.2 Coordinated review by the Schrems II task force

In its Schrems II decision, the European Court of Justice gave the supervisory authorities a clear mandate to act. To enforce the verdict, the DSK set up a task force that is coordinating a joint investigation.

The Schrems II decision of the European Court of Justice in 2020 has had a lasting impact on the data protection landscape.
Since then, data transfers to third countries with mass surveillance without cause have only been permitted with special security measures. Not all business models can be implemented without changing the technical or location-political design (for the judgment and its effects see 29.
TB, Kapitel IV 5).

In addition to the legal requirements for responsible bodies, the Court of Justice has formulated the clear expectation of the supervisory authorities to also implement these bindingly and across the board. in the
In the event of complaints from those affected, it has reduced the discretion of the competent authorities to make decisions. In order to create market equality and to achieve broad enforcement, the DSK set up a task force to deal with the Schrems II decision. Its task is to develop and implement a common, nationwide enforcement strategy, which is also communicated to the European supervisory authorities. the lei

Machine Translated by Google

Management of the task force is the responsibility of the HmbBfDI and the Berlin Commissioner for Data Protection and Freedom of Information. The Berlin colleagues are concentrating on the legal interpretation issues that follow from the judgement, while the HmbBfDI is dealing with the nationwide
Test action coordinated.

The legal analysis includes, among other things, an examination of the security laws of the USA in order to understand the scope of the Court's remarks for other companies

average For this purpose, the task force received an expert opinion from Prof.
Stephen Vladeck of the University of Texas. The legal expert had previously acted as an expert in the Schrems proceedings for Facebook. According to his findings, the scope of application of the US surveillance laws is much broader than previously assumed in Europe. So

can the constituent element of the electronic communication
service, depending on the individual case, also applies to companies in all sectors if they use the corresponding internal software products. It is planned to publish the report in early 2022.

Ten countries take part in the test campaign led by the HmbBfDI
data protection authorities and a church supervisory authority. In
In a joint vote, the task force agreed on five case groups, which are checked in the respective area of responsibility. Uniform questionnaires were developed for each case group and published at www.datenschutz-hamburg.de/pages/fragebogenaktion/. It is up to each participating authority to decide for itself which of the questionnaires to use and how many addressees to write to. The case groups of web hosting and mail hosting were selected because service providers from third countries are often used for this, while adequate European alternatives exist and a change is relatively uncomplicated and possible in a timely manner. Due to the special need for protection of applicants, applicant management systems are also considered. Another questionnaire concerns web tracking in view of the practical relevance of The

Machine Translated by Google

mas. In addition to the use of the external service providers mentioned
also the exchange of customer data within the group
of a group of companies as a further case group, since the Schrems decisions of the European Court of Justice are based on such a constellation.

The participating supervisory authorities assess each case individually based on its uniqueness and make independent discretionary decisions. To ensure that this takes place in a coordinated manner, they exchange information on the status of the procedures and how the responses from the responsible bodies are being handled at regular meetings. On the one hand, legal issues can be evaluated in a uniform manner in this way, on the other hand, procedural issues such as the granting of implementation deadlines for rectifications can also be coordinated in this way.

In the first step, the HmbBfDI wrote to 23 Hamburg companies. In seven procedures, he used the web hosting questionnaire. He concentrated on the websites of market-relevant online shops. In view of the importance of Hamburg as an important, nationwide mail order location, all the key players in the industry are examined. Twelve companies received the questionnaire on intragroup data traffic and the questionnaire on applicant management was used four times. Findings from a comparable action from 2015 after the Schrems I decision were evaluated to select the addressees of both case groups (on the review at the time, 25th TB, Chapter X 1; 26th TB, Chapter IV 4). This made it possible to write to the responsible departments where there is reason to assume that they are actually carrying out the data processing to be checked.

Due to the great complexity of most of the answers, the tests in Hamburg are still ongoing. First findings show a
differentiated picture. While the answers partially discernible
give that so far not even a satisfactory off

Machine Translated by Google

After dealing with the new legal requirements, other responsible persons sometimes present well thought-out and effective solutions for the implementation of the requirements of the European Court of Justice. Where there are still deficits, an end to the data protection violation should first be brought about in a cooperative dialogue. If this is not successful, administrative measures may be necessary.

Machine Translated by Google

Machine Translated by Google

Machine Translated by Google

ADVICE TO PUBLIC AUTHORITIES 6.

Machine Translated by Google

consultations with public authorities

6.1 Health data in the IT procedure “digital aid”

The authentication process of "Beihilfe digital" does not meet the requirements of the state of the art.

Article 9(1) of the General Data Protection Regulation makes it clear that health data is particularly sensitive data. This is a consensus in many areas, for example in the patient file and in the practice information system. This does not only apply in the health sector, but whenever healthy

security data are processed.

Large amounts of health data are also processed in the administrative area when processing benefits. In this process, sensitive health data such as copies of prescriptions and doctor's bills are transmitted and stored, which not only originate from the treatment by a doctor, but from the various treatment contexts of a person. in the

Over time, the data from several years come together here

men. Data that has already been submitted electronically can also be called up again via the Internet using the “Digital Aid” procedure.

The HmbBfDI has the Center for Personnel Services (ZPD) of the FHH from

It was pointed out from the beginning that such a retrieval requires, in particular, a 2-factor authentication using a hardware token
requires. The online ID function is particularly useful for this

Question that is already used as a means of authentication in other procedures of the Hamburg administration.

In the course of further consultation, the HmbBfDI examined “digital aid” to determine whether and, if so, under what conditions, an appropriate level of protection can also be achieved with 2-factor authentication using a software token. To

Machine Translated by Google

In the opinion of the HmbBfDI, a software token can only be used if the persons concerned are offered this option as an additional option in addition to authentication with a hardware token that corresponds to the state of the art. On the basis of detailed information about the various options, those affected can then decide which means they would like to use in individual cases

in. This position of the HmbBfDI also takes into account the change in § 336 SGB V made in autumn 2020, with which access to
an electronic medical record for those affected in the way
was regulated that in addition to the authentication process with the
Health card (hardware token) can also be offered an authentication process with a software token to those affected if you tell them about the additional risk involved

en clarified. The legislature has created this option for access to the electronic patient file, in which sensitive health data is processed in a manner comparable to that of “Behilfe

digital" (vgl. 26. TB, Chapter VI 2).

In order to ensure that only authorized persons access this data, registration and registration in the procedure corresponding to the high level of trust is an appropriate technical measure that corresponds to the state of the art. here

You can refer in particular to Technical Guideline TR-03107-1 of
Federal Office for Information Security (BSI) ver
be shown. The aim of this technical guideline is to
electronic identities and trust services for various
Assess e-government processes and trust levels
to assign. These solutions cover different identity management processes at different security levels. The IT planning council also uses this guideline to derive the requirements for means of authentication (see table on next page).

