privacy and

Freedom of Information

Annual Report 2022

annual report

the Berlin Commissioner for Data Protection and

Freedom of Information as of December 31, 2022

The Berlin Commissioner for Data Protection and Freedom of Information has, according to § 12 Berliner

Data Protection Act and § 18 Para. 4 Berlin Freedom of Information Act to the

ordnetenhaus and the Berlin Senate report annually on the results of their

submit activity. This report follows on from the 2021 annual report

and covers the period between January 1st and December 31st, 2022.

The annual report is also available on our website:

www.datenschutz-berlin.de

imprint

Editor:

Berlin Commissioner for Data Protection

and freedom of information

Alt-Moabit 59-61

10555 Berlin

Phone: 030 138 89 0

Fax: 030 215 50 50

mailbox@datenschutz-berlin.de

www.datenschutz-berlin.de

Envelope:

april agency GbR

Sentence:

Print:

work & set.

Spree Druck Berlin GmbH

Contents

List of abbreviations

Abghs.-Drs.

ADHGB

TFEU

Inc

AGG

AktG

ArbGG

ASOG Bln

AsylG

Residence G

GCU

BAMF

BDSG

BerlHG

BerlSenG

BfDI

BfJ

Civil Code

Federal Law Gazette

BGH

BKA

BlnDSG

BLUSD

BMG

BMI

BVerfG

BVerwG

BVG

House of Representatives printed matter

General German Commercial Code

Treaty on the Functioning of the European Union

District Court

general equality law

Stock Corporation Act

Labor Court Act

General Law for the Protection of Public Security

and order in Berlin

asylum law

Residence Act

General Administrative Regulation

Federal Office for Migration and Refugees

Federal Data Protection Act

Berlin Higher Education Act

Berlin Seniors Participation Act

Federal Commissioner for Data Protection and the

Freedom of Information

Federal Office of Justice

Civil Code

Federal Law Gazette

Federal Court of Justice

Federal Criminal Police Office

Berlin Data Protection Act

Berlin teacher teaching school database

Federal Registration Act

Federal Ministry of the Interior and Homeland

Federal Constitutional Court

Federal Administrative Court

Berlin transport company

8th

List of abbreviations

Federal Central Register Act

Federal Central Tax Office

Digital audio broadcasting

Digitization and Data Protection Committee

Digital education meets school

Irish Data Protection Authority

German judges law

General Data Protection Regulation

Conference of the independent data protection supervisory

federal and state authorities

European Data Protection Board

recital

E-government law Berlin

Investigative Note

European Union

European Court of Justice

European Economic Area

Federal IT cooperation

Law to adapt the form requirements in Berlin

state law

constitution

Limited liability company

Global Privacy Assembly

Law and Ordinance Gazette

commercial code

Commercial Register Ordinance

Humboldt University of Berlin

Berlin Freedom of Information Act

Freedom of Information Commissioners Conference

Germany

Information and communication technology

9

BZRG

BZSt

DAB

DiDat

DigiBitS

DPC

DRiG

GDPR

DSK

EDSA

ground floor

EGovG Bln

EHW

EU

ECJ

EEA

FITKO

ShapeCustomG

GG

GmbH

GPA

GVBl.

HGB

HRV

HU

IFG

IFK

ICT

List of abbreviations

IMI

IP

IT

ITDZ

JB

JI Policy

JuHiS

KG

CUL

LABO

LOCATIONSo

LDA

LEA

LG

LKA

LKG

LMÜTranspG

LMÜTranspG-DVO

LUSD

LVwA

MDM

MiStrA

MStV

public transport

OLMERA

OVG

Internal Market Information System

internet protocol

information technology

IT service center Berlin

annual report

Directive (EU) 2016/680 of the European Parliament

and the council

Juvenile Aid in Criminal Proceedings

Court of Appeal

Children's University Lichtenberg

State Agency for Civil and Regulatory Affairs

State Office for Health and Social Affairs

State representative for data protection and law

on file inspection Brandenburg

State Office for Immigration

district Court

State Criminal Police Office

State Hospital Act

Food Control Transparency Act

Food Control Transparency Act-

executive order

Teachers-Teaching-School Database

State Administration Office

Mobile device management

Order on Communications in Criminal Matters

Media State Treaty

Transportation

Online registration information

Higher Administrative Court

10

OWASP

OZG

PDV

POLICIES

RBB

RegVBG

SCC

SchoolG

SGB

StGB

StPO

SUrlV

SWIFT

TTDSG

UIG

FM

UrhG

VG

vig

vs

AWAY

WPD

ZensG

CensusAGBln

ZensVorbG

ZPO

condition cat

List of abbreviations

Open Web Application Security Project

Online Access Act

police service regulation

Police state system for information,

communication and processing

Radio Berlin-Brandenburg

Register Procedure Acceleration Act

Standard Contractual Clauses

School law for the state of Berlin

social code

criminal code

Code of Criminal Procedure

Special Leave Ordinance

Society for Worldwide Interbank Financial

telecommunication

Telecommunication Telemedia Data Protection Act

Environmental Information Act

ultra shortwave

copyright law

administrative court

Consumer Information Act

classified information

Law on home ownership and the

permanent residence

Scientific Parliamentary Service

census law

Census Implementation Act Berlin

Census Preparation Act

Code of Civil Procedure

List of responsibilities for regulatory tasks

11

12

foreword

On October 6 of this year, I was elected by the House of Representatives for a period of five

Years ago elected Berlin Commissioner for Data Protection and Freedom of Information. I

I'm really looking forward to the new task and I'm grateful to be able to walk this path with high-quality

fied experts at my side. Your tireless and

Committed commitment to data protection and freedom of information forms the basic

situation for this annual report.