Machine Translated by Google

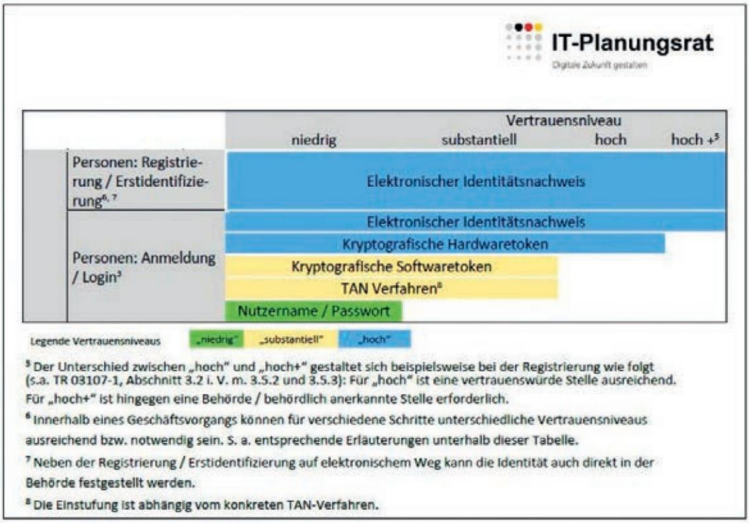


Tabelle: Einordnung der Prozesse in die jeweiligen Vertrauensniveaus Einordnung der Prozesse in die jeweiligen Vertrauensniveaus (Ausschnitt; Quelle: Empfehlungen für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern bzw. der Wirtschaft Handreichung, Stand: 24.02.2020, Version 4.00 ; IT-Planungsrat)

The online identification function of the ID card is particularly suitable as a cryptographic hardware token: the ID card is held up to the smartphone or the card reader and after the PIN has been entered, the required data can be read out securely. Possession (of the ID card) and knowledge (of the PIN) are required.

In this reporting period, too, the ZPD took the view that its solution corresponds to the state of the art in accordance with Art. 32 and 25 GDPR, without naming a source that shows that the necessary requirements are also guaranteed with a software token. The ZPD does not consider the integration of a hardware token to be necessary. Why the sensitive

The health data of the employees of the FHH are not protected to the same extent as the health data of citizens in online services under the Online Access Act is therefore still an open question.

Machine Translated by Google

With this dissent between the ZPD and the HmbBfDI we have
the consultation phase is over. Since the operator of the app and the ZPD have announced that they will "keep an eye on developments in the state of the art", the HmbBfDI continues to see the opportunity
that the registration process for "digital aid" has a high degree of certainty
safety level can be achieved. Sign up for health insurance companies
Corresponding developments are taking place in comparably sensitive applications. This will be an opportunity for the HmbBfDI to continue to talk to the ZPD about "digital aid".

6.2 Digital Personnel File

After the nationwide introduction of electronic file management for the factual and specialist file management of the FHH (EL DORADO), the personnel files and the processing of personnel processes are now to be digitized. When implementing the electronic personnel file, special data protection requirements must be observed.

Personnel administration at the FHH is organized on a decentralized basis, ie the authorities, offices, state companies and institutions usually have their own personnel departments. Previously, the personnel files there were kept on paper. This shall be changed now.

The aim of the Digital Personnel File project is the digitization of paper-based personnel file data and their continuation as digital personnel files (DigiPA). This includes the initial digitization of the existing personnel files by a scanning service provider, including the transfer to the file system and the continuation of the digitization of personnel processes for the DigiPA.

The principles of personnel file management, in particular the applicable legal requirements, remain in place through the introduction of the

Machine Translated by Google

digital personnel file management unaffected. This applies in particular to the principles of transparency, completeness, correctness, admissibility and confidentiality of personnel file management. That is, when digitizing personnel files

as well as the processes based on it are various legal ones
Particularities to be observed by technical and organizational
ical measures are to be implemented in the new IT process.

In addition to the legal admissibility of automated processing of personnel files, the prerequisite for keeping a digital personnel file is quality-assured digitization of the existing files. Just as with the subsequent scanning in the processing of personnel processes, it must be regulated and specified how the original documents are handled, ie whether and when they are destroyed. The requirements from the technical guideline of the Federal Office for Information Security BSI TR-03138 "Replacement scanning

(RESISCAN) must be observed. Just like quality-assured digitization, the possibility of completely deleting documents from the personnel file must be created before digitizing personnel processes. According to the current status of Eldorado 2.0, such a deletion is not yet possible, but should now be implemented promptly. We will do our best to ensure that a rollout only begins when this extension is productively usable in Eldorado.

The file structure standardized according to the requirements of the Hamburg Civil Servants Act, in particular the division into a basic file and several sub-files, must be implemented accordingly.

The digital personnel file of the FHH was developed on the basis of the document management system ELORADO 2.0, in which the personnel files are to be managed. Since access to personnel files is only permitted for certain groups of people, the authorization and role concept and its implementation are also of crucial importance. So will the call

Machine Translated by Google

of the DigiPA can only be carried out via the leading personnel management of the FHH (KoPers) and the access rights there have been followed.

The HmbBfDI was informed about the project at an early stage and was involved bound and is constantly in a very constructive end

exchange with this project.

6.3 IT procedure “My Personal Data”

The “MeinePersonaldaten” (My personal data) procedure is intended to enable employees and pension recipients at the FHH to access their own personal data and, in the future, to simplify processes in personnel administration. The sensitivity of the data requires adequate data protection measures.

In the context of personnel administration, personal data of varying sensitivity are processed, the disclosure of which is obligatory for the employees. This includes, for example, name, place of employment, private address, date of birth, personal number, tax number, social security number, church affiliation, salary group, marital status, account number, but possibly also particularly sensitive data such as entries on severe disabilities and garnished wages. While previously only employees within the personnel administration departments had access to the data stored in the personnel management system (KoPers), this will for the first time be accessible to persons outside of personnel administration via the Internet and the intranet.

"MeinePersonaldaten" is a platform through which the employees and pension recipients of the FHH can, in the first phase, submit their payslips or pension notifications as well as tax and social security documents via the Internet or the

can view and download on the intranet. In the 2nd phase should

Machine Translated by Google

also allows changes (e.g. address changes or changes to the account number) and the uploading of documents
will.

The level of protection of this data places corresponding demands on the identification and authentication solution to be used.
It must be ensured that only employees and pension recipients can access their own payslips.

The HmbBfDI has been supporting the process for about 2 years and, due to the sensitivity of the data, advocated 2-factor authentication very early on. Fortunately, this was also implemented by the project for access via the Internet.

Access from FHH workstations via the intranet/FHH Net has now been greatly “simplified” conceptually. This should enable access without explicit registration by the user and without the need for additional registration in the process (single sign-on). This means that access is only secured by the user ID and password of the Windows account. Here, the HmbBfDI continues to advocate for additional technical and organizational measures. This could at least be a procedure-specific password that those affected assign instead of using the single sign-on.

The terms of use of the procedure have so far stipulated that the participants must give their consent to the data retrieval and thus to the processing by MeinePersonaldaten if they want to use digital access to the MeinePersonaldaten service themselves and register for it. However, this is not a conditional activation of the personnel cases for external retrieval by setting a corresponding indicator (flag) only after the consent of the person concerned (opt-in), but rather the consent to the actual processing using the "My Personal Data" procedure. Rather, all databases

Machine Translated by Google

connected to the process even before individual registration and then activated by the respective registration of the employees.

No separate “online database” was provided for online access by employees and pension recipients, which would ideally only contain the data of those who want to use this procedure and have consented to the online availability of their data. The activation of the data and the associated risks basically affect all employees and service recipients of the FHH - regardless of their actual intention to use it.

If you do not agree to the activation of your individual personal data for online access, you can currently only have it blocked by Human Resources (opt-out). A technical function is to be created for this in the future. However, this blocking always refers to the person stored in KoPers and the associated employment relationship, regardless of the type of access. This means that you either accept both access paths or neither. This means, for example, that access from the Internet can be secured with a high level of protection by means of

Online identification function of the ID card not exclusively active

fourth without having to accept weaker access options from the intranet.

The HmbBfDI will continue to advocate data protection-friendly solutions deploy.

Machine Translated by Google

6.4 Updates on User Accounts and OfA Services

With a user account, citizens will in future also be able to use the online services of all other federal states and the federal government. At the same time, the Senate Chancellery announced that the standards for cross-state use should not apply to use within Hamburg.

Current status of user accounts:

The nationwide digitization of public administration is progressing in small steps. For this purpose, the Online Access Act (OZG) was updated in December 2020. One goal of this update is that citizens with a

User account of a federal state or the federal government also all On
line services of the other federal states and the federal government
can. So you only have to register once. The data is processed on the basis of Art. 6 Para. 1 e) GDPR, in conjunction with Section 8 Online Access Act (OZG), Section 4 Hamburg Data Protection Act (HmbDSG) and Section 25 Telecommunication Telemedia Data Protection Act (TTDSG). . These regulations form the legal basis for storing personal data in the user account. The intended use of the data has been expanded to include storage for cross-border use. However, such storage only takes place if a user individually agrees to this storage or, as worded by the legal text, "consents".

The person concerned must also agree to the transmission of data from the user account to an online service in accordance with Section 8 (5) sentence 1 OZG. The HmbBfDI has worked to ensure that this consent only applies to the respective individual case and that the user is specifically shown which data is to be transmitted to the online service in this individual case. So he can before

Check whether this data is still up-to-date and correct it if necessary.

Machine Translated by Google

intervene to correct. This regulation serves in particular to ensure transparency. The project group of the IT planning council, in which the Ver responsible for user accounts of all states and the federal government ten has taken up this suggestion and decided to use the data in the user account across countries.

However, the situation is different when using the data stored in the user account for the use of an online service within the same federal state. Those responsible could not agree on a uniform procedure for this case constellation. In 2021, for example, the Hamburg Senate Chancellery long held the legal opinion that the internal transmission of data to a Hamburg online service does not require approval in each individual case. It is also of the opinion that the user does not have to be shown this data when the data from the user account is transmitted to the online service. From the point of view of the HmbBfDI, the OZG does not offer any indication that would justify such a disadvantage when used within Hamburg. The different approach is neither legally justifiable nor is it transparent for those affected.

Shortly before the editorial deadline, the HmbBfDI received a letter from the Senate Chancellery on request, which stated that the user would then also be shown an overview of all data that was sent to a Hamburg online service. This is an implied consent that takes into account the requirements for consent within the meaning of the OZG and the GDPR. Even if the discussions on this have not yet been concluded, there are signs of an understanding on this point.

In the future, the user account will also contain a mailbox via which the decisions of an online service, such as a notification of an application, can be sent to the person concerned. This aspect was also newly regulated with the update of the OZG 2020. Here, too, the user's mailbox may only be used for the notification delivery if he explicitly agrees to this form of notification delivery. This is regulated in § 9 OZG.

Machine Translated by Google

In the opinion of the HmbBfDI, this approval must also be given in each individual case. The Federal Ministry of the Interior, Building and Community also represents this legal opinion. The reason for this is that with the passing of the new § 9 OZG, the user was required to be solely responsible for regularly checking whether there was a new inbox in his mailbox.

As a rule, the user is informed by email about such a new entry in the inbox of his user account. It is of great importance, however, that a decision is also deemed to have been delivered if it has arrived in the inbox of the user account, even if the user was not informed of this receipt. In addition, deadlines begin to run immediately upon delivery, within which the user must, for example, lodge an objection. So it can be good

that a user with the data from his user account

would like to submit an application, but does not want to or cannot carry out this regular additional check of an inbox in his mailbox. In such cases, the notice would be delivered via a different route, such as by post.

Regarding this question, there is currently between the responsible

There is still no consensus between the federal states and the federal government. The cross-country

Due to this open legal question, effective use is likely to be delayed until well into 2022. The Hamburg Senate Chancellery has also announced that it will require individual-case consent for the delivery of notifications

does not consider it necessary and at least for the innerham

Burgische application will not be realized. Despite repeated inquiries, the HmbBfDI has not yet received any explanation of the legal basis on which the Senate Chancellery bases its interpretation.

The user account is intended to provide a secure, data protection-compliant and user-friendly option. je

according to service, data with very different sensitivity

processed. In order to be able to meet these different requirements, the legal bases provide for different levels of trust when registering. That is to be welcomed

Machine Translated by Google

the Senate Chancellery has long since included the online identification function of the ID card as an option when registering for the user account. However, other variants that are relatively widespread are not yet available and are not planned for 2022 either. An example of this is the Elster certificate, which is known from the electronic submission of the tax return. Since the OZG update 2020, this certificate can also be used for the authentication process when logging into the user account. There are still no plans as to whether and when this variant can be used for logging into the user account in 2022. This also applies to the new Smart eID and to 2-factor authentication with an authenticator app, which is known from online banking, for example, and which increases the security when registering compared to simply entering the user ID and

Password significantly increased.

To the OFA services:

The Online Access Act obliges the German administration to also offer its services to citizens and companies digitally by the end of 2022. 575 OZG services, consisting of more than 5,000 different individual processes, must be digitized in a user-friendly manner and without media discontinuity by the end of 2022.

This large number was assigned to subject areas. One federal state or the federal government **("Einer")** takes the lead in developing the online procedures for a subject area. The programs developed in this way are then available **"for everyone"** for further use. "One for all" (EfA) is a comprehensible approach in a federal structure, which not least

ensures a uniform level of data protection. The devil is stuck

in detail. There are still more descriptions of open legal questions and especially open data protection aspects than answers. Concepts for the technical implementation of an EfA subsequent use have not yet been made available to the HmbBfDI despite inquiries. Nevertheless, the HmbBfDI will continue to work constructively on the data protection-compliant digitization of the Ver

Machine Translated by Google

participate in administrative action. Even if there is still a long way to go before the statutory target, according to which the federal states should have completed implementation by the end of 2022.

6.5 Childhood-Haus

In late summer 2021, the HmbBfDI was consulted on the introduction of a video interrogation system in the so-called Childhood House (CHH). The CHH was set up at the University Hospital Hamburg-Eppendorf (UKE) to examine, advise and interview children and young people who have been victims of or witnessed abuse, sexualized violence or neglect in a child-friendly environment and in an interdisciplinary manner under one roof be able. The Authority for Justice and Consumer Protection (BJV) and the Hamburg police are responsible for the conception of the video interrogation system and asked the HmbBfDI for a prior assessment of the technical and legal design.