We are still waiting for a modern transparency law to be passed

for Berlin. Does the administration proactively provide the information that

are the basis for administrative action and political decisions, enable

it facilitates the timely discussion and comprehensibility of the decisions

gen. Ultimately, the administration itself also benefits from the publication by

Information required by other authorities via a transparency portal on the

receive short official channels. Such a portal requires that administrative information

are available electronically and without media discontinuity from digitized processes

can be provided. Against this background, it is also important that

Digitization of the Berlin administration continues to pick up speed. With the simultaneous

Further development of the online access law will hopefully more and more administrators

services made available digitally. At the same time, the missing data

protective legal bases and the responsibilities clear and unambiguous

be mapped. It must always remain transparent what exactly is involved in the claim

acceptance of digital administrative services with personal data happened and

who is responsible for what. Because people's trust is crucial

for the acceptance of the procedure.

When checking data processing by the police and the public prosecutor's office

we look for legal obstacles, since the Berlin state law is still working on the implementation

tion of the effective enforcement instruments provided for by European law for our

authority is missing. The pressure from Brussels is growing, since the EU Commission has the missing

taken the powers as an opportunity to file a breach of contract

initiate proceedings.

Our job is to protect fundamental rights and to inform people about it.

to benefit from digitization and the use of technology without relying on self-

mood, anonymity, free access to information and opinion-forming, as well as other

time unobserved freedom of development. For the growing up

Generations and thus for the education and school sector, this is of particular importance

Significance: We must enable children and young people to take advantage of this freedom

to obtain in the future. At the same time, they should use digital learning aids and

can learn unobserved in digital lessons. It is precisely these standards that apply to

the procurement of digital devices and the further development of the legal basis in

school area and the Berlin school portal.

The requirements also help in the area of business and the Internet economy

of data protection, freedom of decision, possibilities of intervention and

to preserve communication diversity. With the digital package and the data strategy of

European Union and the planned regulation of political targeting

new legal developments are imminent that will influence our work. The

The work of our authority will continue to be based on the rule of law assigned to it in the future

be geared towards preserving and protecting fundamental rights. I am happy

to the developments in this highly dynamic field of activity.

I wish you informative reading

Meike Kamp

Berlin Commissioner for Data Protection and Freedom of Information

1 Digital Management

1.1 Status of digitization projects - The problem lies in the detail

In the field of administrative digitization, Berlin still has considerable need to fetch. In some areas, the Senate has begun to develop central building blocks to implement digital management. The concrete implementation is with many technical challenges and raises numerous privacy issues with which we have worked intensively this year.

In the meantime, authorities can also provide important administrative services at very short notice make it available via a digital application. It also starts for parts the approx. 120,000 administrative employees said goodbye to the paper file. The The Mitte district office is currently running the basic ICT service as part of a pilot project, for example "Digital file" a.1 In the course of our consultations on the introduction of the digital file 2 we have the ICT control at the Senate Department for the Interior, Digitization and Sport, which provides the basic ICT service "digital file", supports to develop a framework data protection concept. This is now used by the specialist authorities Basis for a data protection-compliant introduction of the digital file.

In this context, we also asked the social welfare office in Mitte to draw up the data protection concept and the data protection impact assessment. The ones there The resulting documents should now also be in the social welfare offices of the other districts find use. According to the same model, we will add other specialist offices and service provide support to district offices in preparing data protection documentation to create a digital file that can then be "reused" by other authorities

1

2

The Senate Department for the Interior, Digitization and Sport provides the administration with the most important internal and external components for the provision of the E-government offerings as so-called basic ICT services (basic information and communication technology) (see Section 10, Paragraph 2, Clause 3 of the Berlin E-Government Act (EGovG Bln) and § 24 para. 2 sentence 1 EGovG Bln), e.g. B. in the form of the "Digital File" and the "Digital Application".

See JB 2021, 2.1.

can. Overall, a considerable reduction in the effort for the individual be reached by specialist authorities that introduce the digital file. This should be a role model for the future introduction of further basic ICT services.

In March, the Senate announced that it was a particular success of the digitization of administration the start of the digital procedure for applying for a residence permit for Ukrainian cal refugees are registered with the State Office for Immigration (LEA). This method is based on the basic ICT service "digital application".3 The administration is therefore responsible effective tool for the short-term management of large volumes of applications for decree. However, fundamental data protection issues still need to be clarified here.

This corresponded to the data protection information provided to the user when were made available digitally, do not meet the requirements of the General Data Protection regulation (DSGVO): The data protection declaration did not indicate which authority how the personal data of the data subjects are processed. It was across the board on a joint responsibility 4 between the ICT control, the provides the service and referred to the LEA, although the ICT control the personal data of the applicant refugees in the absence of legal basis should not process at all. Against this background, we support

The bodies involved are now preparing the information and documentation for the digital

adjust the request accordingly.

It is important that when using digital administrative services for those affected

always remains transparent which of the numerous public and

private bodies process their personal data on what basis

and who selects the right contact person for the fulfillment of their rights as a data subject

of the GDPR.5 Only with clear responsibility structures and the greatest possible

Transparency with regard to the handling of personal data

Administration can win the trust of citizens in digitization.

3

4

5

See 2020 Annual Report, 2.1.

I.S.v. Art. 26 GDPR.

See e.g. B. Art. 15 GDPR (right to information) and Art. 17 GDPR (right to erasure).

1.2 Implementation of the Online Access Act in the federal government and countries - when will the knot burst?

With the necessary adjustment of the Online Access Act (OZG), the necessary

relevant data protection legal bases are created, which in the previous

Gen version of the OZG from 2017 is missing.