In its press release of October 21, 2021, the UKE presents the new competence center for child protection. In it, Prof. Dr. Ondrus chka, Director of the Institute for Forensic Medicine of the UKE:
*"Child protection concerns us all. We all need to ensure the protection of the youngest and most vulnerable in our society. We are very pleased that we are now taking another important step for our city with the Childhood-Haus Hamburg as a competence center for child protection at the UKE. For everyone involved, the ultimate goal is to avoid re-traumatization of the children and to make the examination processes as child-friendly and efficient as possible." (https://*www.uke.de/allgemein/presse/pressemitteilungen/detailseite_112971.html)

Children and young people should be in the familiar surroundings of the CHH as part of investigations by the responsible authorities

Machine Translated by Google

can be questioned in a child-friendly atmosphere and environment. The interrogation room in the CHH is to be equipped with cameras and microphones. The police and, if necessary, the public prosecutor's interrogations should be audiovisually documented or transmitted in real time to the criminal justice building in the course of court proceedings. The transmission can be controlled from an adjoining room or the data can be stored on a data medium. The project pursues the goal of structuring the necessary surveys and interrogations for children and young people as gently as possible.

Under this condition, the HmbBfDI was invited by the lead BJV in September 2021 to a meeting with the Hamburg police and those involved from the judiciary to discuss the basic data protection requirements in general and the technical and organizational measures to protect the to talk about the children's personal data as part of the video interrogation in the Childhood House.

In the course of this initial consultation, various aspects were discussed, in particular the installed technical (Videokon
reference) systems and workstations.

The question of data protection responsibility was also discussed intensively. Responsibility for Compliance
of data protection and the protection of the rights of those affected
Persons lies with the so-called responsible person, who is assigned various obligations by law. Due to the large number of participants in the project – including the police, the courts, but also the UKE – and the varying amounts of contributions and actual opportunities for influence and influence of each individual participant, determining who is responsible under data protection law is complex. If several parties are involved in a data protection project, it is possible that there are several responsible persons and that these are so-called joint responsible persons (§ 63 BDSG), or one or more participants as processors

Machine Translated by Google

(§ 62 BDSG) for the (joint) responsible person the data
en process.

Responsible in the sense of data protection law is any authority, institution or body that alone or jointly with others decides on the purposes and means of processing personal data (§ 46 No. 7 BDSG). Processor is any authority, institution or other body that processes personal data on behalf of the person responsible. If there is joint responsibility, in addition to the obligations assigned by law, the other requirements under § 63 BDSG must also be observed; in the case of order processing, the specifications according to § 62 BDSG.

Based on the information provided at the time of the first integration, the HmbBfDI was initially not in a position to clearly assess which role was played by which party and which data
intellectual property issues still require further clarification between the parties involved. At the beginning of October, after consultation with the parties, the HmbBfDI then sent an extensive catalog of questions with the aim of making these open data protection issues tangible for the bodies involved in the process and enabling better assessment and coordination among themselves.

In addition to clarifying who is responsible, the question of adequate logging was also particularly important to the HmbBfDI, the access to the systems and the associated use as well as inspection of the stored videos

documented. This is to control data protection law
Operations according to the requirements of § 76 BDSG required. In a follow-up discussion with the BJV, the HmbBfDI was presented with a logging solution that enables these processes to be checked. A logging concept, which also includes the planned evaluation of these log entries, is to be developed

will.

Machine Translated by Google

The HmbBfDI has also advised, among other things, that the technology used, the existing interfaces and the regularly held finding related data flows to clarify and a detailed deletion concept for the personal data create.

Both the police and the BJV have dealt very intensively with the questions raised and the answers made available to the HmbBfDI. As a result, it can be stated that measures have been taken to ensure the protection of those surveyed: access to the rooms is controlled by the CHH's case management, the hardware is located in locked cupboards, data carriers are encrypted and there is a video conference insulated and transportable

encrypted via the FHH network. For the video conferencing switch the Skype for Business operated by Dataport is used, so that no further external service providers are included in this communication tion to be included. The recording of an interrogation can be transmitted to the judiciary via the FHH network in transport-encrypted form. Police interrogations are transferred to portable data carriers, which are included in the investigation files together with transcripts of the audio recordings.

After evaluating the feedback, however, there were still various open questions that the HmbBfDI believes must be clarified between the parties involved. At the time of going to press, for example, it still needs to be clarified to what extent the UKE itself is involved in the process, since it makes the premises available and also takes on the access management. The specific technical design of the necessary client separation for restricting access to the video recording was also the subject of discussions between the police and the BJV. The same applies to the planned automated deletion of recordings on the computers in the CHH. An exact time window has yet to be determined and documented.

Machine Translated by Google

As a result, the HmbBfDI welcomes the early involvement in the
Procedure, since it was still possible to exert influence and data protection requirements
became the focus of planning
became.

6.6 ITS Congress / Transport Projects

Particular importance is attached to the consideration of data protection and data security when it comes to Intelligent Transport Systems / Intelligent Transport Systems (ITS).
In the reporting year, the ITS World Congress took place in Hamburg. The HmbBfDI has accompanied individual ITS projects in an advisory capacity and sensitized those responsible for the project to create a balance between data protection and the goals of efficient, safe and "smarter" usable and thus, among other things, more environmentally friendly mobility.

Particular importance is attached to the consideration of data protection and data security when it comes to Intelligent Transport Systems / Intelligent Transport Systems (ITS).

In the reporting year, the ITS World Congress took place in Hamburg. The HmbBfDI has accompanied individual ITS projects in an advisory capacity and sensitized those responsible for the project to strike a balance between data protection and the goals of an efficient,
safe and usable in a "smarter" way and thus, among other things
to create more environmentally friendly mobility.

The ITS World Congress is the world's largest event for innovations in the fields of mobility, logistics and IT. Each year a different city hosts the congress and in September 2021 Hamburg became the exhibition venue for a week. Extensive press coverage accompanied the most important events and announcements related to the congress. As a host, Hamburg made an effort with innovation and lighthouse pro

Machine Translated by Google

projects to emerge. In this context, the HmbBfDI was available in advance to advise various city projects and was able to gain an insight into the developments in industry and research during the congress. Many of the scientific lectures, discussions and product presentations showed how the future of the transport sector can be written. For the citizens, this can be done, for example, by

increased comfort with automated driving and smarter traffic leadership become noticeable. On the other hand, there are new dangers from the possibility of monitoring people and new ways of cyber attacks on networked infrastructure and vehicles. In addition to many approaches to make traffic and transport more environmentally friendly, the main focus is on generating, exchanging, collecting and interpreting data. If a vehicle constantly collects information about the driver, such as seating position, alertness, reaction times, tension and stress level, but also records and shares data about other passengers and the environment, this can lead to increased safety for all road users. The manufacturers promise that the newly acquired amount of data will benefit them – but also third parties such as

Insurance companies - this information from elsewhere value and to be able to continue to use them lucratively under certain circumstances.

It was heard from various sides, collected data sets are often not accessible to everyone due to a lack of standards and closed systems or cannot be integrated into services. It was reported, for example, that when a city wants to propagate certain alternative routes to promote the flow of traffic based on measured traffic volume, the manufacturers of frequently used car navigation systems lack the will to cooperate. The city needs to find other ways to

to inform road users.

The HmbBfDI was able to exchange ideas with transport authorities and companies. Various concepts are used in almost all conurbations with high traffic volumes

Machine Translated by Google

looking for solutions in the areas of mobility, logistics and IT.
Thanks to the nature of the trade fair, discussions with manufacturers of Hard- and software often an informative demonstration
of products and services. This was particularly helpful for future consultations and tests with regard to the planned use of these products in Hamburg.

As part of the ITS Congress, the FHH presented 42 so-called anchor projects for the six fields of action named in the ITS strategy: intelligent vehicles (automated and networked driving), data and information, intelligent traffic control/steering, intelligent infrastructure, intelligent parking and mobility as a service were presented.

In the run-up to the projects mentioned below, there was an extensive exchange between the project managers and the HmbBfDI, which acted in an advisory capacity. With regard to the projects that are being continued or are still being implemented, the consultation will continue beyond the reporting period.

6.6.1 Hamburg Electric Autonomous Transportation (HEAT)

The HmbBfDI has already reported on the HEAT project, an automated minibus in the HafenCity, based on the basic advice given in the past (cf. 27. TB, Chapter V 2.2.1) . This is a research and development project by Hamburger Hochbahn AG and other project participants, as part of which the use of such a bus in local public transport was to be tested. In what is known as the third integration stage, HEAT was on the road in passenger operations shortly before and during the ITS Congress. In view of this, it was also relevant from a data protection point of view that the

Bus with different cameras - outside and inside
- is equipped, the latter combined with the possibility of event-related observation by the control center.

Machine Translated by Google

When the project was presented, questions were discussed with those responsible for the project, above all with Hamburger Hochbahn AG, in particular on the legal basis for the data processing associated with HEAT and on transparency for users and for those involved in traffic who are passively affected. This went through the different integration stages and resulted in an on-site appointment in July 2021, at which the technology used could be inspected and employees of the project participants answered questions from the HmbBfDI. In addition, additional documents were made available, documents revised and more transparency created for those affected – by means of further information on and on the bus, at the bus stops and on the website

of Hamburger Hochbahn AG.

HEAT is currently suspended. A decision on whether to continue the project is expected to be made in spring 2022
will. Then the HmbBfDI HEAT would continue to be advisory

to accompany.

6.6.2 Check-in/Be-out – hvv Any function in the hvv switch app Check-in/Be-out (CiBo) is a new procedure with which Hamburger Hochbahn AG allows users would like to make it possible in the future to have the cheapest tariff determined and paid for the transport services used. This is to be done on a smartphone using the hvv Any function in the hvv switch app. For this purpose, Bluetooth signals, so-called beacons, are sent out by bus stops and vehicles and processed by smartphones. Users of Hamburger Hochbahn AG must also grant access to other system services, such as GPS and motion sensors.

The processing of corresponding transaction data should only take place if the users expressly and
informed have given their consent and exclusively for Ver

Machine Translated by Google

performance. The creation of movement profiles is expressly not the purpose of processing the corresponding location and movement data. This is to be ensured by technical and organizational measures, such as pseudonymised processing and the timely deletion of transaction data after billing.

The HmbBfDI held talks with those involved in the project in particular on these technical and organizational measures and on how to deal with interruptions in the mobile phone connection or errors/crashes in software and operating systems. In connection with this project, too, if the procedure is to be used from spring 2022, it will be a question of ensuring transparency and providing users with all the necessary information on the functionality so that they can be informed about the use of the function hvv Any ent

can divorce. For this there will be further exchange between the HmbBfDI and Hamburger Hochbahn AG.

6.6.3 Smart delivery and loading zones (SmaLa)

In 2021, the Ministry for Economics and Innovation (BWI) launched a pilot project called SmaLa, which is intended to test how delivery and loading zones in urban traffic can be used more efficiently. Parcel service providers, couriers or suppliers can use a digital booking system to reserve four model loading zones with eight parking spaces in the Hamburg-Mitte district in the first project phase. These are zones in the absolute ban on parking, which is for the

booking period, i.e. the period of the expected delivery, has been overridden in a way that is understandable for the law enforcement officers who are checking it.

Within the SmaLa app, registered (test) users can store one or more license plates in combination with information on the respective vehicle length and the average booking duration. If a booking is made for a license plate,

Machine Translated by Google

generates a ticket ID, which is displayed in the app and in abbreviated form on the digital signs set up to identify the Smart Delivery and Loading Zones.

Parcel service providers, couriers or suppliers are the target group of SmaLa and test users of the booking system
usually companies in focus. Insofar as the vehicles whose license plates are stored in the app are registered with companies - and thus legal entities - the processing of the corresponding data relating to the booking of the loading zones does not fall within the scope of the GDPR. Because the GDPR does not apply to the processing of personal data of legal persons and in particular companies established as a legal person, including name, legal form or contact

data of the legal entity (see recital 14 of the GDPR).
Insofar as the GDPR applies because a natural person registers for the SmaLa app and deposits a license plate number there, the processing of the data in connection with this takes place for the purpose of fulfilling the contract and on the basis of Art 6 paragraph 1

lit. b DSGVO.

The project is evaluated purely statistically. A combination with the registration codes does not take place, so that no conclusions can be drawn about the booking behavior of a specific driver.

In phase 2, the project is to be expanded to include up to 25 smart delivery and loading zones. In addition, the zones will be equipped with lowerable bollards, for example. Consideration is being given to realizing such an automatic system with the help of cameras that capture the license plate numbers of the approaching vehicles and record them match the license plate number for which the delivery and loading zone booking was made. Because license plates of uninvolved private vehicles would probably also be recorded, the HmbBfDI suggested other implementation options, e.g. via the app

Machine Translated by Google

consider. The HmbBfDI will also provide advice on how this equipment can be implemented in compliance with data protection regulations in 2022
To be available.

6.6.4 Probe Vehicle Data (PVD) in the test field for automated and connected driving

The approximately 9 km long test track for testing the automati
ated and networked driving at the FHH was already a topic at the
Activity reports of the HmbBfDI from the years 2018 and 2019 (cf.
27. TB, chapter V 2.2.1 and 28. TB, chapter V 2.1). Most recently, the focus was on equipping the traffic light systems on the test track with so-called roadside units, via which the traffic light phases are transmitted unidirectionally to vehicles that are ready to receive them (infrastructure2vehicle communication). This is from the data point of view

Protection is usually not a problem, since this does not result in the processing of personal data.

In the reporting period, the task was to test to what extent the Cooperative Awareness Messages (CAMs) that are relevant for communication in this area and that modern vehicles send out are
Roadside ITS stations can receive and the information they contain can be evaluated to improve the traffic situation analysis – in addition to the technology previously used for this, such as induction loops or thermal imaging cameras (Vehicle2Infrastructure communication). When transmitted by radio

NEN CAMs are status information, among other things
about the traffic flow, the vehicle position, the driving speed, the driving direction and the vehicle condition. The so-called certificate ID, which identifies the vehicle and

ultimately makes the holder identifiable.

With Section 63e of the Road Traffic Act (StVG), in the summer of 2021, the German legislator created an initial legal basis for the processing of the relevant data, which is exhaustively listed in the standard, by the responsible road construction authorities for the purpose of traffic management. The standard writes to you

Machine Translated by Google

anonymous evaluation of the data transmitted with the CAMs and subsequent immediate deletion.

As part of the test, the State Office for Roads, Bridges and Water (LSBG) responsible for data processing
opted for a consent solution. Only CAMs of a limited number of test users are processed, essentially
Companies that have previously consented to the evaluation. Technically, the restriction to the test users is ensured by signing the CAMs of the test vehicles with keys that were generated using the manufacturer certificate requested by the FHH for the Hamburg Public Key Infrastructure. The LSBG cannot assign the CAMs to specific drivers of the test vehicles.