It has been foreseeable for a long time that the federal and state governments will

laid schedule, the main 575 administrative services by the end of this year

to make them digitally available to citizens via administrative portals,6 not

can hold. Against this background, the lead Federal Ministry of the

Inside and for home (BMI) as part of the "OZG 2.0" presented in February

project to adapt the OZG in order to set the course for a short-term acceleration

to face the OZG implementation.

Already in autumn 2020, the conference of the independent data protection supervisory

federal and state authorities (DSK) set up a sub-working group

dealing with data protection issues in connection with the OZG

implementation and an ongoing consultation and coordination process

zess with the Federal Ministry of the Interior and the Federal IT Cooperation (FITKO).7 With a view to that

The DSK has the sub-working group for current legislative procedures on the OZG

Converted to the "OZG 2.0" contact group at the end of 2021. We have the presidency

and coordinate the consultations with the Federal Ministry of the Interior. We are pleased that the

responsible specialist department of the BMI also because of our intensive consultation

view of data protection has taken up the most important regulatory projects. the other

Delay in the legislative process poses a significant problem: None

Corresponding adjustments can be made in compliance with data protection regulations of the OZG

not guaranteed in view of the lack of a legal basis for data processing

become. Against this background, the procedure must now be brought to an immediate conclusion

to be brought.

6

7

See 2020 Annual Report, 2.2; JB 2021, 2.3.

See AGM 2021, 2.3.

With the adjustment of the OZG, the administrative digitalization in Germany

finally the knot burst. As a prerequisite for this, without further delay

ments also implemented the regulations on data protection that were still missing

become.

2 Home and Sports

2.1 Growing pressure from Brussels - No effective ones

Enforcement powers with police and

Public prosecutor

In the past, our authorities in Berlin and Brussels have repeatedly

pointed out that important European requirements in the field of control of

Authorities responsible for the prevention and prosecution of criminal offenses and for the enforcement of

responsible for extension have not been implemented in Berlin state law. Well

we receive support on this issue from the European Commission, which is a

formal infringement proceedings against Germany.

The European Commission can start an infringement procedure if a

Member State of the European Union (EU) an alleged violation of EU law

not fixes. The issue at hand is the inadequate implementation of the so-called JI Guideline 8,

the processing of personal data by authorities for the prevention and

the prosecution of criminal offenses and the enforcement of sentences uniformly throughout the Union.

Authorities are when they need data to prevent, investigate, detect or prosecute

criminal offenses or for the execution of sentences, from the scope of the

directly applicable General Data Protection Regulation (GDPR) excluded.9

For the police, public prosecutors, criminal courts and the penal system, the

provisions of the JI Directive apply, which - unlike the directly applicable GDPR -

must be transposed into national law. On the one hand, this should be given to the Member States

grant greater freedom in individual questions, but on the other hand harbors the risk that

EU law is implemented inconsistently and less effectively. So also in Berlin: The

The powers of our authority are limited by the relevant state law

8th

9

Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016

to protect natural persons in the processing of personal data by the

competent authorities for the purpose of prevention, investigation, detection or prosecution

criminal offenses or the execution of sentences, as well as the free movement of data and repeal

of Council Framework Decision 2008/977/JHA.

Art. 2 Para. 2 lit. d GDPR.

19

permission to be informed about objected processing operations by authorities responsible for the

Responsible for the prevention and prosecution of criminal offenses and the execution of sentences

are, after a mandatory attempt at agreement, to the responsible committee of the

to report to the House of Representatives.10 This is what the supervisory work of our authority always threatens

to be negotiated purely politically, without being enforceable and justiciable.

The JI directive from 2016, the specifications of which will be fully implemented in national

national law should have been implemented, provides, for example, that the supervisory

authority instruct a responsible body or a processor directly

must be able to, processing operations with the relevant regulations in accordance

to bring sound. This can be done in particular by ordering the correction or

Deletion of personal data or restriction of data processing

11 According to the JHA Directive, it is important that remedial powers are effective. The

Remedial powers must be able to be directed against the responsible body

and must not be subject to further conditions, such as the material

of an infringement or of a previous complaint.

To date, these European requirements have only partially been implemented at federal and state level.

implemented wisely. The European Commission has therefore now issued a formal

Infringement proceedings initiated, which are referred to the Federal Republic of Germany as

Member State of the EU is addressed, but also the failures of the Berlin State

legislator and clearly identifies them as insufficient. The

The Commission emphasizes that the often quoted expectation that authorities would

Dubious behavior in accordance with the law, not an effective measure within the meaning of the JI Directive

represents. If the guidelines are not implemented, the commission will end up

must decide whether to take these failures to the European Court of Justice

(ECJ) brings.12

The need for effective authority to issue orders, also in the area of

prevention of criminal offenses as well as criminal prosecution and enforcement we have in

Consultations and statements to the House of Representatives again and again

reminded. It is precisely in these areas that encroachments on fundamental rights are opposed

10

11

12

See § 13 Para. 2, 3 Berlin Data Protection Act (BlnDSG).

Art. 47 (2) JI Directive.

See Art. 258 Treaty on the Functioning of the European Union (TFEU).

affected persons in general are often particularly sensitive or particularly

numerous. Federal and state legislators would be well advised to

not to risk a conflict with Brussels on this important issue.

The more closely the implementation of the JI Directive is examined from there,

the narrower the room for maneuver in the implementation.

2.2 What lasts for a long time still lasts - Overtime

Processing times for self-disclosures

the police

Again and again we receive complaints from citizens that the information

with the police take too long. Also because the state legislature opposes it

has decided to set a mandatory deadline for self-disclosures in this area

write, the enforcement of important rights of citizens is impaired.