6.6.5 Traffic volume recording The
implementation of the automated traffic volume recording has already been accompanied by the HmbBfDI in the past (cf. 28.
TB, Chapter V 2.2). At that time, the data-saving approach using thermal imaging cameras was praised and classified as harmless. Many further developments in the field of technology make expansion possible
the existing infrastructure. The Authority for Transport and Mo
bilitätswende (BVM) commissioned Hamburg Verkehrsanlagen
GmbH (HHVA) with the construction of a nationwide automatis
ated traffic volume recording and additional travel time determination.

For this purpose, the manufacturer was selected, whose thermal imaging cameras are already installed for traffic volume recording at the major junctions in the area of the traffic lights. newer
Camera models from this manufacturer come with a Wifi module
allowed, which can receive the Wifi signals of the smartphones carried by road users. This approach takes advantage of the fact that Wifi-enabled devices search for Wifi access points that are known to them. For this purpose, "Wifi Probe Requests" signals are sent at regular intervals

Machine Translated by Google

contain a MAC address assigned to the device. The MAC addresses received by the traffic signal systems are to be saved so that the travel time for the
Test area can be determined.

The HmbBfDI is also accompanying this project and is in lively exchange with those responsible for the following problems: It has not yet been decided on which legal basis those responsible can rely and whether Section 63e of the Road Traffic Act (StVG) can be applied. The information requirements according to Art. 13 GDPR would have to be satisfied. A website is currently being planned on hamburg.de, although it is unclear how those affected should be referred to this website.

Current smartphones are constantly changing the MAC addresses used for the signals described in order to make reliable recognition more difficult. It is unclear whether the camera manufacturer can achieve meaningful results over a longer period of time with the desired method and whether it is therefore a suitable means of fulfilling the purpose at all. Furthermore, from the point of view of the HmbBfDI, an unnecessarily long storage of the MAC addresses is planned. Processing in a cloud infrastructure from an American provider also appears to be problematic. With this solution, the Schrems II problem (cf. TB 29, Chapter IV 5) is in the room, so that an evaluation of the MAC addresses

cannot be prevented by American third parties.

Machine Translated by Google

Machine Translated by Google

Machine Translated by Google

Machine Translated by Google

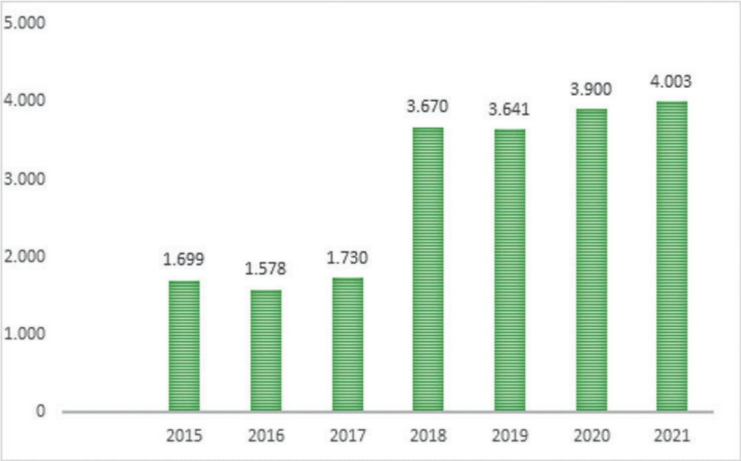
7. Information on government activities

1. Statistical Information (Facts and Figures)

Every year, at this point in the activity report of the HmbBfDI, it is reported that the incoming numbers in the reporting period are higher than ever. This was the case again in 2021,

in which the HmbBfDI received 4,003 written entries. In addition to the 320 receipts under freedom of information law and the 12 requests for information to the HmbBfDI (Art. 15 GDPR), there are 3,671 written receipts that were addressed to the HmbBfDI as the data protection supervisory authority. This is a new record.

Written receipts at the HmbBfDI 2015 - 2021 (total)

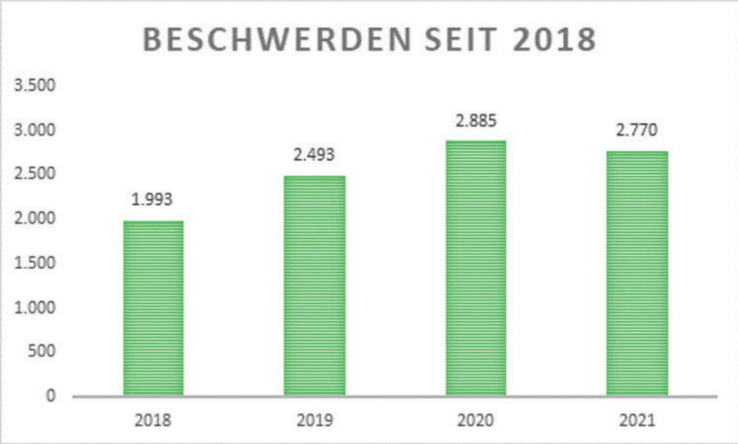


1.1 Complaints and advice

that the processing of the personal data concerning you violated the provisions of the GDPR (Art.

77 GDPR). In 2021, the HmbBfDI received 2,770 such complaints reached, that is around 69% of the total number of written receipts. That is significantly fewer data protection complaints than in the previous year (2,885 or 76%), but the second highest value since In entry into force of the GDPR:

Machine Translated by Google



Those affected, companies and authorities also turn to the HmbBfDI for advice on data protection issues. These inquiries reached the HmbBfDI again in 2021 both in writing and by telephone:

Consultations 2021

	Affected	companies	Authorities	total
in written form	331	171	35	537
by phone	461	125	56	642
total	792	296	91	1.179

The number of written consultations is slightly higher than in the previous year (537 to 486 - 29th TB, Chapter VII 1.1) and the number of telephone consultations has remained approximately the same (642 to 634 - 29th TB, Chapter VII 1.1), so that there was a moderate increase of around 50 cases overall. It cannot be said whether these figures confirm or deny the trend that was announced as an object of observation last year. This requires the evaluation of the figures for the coming years.

Machine Translated by Google

1.2 Opinions in legislative procedures Due to the 'guideline for the participation of the HmbBfDI', the HmbBfDI is involved in the coordination of printed matter before it goes to the Senate and the Hamburg Parliament. In 2021, this involvement took place in 75 cases, 44 of which related to legislative and legislative projects (including the conclusion of state treaties).

1.3 Remedial Actions

Also in this reporting period, the HmbBfDI has again of its made use of various remedial powers (Article 58 (2) GDPR). Specifically, the following measures were taken in 2021:

measure	legal basis	Number 2021
warnings	Art. 58 Abs. 2 lit. a	1
warnings	Art. 58 Abs. 2 lit. b	7
instructions and arrangements	Article 58 paragraph 2 letters c – g and j	3
fines	Art. 58 Abs. 2 lit. i	18
revocation of certifications	Art. 58 Abs. 2 lit. h	0

1.4 Obligation to report under Art. 33 GDPR

Hacker attacks, data leaks and other violations of the protection of personal data must be reported to the competent supervisory authority immediately (if possible within 72 hours of becoming known) if there is likely to be a risk to the rights and freedoms of the persons concerned.

In the reporting period, the HmbBfDI received 871 such reports, of which 88 were identified after examination as non-reportable incidents. Nevertheless, the number of reports increased significantly by almost 100 cases to 783 compared to the previous year (686 - 29. TB, Chapter VII 1.2).

Machine Translated by Google

With 269 individual reports, the most frequently reported violation of the protection of personal data is again incorrect mailing, i.e. sending e-mails and postal items to the wrong recipient; with 196 individual reports, however, hacker attacks are also at a very high level and, compared to 2020 (156 - 29. TB VII 1.2), have again increased significantly.

1.5 European procedures If
citizens of several European countries are affected by data processing, this fact is entered in the Internal Market Information System (IMI) of the European Commission. The supervisory authority in whose area of responsibility the controller has its European headquarters is then responsible for processing; all other supervisory authorities can contact the

Report procedure as affected.

In 2021, the HmbBfDI was involved in 21 European procedures:

European procedure	Number 2021
Proceedings with concern (concerned)	16
lead process	5
Further procedures acc. Chapter VII DSGVO (Art. 60 ff)	No statistical recording

Machine Translated by Google

2. Press and public relations work

In the 2021 reporting year, the HmbBfDI received around 300 press inquiries. The most important topics here were data protection issues relating to WhatsApp and Facebook, the concerted questionnaire campaign regarding the implementation of the Schrems II judgment and data protection issues in the context of the corona pandemic.

The reduced number of inquiries from the press and media compared to the “record year” 2020 can probably be attributed to the large media focus on topics such as the corona pandemic and the federal elections. The four-month interim phase associated with the change in management of the HmbBfDI may also have been a factor.

Nevertheless, some topics in which there was already great interest in 2020 continued to attract a large number of inquiries. In particular, the entire complex surrounding Whats App and Facebook should be mentioned here, i.e. the change in the WhatsApp terms of use, the question of data exchange between the two companies, the emergency procedure of the HmbBfDI against Facebook and the associated decision of the European Data Protection Board. The questionnaire campaign by the HmbBfDI and other German data protection supervisory authorities with regard to the implementation of the Schrems II judgment in companies as well as the HmbBfDI's audits of the two US providers Clubhouse and Clearview also generated great interest. As already in the

In recent years, the HmbBfDI has received numerous inquiries from foreign media about such cross-border topics.

As in the previous year, other important topics were data protection aspects in connection with the corona pandemic; here, for example, the discussion about the use of the Luca app, questions about data security in corona test centers and uploading vaccination cards to social media.

Machine Translated by Google

With regard to specific Hamburg issues, the fine of the
HmbBfDI against a company belonging to an energy supply group as well as a warning to
the Senate Chancellery of the City of Hamburg regarding the use of the Zoom video conference
platform
to emphasize Furthermore, the change of office at the HmbBfDI from
Johannes Caspar on Thomas Fuchs as a highly requested topic
to name.

On the occasion of the third anniversary of the GDPR, as in previous years, the HmbBfDI received several statistical inquiries about the number of complaints, data breaches and sanctions.

In the 2021 reporting period, the HmbBfDI received a total of 297 press inquiries, which is around 25% fewer than in the previous year 2020, which had an “all-time high” of 398 inquiries. On average, around 25 inquiries per month were processed in the 2021 reporting year.

With regard to the two large Internet companies Facebook and Google, it can be said that the inquiries in this regard - in particular due to the issue of WhatsApp - have increased significantly, from approx. 8% of the total number of inquiries in 2020 to approx. 24% in 2021. From Of the two groups, Facebook (21%) is far ahead of Google (3%).

With regard to the local origin of the inquiring media, it can be stated, as in the previous year, that by far the most inquiries come from national German media. Inquiries from foreign media have remained at the same level as in 2020, as shown in the table below:

Press inquiries...	2020	2021
regional media: national	107	83
media:	219	143
foreign media:	72	71
In total:	398	297

Table 1: Press inquiries to the HmbBfDI 2020 and 2021

Machine Translated by Google

In addition to this Activity Report Data Protection 2020, there were no other publications in the print area in the reporting year.
The Internet offer of the HmbBfDI is constantly being further developed; In the year under review, the issue of accessibility was also tackled more intensively. During the reporting period, the HmbBfDI published 11 press releases.

In addition, the Hamburg data protection officer and
several employees of the authority again
and presentations on aspects of the GDPR as well as on various topics of data protection and takes part in round tables 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 and campaigns (see Chapter VII 3 below for details).

3. Promotion of data protection competence by the HmbBfDI

Education and the promotion of media and data protection skills are among the most important tasks of modern democratic society: active and informed participation in society and democracy can only succeed through awareness-raising, education and targeted educational measures.

The ongoing corona crisis has shown once again that the internet is omnipresent these days. We are experiencing a digitization of society in which social networks, intelligent devices and artificial intelligence are becoming increasingly important to society. The dangers of identity theft, cyberbullying and the influence of social media on political and social opinion-forming have long since become reality.

Machine Translated by Google

Despite the ongoing Corona crisis, the HmbBfDI has also
last year 2021 seminars and workshops in schools and other educational institutions on topics such as “Fake News & Data Protection”, “Data Protection & Democracy” or “Data Protection at
messengers”. While these could still take place in person at the beginning of the year in compliance with the hygiene regulations at the time, most of the workshops and events then took place digitally.

It quickly turned out that the FHH for Ver
The provided video conferencing services "Skype for Business" and "Cisco Webex" do not work for this application scenario
external participants can only register with an additional
sign any effort to these video conferencing services. In addition
From a technical and didactic point of view, the two systems entail a workflow that is no longer up-to-date due to the lack of functions such as break-out sessions, direct visual feedback ("raise your hands", "thumbs up") and ad-hoc surveys met with low acceptance among external participants.

Therefore, the HmbBfDI commissioned BigBlueButton as a managed service. BigBlueButton is a data-saving and transparent video conferencing platform, since it was developed as an open source. The reasons for the purchase were in particular the easy-to-use interface, the features mentioned above, collaborative whiteboards and screen-sharing functionalities. The experiences of all parties involved with BBB are consistently positive

to rate.

In April, the HmbBfDI participated in the Germany-wide Girls' Day and Boys' Day. The goal of the nationwide day of action is stereotype-free professional orientation. For example, Girls' Day and Boys' Day are intended to offer girls and boys the opportunity to gain an insight into occupational fields that deviate from traditional occupational profiles. Under the title “Data protection is boring? Because of that!” he asked
HmbBfDI the professional fields of the lawyer
and that of computer scientists. Already after

Machine Translated by Google

After a short time, the 20 available places were fully booked, so that a total of 40 schoolchildren took part in the campaign
HmbBfDI participated.

Two months later, as part of Digital Day, the HmbBfDI and the Youth Information Center (JIZ) organized a series of events on the topic of disinformation in social media. The aim of the Digital Day is to promote digital participation, because everyone should be empowered to move safely, confidently, and self-determinedly in the digital world.

Thus, in addition to a seminar on the subject of fake news and data
Protection in a vocational school also held a digital discussion round on the topic “A question of power – the influence of social media on our democracy” with experts. The lively participation of the guests testified that this format and the issues discussed were very sociable

arouse scientific interest.

Furthermore, the HmbBfDI has played the role for the second time
involved in the expert advice on a production of the FWU Institute for Film and Image in Science and Education gGmbH. In the second educational film "Social Media: How can I protect my data?"
learn students - based on the goals of
“Education in the digital world” strategy of the Conference of Ministers of Education (KMK) – know popular social media platforms and who
sensitized to possible dangers during use. In addition, it is explained for the target group why data protection is also relevant in the everyday life of adolescents, and strategies for protecting one's own data are presented in the film.