Data processing by the police is largely not subject to the regulations

ten of the GDPR,13 so that there is also the usual one-month period for information about the

Processing of personal data of data subjects from Art. 15 Para. 3 GDPR

does not apply. Although the relevant JI Directive provides instead that

the right to information should be able to be asserted "without any problems".14 This would have

can be secured, for example, by a binding deadline for the provision of information

but the legislature unfortunately has to implement the directive in state law

no deadline foreseen.15

A speedy processing time is essential for the effective enforcement of data subject rights

essential: only with the knowledge of which data is processed in detail

Citizens can decide whether to defend themselves against such measures

want to set. Especially where personal data is processed without the knowledge of the person concerned

fenen or processed against their will, the individual must

effective control is possible. The rectification of the processed data is also possible

only demand those who know the inaccuracy at all. The experience of the complaint

13

14

15

See Art. 2 Para. 2 lit. d GDPR.

Recital (EG) 43 sentence 1 JI Directive.

See §§ 43, 45 BlnDSG.

practice shows that timely responses to those affected contribute to transparency
Establishing trust and taking care of it. Already in spring
In 2019, we raised this issue with the Chief of Police.16 After
about a quarter of the police responded to this question again
of data access and deletion requests still have processing backlogs of seven to
eight months, the rest would be decided earlier. We hope through here already
new appointments that have been made and announced will continue to improve.
The right to information about the storage of personal data and to
Deletion of this data is an essential right of data subjects. As an important stock
part of self-data protection, they represent a core component of the informational
right to self-determination. Effective implementation must be guaranteed, in particular
special must not overly long processing times the nature of the applications
as control instruments. In this respect, we strongly recommend using the
Introduction of a legal deadline for the provision of information a synchronism with the
establish the requirements of the GDPR.

2.3 Data Storage Relating to Children and Adolescents in the environment of organized crime

No criminal investigations may be conducted against children under the age of criminal responsibility
be led. Nevertheless, it may be necessary under certain conditions
be that on the part of the police, corresponding data on criminally relevant incidents
cases are processed for the purpose of averting danger.

From the ranks of the Chamber of Deputies we were on a parliamentary

Inquiry about police measures in relation to "combined operations, clan criminal

tät' and trade surveillance" 17 drew attention to this, in particular with regard to

the storage of personal data of suspects. From the answer of

Senate Department for the Interior, Digitization and Sport shows that the police in

their file system POLIKS a total of 19 minors with the investigative

16

17

See AGM 2019, 3.3.

Written question of February 25, 2022, Abghs.-Drs. 19/11121.

supporting note (EHW) "Clan crime". Of these were

at the time of reporting, four of those affected were not yet 14 years old and therefore not criminally responsible.18

Investigation-supporting information should help to ensure that police action is

to control them in a targeted manner, and thus serve the statutory task fulfillment as well as ideal

larly to protect those affected and the police officers deployed. Loud

The answer of the Senate administration from March 2022 was "clan crime" in the EHW

POLIKS assigned to 425 people;19 in the summer of 2020 there were still 154 people.20

The number of victims who were in POLIKS under the

EHW "Clan Crime Environment" were saved: In the summer of 2020

this only 14 people,21 in March 2022 already 87 people.22

The Federal Criminal Police Office (BKA) understands "clan crime" according to the Federal

bild 2020 “the commission of crimes by relatives of ethnically isolated

subcultures. It is shaped by family relationships, a shared

men ethnic origin and a high degree of compartmentalization of the perpetrators, thereby increasing the

committing the crime is promoted or the investigation of the crime is made more difficult. This comes with

own system of values and the principled rejection of the German legal system

ordnung." 23 However, the term is controversial in the criminal policy debate, since

there is a risk that certain population groups or family groups

clichéd criminal behavior is attributed. Accordingly, its

use has been criticized.24 The BKA has apparently reacted to this criticism and summarizes the

Criteria in his current report factual.25

18

19

20

21

22

23

24

25

See Section 19 of the Criminal Code (StGB).

See Abghs.-Drs. 19/11121.

See Abghs.-Drs. 18/23777.

See Abghs.-Drs. 18/23777.

See Abghs.-Drs. 19/11121. The legal basis for such notices are §§ 18, 28, 42 et seq.

General Security and Order Act (ASOG Bln) i. V. m. installation orders,

which must be drawn up separately for each note. The review and erasure periods

result from §§ 43, 48 ASOG Bln and from the regulation on inspection periods

police data storage (test period regulation).

BKA: Organized Crime, Federal Situation Report 2020, Wiesbaden 2021, p. 24.

See Thomas Feltes and Felix Rauls: "'Clan crime' and the 'German Angst'", in: Sozial

Extra (2020), vol. 44, p. 372 ff.

See BKA: Organized Crime, Federal Situation Report 2021, Wiesbaden 2022, p. 23.

We have checked a meaningful sample of the entries in POLIKS. Included
the police explained that there were usually facts about the entries in
to which those affected repeatedly and jointly with family members u. a.
had come to the attention of the police in connection with crimes of brutality. The
Reasons for storage resulted directly from the stored data sets
and although they were not pedagogically balanced in parts, they were nevertheless reproduced in a neutral way.
give. The justification for the corresponding categorization appeared under consideration
of the basic criminological assumptions of the police, the classification
was based neither exclusively nor predominantly on ethnic characteristics. The entry
conditions could be summarized under the defined characteristics, the justification for the
The inclusion in the database usually appeared detailed and task-oriented.
The question of the extent to which, with regard to organized crime, the reference to
specific features for successful investigative work and averting danger
imperative, should engage in exchanges with science and police
civil society again and again. We were able to identify indications of violations
not found in the checked datasets.

2.4 Digital Mind Reading - Smartphone Forensics

by the immigration authorities

As early as 2019, we started evaluating data carriers for identity
as well as determining the nationality of foreigners who are required to leave the country
the immigration authorities 26 concerned. At that time, the immigration authorities - unlike
the Federal Office for Migration and Refugees (BAMF) - no special software for

evaluation on. At the time, we were unable to breach data protection law

determined. Due to new findings, we have the exam again this year

of the measures taken by the immigration authorities.

26

According to No. 36 list of responsibilities for regulatory tasks (ZustKat Ord), this is now the case

State Office for Immigration (LEA), unless the district offices according to No. 22a Para. 2

ZustKat Ord are responsible.

24

Chapter 2 Interior and Sport

For the evaluation of data carriers 27 from foreigners there is a federal

statutory regulation,28 that by the law on the redefinition of the right to stay

and the termination of residence was introduced.29 This regulation empowers the

competent authorities,30 data carriers of those affected or obliged to cooperate

to evaluate dead foreigners in order to determine their identity and nationality

and, if applicable, a return option to another country

make. The evaluation of data carriers is subject to the legal admissibility

requirements that this is for the determination of identity and nationality

of the foreigner and for the determination and assertion

possibility of being returned to another country and the purpose

of the measure cannot be achieved by milder means.31 Furthermore, a

Such an evaluation can only be carried out by employees who have the

d. H. have two legal exams,32.33 An evaluation of

Data carriers is also always inadmissible if there are actual indications for the

Assumption exists that this alone provides knowledge from the core area of private

way of life would be obtained.34

Based on our audit from 2019, we have so far assumed that the

State authorities check the mobile phones of foreigners manually

Qualified employees are evaluated according to the legal requirements

the. From media reports this year we learned that the responsible

State Office for Immigration (LEA) since 2020 instead of the previous manual

Method uses software for data carrier evaluation, with the licenses

as well as devices for this have been purchased by the police on behalf of the state office

be. This was confirmed in our new test. The LEA stated that

to use the hardware and software, a service agreement with the police or

the State Criminal Police Office (LKA) had been concluded. In practice, the

state authority if the legal requirements are met 35 the mobile device of

27

28

29

30

31

32

33

34

35

Mainly it is likely to be mobile phones, especially smartphones.

Section 48 (3a) of the Residence Act (AufenthG).

See law of July 27, 2015, Federal Law Gazette I, p. 1386 et seq.

See § 71 AufenthG.

Section 48 (3a) sentence 1 of the Residence Act.

See § 5 Para. 1 German Judges Act (DRiG).

Section 48 (3a) sentence 4 of the Residence Act.

Section 48 (3a) sentence 2 of the Residence Act.

See § 48 Para. 3a AufenthG.

affected person and sends this to the LKA. The LKA then leads the
Data backup and data processing on behalf of the LEA using the appropriate
the software on a computer located there. The ones from the mobile devices
The data records obtained are then stored on removable storage media
(CD, USB stick or similar) sent to the LEA and by its employees with a
second computer and the associated analysis software.

As part of our audit, we initially received no answers to our questions
the specific software products used. This was justified by the fact that this
technical scope of services of the LKA and thereby
the decisive disadvantages would arise in the future investigation of criminal offences.
Against the background of our legal confidentiality obligations, the fundamental
comprehensive duties to cooperate in the clarification of data protection checks
and the fact that we are not only the competent supervisory authority for foreigners
authority, but also the police, such a refusal at the information
grant not justified.

We have also pointed out to the LEA that due to the nature of the
software and the great depth of intervention of the measures based on it
high risk for the rights and freedoms of those affected. considered
looking at the practical use of smart phones, it is obvious that these devices
are now more than just a means of communication. For many people they represent
a central interface between public and private thoughts and opinions
not only can, for example, based on the exchanged with other people

News draw conclusions about sexual orientation or political views

hen; via functions such as appointment management, health

security data on the device. According to the GDPR, such data that the special

Categories of personal data are attributed, specially protected and

may only be processed under certain conditions.36 The Federal

Federal Administrative Court (BVerwG) has also with regard to the in asylum procedures at the

36

Art. 9 GDPR; according to Art. 35 Para. 3 lit. b GDPR is a data protection impact assessment

etc. required when extensive processing of special categories of

personal data in accordance with Art. 9 Para. 1 GDPR; see also

https://www.datenschutz-berlin.de/datenschutz/datenschutz-kundenabschaetzung.

regular evaluation of digital data carriers 37 decided that

these in the absence of passports or passport replacement papers without sufficient consideration

inspection of other existing findings and documents is not lawful.38

Against the background of this fundamental decision, our examination of the

Measures by the LEA for the evaluation of data carriers are currently still pending. Furthermore

in particular questions about responsibility and the technical and organizational

to clarify satirical measures.

Our data protection review will be continued to clarify the remaining questions,

even if the LEA informed us that reading out using the special software

promptly discontinued and the service agreement with the LKA rescinded

should, since the high effort involved in viewing the data obtained is not

relationship to the success of the measures.

2.5 Don't forget the alien file

When inspecting the documents assigned to him at the immigration office, a citizen provided 39
the files kept state that there were still various documents that were too long ago
included in the criminal proceedings. Among them were sometimes more than
20 year old court orders. One document even referred to a misdemeanor
his youth. Since these procedures have already been deleted from the federal central register
were, the person concerned had doubts as to the legality of these long
preservation and turned to us.
In the course of our examination, we found that the immigration authorities
ten of the relevant criminal judgments at the time due to legal obligations to cooperate
received from law enforcement agencies. Even according to the provisions in force today
Public bodies must inform the competent foreigners authority immediately
inform when related to the performance of their duties by a

37

38

39

See Section 15a Paragraph 1 Clause 1 of the Asylum Act (AsylG), which has almost the same wording as Section 48 Paragraph 3a Clause 1
AufenthG is.