The film and the accompanying teaching material are available to all Hamburg schoolchildren via the school media center in Hamburg.

The link to the film is also available in the FWU's own media library: https://www.fwu-mediathek.de/record?id=xfwu-5523058

Machine Translated by Google

In addition, the HmbBfDI 2021 played a key role in revising the joint youth portal of the independent Da
data protection supervisory authorities of the federal and state governments as well as of the Canton of Zurich, Youngdata.de. The aim of the relaunch is a complete technical and content revision. The Youngdata page is aimed at young people aged 13-16 with the aim of providing information on the subject of data protection and for the

raise awareness of the safe handling of personal data.
With that, the German data protection supervisory authorities are coming to their Educational mandate according to Article 57 Paragraph 1 b GDPR. On the basis of scientific findings, the operation of the site is adapted to the habits and needs of the target group. The content is also being redesigned to be more specific to the target group, both in terms of the selection of topics and how young people are addressed in texts and videos. The content will continue to be under a free license that allows for reuse. Teachers, educators and parents can also obtain information from the site and use it didactically.

Pronounced media competence is also indispensable for parents today. With their media use, parents have a role model function and are therefore the key to their children's media education.
Unfortunately, you often only have a few information resources at your disposal: Accessible and uncomplicated information material is rare, as are competent support and advice systems that parents can turn to with questions. For this reason, the data protection authorities of Hamburg and Mecklenburg-Western Pomerania have joined forces with the Hamburg citizens' broadcasting service and media competence center TIDE and have joined the DEAP (Data, Education, Awareness and Protection) project on EU funding

funds as part of the Citizens, Equality, Rights and Values program (CERV). The DEAP project wants data protection for
Make parents tangible and understandable. This is to be done in online semi Naren and (barrier-free) offline events to raise awareness of data protection education issues. In addition, multilingual publicly accessible education

Machine Translated by Google

material created and the construction of local multiplier structures get supported.

DEAP's special focus on promoting the digital skills of socio-economically disadvantaged parents is not only innovative, but also promising: A critical and informed approach to media strengthens social participation, professional success, democratic education and personality development.

Machine Translated by Google

4. Allocation of tasks (status: 01/01/2022)

The Hamburg representative
for data protection and freedom of information
Ludwig-Erhard-Str. 22 (7th floor), 20459 Hamburg

Phone: 040/42854-4040
Fax: 040/42854-4000

E-Mail: mailbox@datenschutz.hamburg.de Internet-
Address: www.datenschutz-hamburg.de

Head of department:	Thomas Fuchs
Deputy:	Ulrich Kuehn
antechamber:	Heidi Niemann
Representative for the budget, personnel and organizational management, Entrepreneurial duties, controlling	Arne Gerhard
Budget management, planning and management, reporting, Controlling, basic questions of fee law and procurement	Robert Flechsig
Press and public relations, IT management, Internet offer of the HmbBfDI	Martin Schemm
Education and training, administration, travel expenses, fees and fines, building matters and procurement	Rolf Nentwig
antechamber, office	Heidi Niemann
Registrar	Frau Vukšiÿ
Registry, information according to Art. 15 GDPR	Silk Saree

Machine Translated by Google

Promotion of data protection competence and media education, public relations	Alina Feustel
Registrar	Komal Tariq
Basic questions DSGVO, BDSG, HmbDSG and HmbTG, VIG, HmbUIG, representation of the HmbBfDI in court proceedings	Dr. Christoph Schnabel
Basic questions HmbVwVfG, VwGO, VwZG, labour, service and disciplinary law, sanction and remedial notices, case-by-case processing	Richard Heyer
Policy issues Sanctions and file management, individual case processing, Sanction and remedial notices	Cornelia Goecke
Questions of principle Art. 58 and Art. 32 f. GDPR, sanction and remedial notices, case-by-case processing	Steffen Sundermann
Department of Interior and Sport, Police, Office for the Protection of the Constitution, Authority for Justice and consumer protection, public prosecutor's office, courts, law enforcement	Anna-Lena Greve
Passport, identity card and registration system, civil status, archiving, Statistics, census, microcensus	Uta Cranold
Ministry of the Interior and Sport, Police, protection of the constitution, fire brigade, foreigners, cemeteries, gun law, port security law, Security clearance law	Dirk Pohl

Machine Translated by Google

Freedom of information (HmbTG, UIG, VIG), press law information claims	Swantje Wallbraun
Deputy Hamburg resident Data Protection Officer, Accreditation and Certification	Ulrich Kuehn
ePrivacy, press and broadcasting, telemedia and telecommunications, advertising and Direct Mail, Culture, Accreditation and Certification	Katja Weber
Tracking and cookies, cross-topic processing	Amina Merkel
education (schools and colleges), advertising and direct mail, research, geodata	Alexander Schierman
Development of testing tools, smart devices, Internet of Things, technical support in case and case processing	Roland Schilling
E-mail and game provider, eGovernment cloud service, apps, review portals	Felix Wagner
Questions of principle Chap. VII GDPR, coordination of European procedures as well as procedures of cooperation and coherence, Accreditation and Certification	Frau Jacobson
search engines (esp. Google, NorthData)	Dr. A.S. Let's Come Together

Machine Translated by Google

Social networks (esp. Facebook, XING, Twitter), Datingportale	Simone Hoffmann
Accreditation and certification, technical support in case and processing	Mr. Schneider
Technical fundamental questions in eGovernment, technical-organizational counseling and testing	Dr. Sebastian Wirth
Basic technical questions in biometrics, artificial intelligence, video surveillance, Design and operation of the testing laboratory, technical and organizational advice and testing	Eike Kleinfeld
Technical and organizational counseling and testing	Jutta Nadler
Basic technical questions networks and mobile devices, Design and operation of the testing laboratory, technical and organizational advice and testing	Mr. Maka
Basic questions economy, international data traffic, parliaments, parties, Parliamentary groups and elections, chambers	Dr. Jens Ambrock
Employee data protection	Oksan Karakus
banking, construction and housing, environment, agriculture	Viola Büchl

Machine Translated by Google

Commercial Services, Industry, insurance industry, lawyers, Security services, notaries, employees privacy	Pieter Jaurnig
finance and taxation, tax advisor, auditors, clubs, sports, foundations	Heike Wolters
health and social affairs	Behrang Raji
Stationary trade, video surveillance non-public bodies	Bianka Albers-Rosemann
Mail order, debt collection, credit bureaus	Eggert Thode
Utilities (electricity, gas, waste), transport, Smart City, gastronomy, market and polling, churches	Sabine Siekmann
cross-thematic processing	Sebastian Reich

Machine Translated by Google

Machine Translated by Google

INDEX

Machine Translated by Google

Machine Translated by Google

In

Y

FROM

Machine Translated by Google

Machine Translated by Google

Circulation: 750 copies
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Photo front page: Martin Schemm, edited by Thomas Krenz Print:
oeding print GmbH

Machine Translated by Google

Publisher:
The Hamburg Commissioner for Data Protection and Freedom of Information
Ludwig-Erhard-Strasse 22 20459 Hamburg Tel.: 040/42854-4040

Email: mailbox@datenschutz.hamburg.de

The Hamburg representative for
Privacy and Freedom of Information

Hamburg