BVerwG, judgment of February 16, 2023, 1 C 19.21.

According to No. 36 ZustKat Ord, the tasks of the foreigners authority are with the LEA, if not
the district offices are responsible according to No. 22a Para. 2 ZustKat Ord.

reason for expulsion.40 Those for the initiation and implementation
The authorities responsible for criminal proceedings are also obliged to
authorities immediately about the initiation and completion of criminal proceedings

inform.41

However, the documents kept in the foreigners file are subject to legal regulations

Destruction or Deletion Obligations. There is an obligation to immediately

deleting documents or data that have (lawfully) entered the foreigners file,

if they are irrelevant to an upcoming decision under immigration law and

presumably also not relevant for a later decision under immigration law

42 This expressly also applies to documents that are submitted without a request

were sent to the immigration authorities. In addition, the person concerned may

son in cases in which the entry of a conviction in the Federal Central Register

has been erased or is to be erased, the offense and conviction no longer exist in legal transactions

held against them and no longer used to their detriment.43 For criminal law

Convictions that are subject to this ban on material exploitation can

Relevance for a later decision under immigration law is therefore regular

be excluded. This is a comprehensive ban imposed by

must be observed by all government agencies from the date of repayment or maturity – independently

of how they obtained the relevant information.44

As part of our hearing procedure, the responsible for the leadership of the Foreigners

file now responsible LEA that the relevant documents are still in

of the file. To what extent further storage of the documents on the criminal

judicial proceedings for a specific immigration law decision

was, however, was not carried out. Rather, the LEA stated that these intermediate

should have been destroyed in time, and regretted that this was not done.

We then issued a warning. The documents ready for deletion were as

the person concerned confirmed to us, immediately removed from the file.

40

41

42

43

44

Section 87 (2) Residence Act.

Section 87 (4) sentence 1 of the Residence Act i. V. m. No. 42 of the order on notifications in criminal matters (MiStrA).

Section 91 (2) AufenthG i. V. m. Section 91.2.2 of the General Administrative Regulation on

Residence Act.

See Section 51 (1) of the Federal Central Register Act (BZRG).

See BVerwG, decision of September 23, 2009, 1 B 16.09.

In the management of files and files by the immigration authorities must be on

care must be taken to ensure that only the residence law procedure requires

documents and data are kept available. The statutory cancellation and

Deadlines for destruction must be observed.

2.6 Census 2022 - The great census

This year it was that time again: Many Berliners received mail from the Office for

Statistics Berlin-Brandenburg. They were asked to answer a question

to answer numerous questions about their personal living conditions

and thus reveal information about yourself. Private owners of residential

ments or buildings with living space were also required to provide information

to own their own home.

Due to a regulation of the EU 45 must in all member states and thus

A census of the population is also carried out throughout Germany every ten years

become. Such a census is also known as a census. In addition to information

information on the population is also collected as part of the census of buildings and

Information on the building and housing stock is determined. In Germany found the
last comprehensive census of the population took place in 2011. A originally for
The census planned for 2021 was postponed by one year because the extensive
Preparatory measures not implemented on time due to the corona pandemic
could become.
In particular, the census determines how many people live in Germany
how they live and work. Many rely on these statistical surveys
Federal, state and local decisions. In order to
The EU has to receive uniform data on the population and their housing situation
a catalog with characteristics to be collected. Primarily for this
Data from the population registers is used.46 The registration authorities transmit data for this
of all registered persons to the statistical offices of the federal states. In addition, one

45

46

Regulation (EC) No. 763/2008 of the European Parliament and of the Council of 9 July
2008 on Population and Housing Censuses.
Accordingly, this procedure is also called “register-based census”.

Household survey carried out by random sample. The households to be surveyed
Persons are determined by random selection and by the responsible statistical office
State office contacted. This household survey is used for quality assurance
determining the official number of residents. There are thereby over and
Under-recordings uncovered and missing data in the population register
established. In addition, surveys are also carried out for household samples
led, in which extensive information must be given.

The census in 1983 was the reason for the first fundamental judgment of the Federal constitutional court (BVerfG) regarding data protection. Thus the BVerfG has enacted census law to be partially unconstitutional explained and the count stopped. In this so-called census judgment that became The fundamental right to informational self-determination was formulated for the first time.47 It has been one of the main pillars of German data protection. Regarding the register-based survey method, in which the existing databases of the state Administrative registers used as basic information and through household samples be supplemented, the BVerfG confirmed in 2018 that this procedure constitutes is compliant.48 This results in a so-called full count, in which all citizens be counted and questioned in Germany. Since there is less house need to be questioned, the collection of data from individual persons will also become necessary limited to a minimum.

It cannot be denied that in the course of carrying out the census in large amount of personal data is processed. For those affected The data processing must therefore be traceable to persons.

Compliance with the transparency requirement is particularly important because the processed information is not only collected from the citizens. It requires e.g. therefore specific legal bases for the census procedure.49

47 See BVerfG, judgment of December 15, 1983, 1 BvR 209/83.

48 See BVerfG, judgment of September 19, 2018, 2 BvF 1/15.

49 With regard to the 2022 census, these can be found above all in the 2022 Census Preparation Act (ZensVorbG 2022) and in the 2022 Census Act (ZensG 2022) and specifically for Berlin in

Census Implementation Act Berlin 2022 (ZensusAGBln 2022).

2.7 Open distributors remain a problem

sports clubs and gyms

It's true that the first e-mail was sent more than 50 years ago: the tiresome thing

Regrettably, the problem of "open distributors" still does not belong

of the past.

If you write e-mails, you have the option of sending the text to several recipients at the same time.

ger:innen to send. In the usual e-mail programs, in addition to the

classic recipient field "To:" the fields "CC:" (for "Carbon Copy") and "BCC:"

(for "Blind Carbon Copy"). If the e-mail addresses indicate the recipient:in-

between themselves may not be revealed is only the last-mentioned possibility

data protection compliant. Again and again, however, get through careless use

the fields "To:" or "CC:" the e-mail addresses of all recipients in the wrong

hands. When it comes to promoting a gym, like the content

of the e-mail itself to be harmless, the e-mail addresses provided by others

Recipients are not. In the work of the association it also happens that members,

who are in arrears with their membership fees are contacted via a group

become. However, it should be ensured that not all group members

find out from each other who is also still in default.

Even if the relevant incidents are usually due to simple oversights

can be traced back, they should always be a reason to

to subject work processes to a critical examination and employees in the

Training in handling personal data.

It will be the rule rather than the exception that the use of an open

Distribution list to a reporting obligation to the responsible supervisory authority because of a

data breach.50 It may also be necessary to inform the data subjects

to notify.51 Those responsible are well advised to contact the relevant

Familiarize yourself with duties in advance so that, ideally, it doesn't even become one

50

51

See Art. 33 GDPR; see also Annual Report 2018, 1.3.

See Art. 34 GDPR.

data breach is coming. The responsible body may have a data breach

etc. report to us via our website.52

2.8 Not just since the pandemic: working from home in the Club work and the use of private devices

What was still new for some employees at the beginning of the pandemic

may be, has long been the norm for many volunteers in active association work.

Especially where there is a lack of resources and no clubhouse with its own digital

infrastructure is available, personal data is already available

processed by volunteers at home on private devices.

If at all possible, we recommend the purchase of digital end devices that

serve club purposes only. These can be secured separately.

This means that there is no risk of mixing with private data, nor should it

transfer of databases and devices in the event of a change of office, the association

their challenges. Nevertheless, the use of private end devices is

Management of member data is not fundamentally impermissible, but increases for the association

and for the members, the effort and the risks. We generally advise against the

Mixing of private and club-related data, not least because experienced

As a result, also in association work, it cannot be ruled out that after termination

of the cooperation, personal data remain on private devices

it due to negligence or even after separation in a dispute. Whether these risks are effectively

can be caught must be considered by the club management on its own responsibility

and make responsible decisions.

As a minimum safety precaution, we recommend that you only use your own

n, local and fully encrypted storage medium, such as a USB

stick or an external hard drive. At the same time, access control to a

privately used device by means of password protection, which guarantees that the

private device is used exclusively by the club member and in particular also

no household members have access to personal data of members of the

52

See https://www.datenschutz-berlin.de/datenschutz/datenpanne.

have club. Creating a separate device account for club work is

to recommend. In addition to the data itself, data transport must also be encrypted.

It should be a matter of course that current operating and security software

(e.g. virus scanner and firewall) and all security updates are installed or

be installed regularly and promptly.

Furthermore, there must be a deletion concept, e.g. B. to the question of how data ends

can be validly deleted. This includes a binding agreement with

the association member about the secure handling of personal data. A

A passage on secrecy is essential. The association should also

expressly stipulate the right to deal with club-related data on the private end

device to be able to proceed in principle in the same way as with those in the
own systems: The club should have unrestricted access to the data and they
can also be deleted if necessary. This must be done when the cooperation ends
Club member will be obliged to return the data or irretrievably
to delete. However, none of this releases those responsible from
different data categories and dutifully weigh them up: Employ-
Data such as data or account data of members should be treated with the utmost care
and will only be handed over if the processing is not different despite all efforts
can be guaranteed.
If the board of directors decides to use a cloud service, the
Club an order processing contract 53 with the cloud service provider in advance
close. Of course, the relocation of the data to the cloud must not result in a
effect on the level of data protection, this applies in particular to the encrypted one
Transfer and storage of data, the obligation to make backup copies 54 and
Choosing a trustworthy service that is GDPR compliant.

53 See Art. 28 GDPR.

54 See Article 5(1)(f) GDPR.

2.9 Finish only against photo?

We repeatedly receive inquiries and complaints from concerned parents who
consent to the publication of photos at sporting events for their children
should gene. We intervene in particular if participation in the event
is made dependent on such consent, including at events

for adults.

If organizers rely on consent as the legal basis for the

If you want to invoke the data processing under consideration, it should be noted that the consent

must be based on the free decision of the person concerned.55 Only then is

them effective. In addition, consent must be given in an informed manner

be.56 The so-called coupling ban is also decisive. After that, “the circumstance

[to take into account] to the greatest possible extent whether, inter alia, the fulfillment of a

trags[...] from the consent to the processing of personal data

dependent, which are not necessary for the fulfillment of the contract".57 These pro-

schrift applies to participation in sporting events as well as to the

membership in clubs.

If participation in an event can only be perceived in such a way that

consent to data processing must be given in good time, which is not mandatory

is necessary, this does not count as voluntary consent. absolutely necessary

are in the club work and for the implementation of sporting events classical

only show the name, start number and contact details of the athletes, if necessary also theirs

Gender and their dates of birth and payment, but not the illustration of the

people at the event. For the voluntary consent to such

photos, it is therefore irrelevant whether the person concerned would also have the opportunity

attend another event instead, or simply not at all

to compete

It cannot be ruled out from the outset that, for example, the organizing club

take photographs for documentation purposes or for public relations work

55

56

57

See Art. 4 No. 11 GDPR; Art. 6 (1) sentence 1 lit. a GDPR; Art. 7 GDPR; EC 42 GDPR.

Art. 4 No. 11 GDPR.

Art. 7 Para. 4 GDPR.

leaves. Especially with the publication of the photos also about the circle of its members

Beyond that, especially with photos of children, is the necessary balancing of interests

However, those responsible should exercise particular caution. This also applies to

the publication of names, game lists, result or winner lists.

This type of publication seems absolutely necessary - even if it is common -

not: An indication as "N. N." or similar stands for those affected who do not publish

wish, nothing against.58

For external photographers who, for their own financial interest, want to

Produce and sell photos of sporting events are not the organisers:

or the club responsible; nevertheless applies here equally that for a

Publication regularly requires the consent of the persons depicted

is. The situation with press photographers is different again, but they

are also required not to allow single photos of children without parental consent

publish.

It is important to us that clubs and organizers with flawless data protection

declarations and are aware of the legal bases that apply to them

allow the processing of personal data. Enforced Consents

on the other hand, do not provide any effective legal basis for additional desired

works. A link of membership, participation or performance of a contract

with the processing of data that is not required for this is not permitted

and is followed by us.

58

See also JB 2019, 3.9; JB 2021, 3.7.

35

3 judiciary and legal profession

3.1 The scope of judicial activity - When we for courts have jurisdiction

Again and again we receive requests from citizens, decisions from courts or behavior of judges in the oral hearing on data protection review legal aspects. According to the express will of the Basic Law zes 59 but we stay out of everything that the important judicial independence could affect.60 A long-awaited judgment of the European Court of Justice hofs (ECJ) should bring clarity to the question of which activities are involved in individual are meant.61 Unfortunately, even after that, a lot remains open.

The background to the proceedings pending at the ECJ was that a court in the Netherlands journalists granted access to court files in order to include them in the able to give a more accurate report. The personal data of Those involved in the proceedings were not regularly made unrecognizable. The ECJ had to decide whether this granting of access to files was exempt from the control exception is covered and therefore no supervisory powers of the Dutch data protection supervisory authority exists. The ECJ initially finds clear words for this: “Preservation of the independence of the judiciary requires [...] that the judicial functions in be exercised with complete autonomy, without the courts […] of any Provide orders or instructions so that in this way they are attacked or protected from outside pressure, which the independence of the judgment of their could endanger members and influence their decisions.” 62 The Ver-

Works that the supervisory authorities are not allowed to check are therefore not only

59

60

61

62

Art. 97 para. 1 Basic Law (GG).

The European legislator and the House of Representatives are also clear on this: see

Art. 55 Para. 3 General Data Protection Regulation (GDPR); § 8 para. 3 Berliner

Data Protection Act (BlnDSG); Section 46 (1) sentence 2 BlnDSG.

See ECJ, judgment of March 24, 2022, C 245/20.

ECJ C 245/20, paragraph 33.

Processing "in the context of specific legal matters [...], but in a broader sense

all processing operations [...] carried out by the courts in the context of their judicial

activities are carried out".63

The court thus traces the problem back to itself, because what exactly the

framework of the judicial activities of the courts should actually be made clear

be asked. In any case, the ECJ leaves no doubt that wherever

where the "control [...] directly or indirectly the independence of the members

or could influence the decisions of the courts",64 no jurisdiction

of the data protection supervisory authorities should exist. Still, the decision is not

to be read in such a way that they inform other responsible persons who only work for the court

our supervisory activities, because are excluded according to the wording

only the courts themselves. As a result, the disputed document

insight still remain in the area free of supervision, since they belong to the "communication policy

tik to legal matters".65 In any case, it would be "clearly connected" to the

exercise of judicial activity; 66 unfortunately not very selective in practice

Conclusion.

It will therefore still have to be clarified in individual cases which activity is inherently justifiable

is of an objective nature.67 In addition, there is now the question – which is not entirely new to us – as to which one

Activity that in itself does not shape the case law, possibly

nevertheless affects the independence of the courts in such a way that, in the event of a con-

trolls could no longer make unbiased decisions through us. The always necessary

Clarification can only take place in dialogue with the courts and will continue for the foreseeable future

Time master our work in this area, the workload at the

Under no circumstances reduce court administrations and our complainants

cost more nerves.

63

64

65

66

67

ECJ C 245/20, paragraph 34.

Ibid.

ECJ C 245/20, paragraph 37.

ECJ C 245/20, paragraph 38 f.

See also the very successful approach of our North Rhine-Westphalian

Colleagues at https://www.ldi.nrw.de/zustaendigkeit-der-ldi-nrw-bezueglich-der

-activities-of-courts.

In all of this, it should be noted that in the Netherlands a specific judicial

staffed "Commission for the Protection of Personal Data for Administrative

judge" is established 68 and the persons concerned in the initial case thus have an actual

lich responsible contact person.69 Different in Germany: From the

Establishment of “special bodies in the judicial system”, the equivalent according to the GDPR

deal with complaints and ensure compliance with the GDPR,70 are

we are still far away in this country. Supervision by the presidents of the

Courts is not sufficient for this, as conflicts of interest may exist. Also

the CJEU emphasizes that the GDPR does not intend to make the courts of any

to withdraw supervision.71

3.2 Now for free and without registration:

The open commercial register

Since the adoption of the General German Commercial Code (ADHGB)

in 1861 the commercial register in Berlin - formerly under the supervision of

Corporation of the Berlin merchants - now managed by the courts and

fulfills its important contribution to the protection of confidence in legal transactions there.

In order to liven up this task, the register must be public for all interested parties

be accessible.72 With the Register Procedure Acceleration Act (RegVBG).

in 1993 the possibility was also created to publish the commercial register electronically

form.73 Since August, the information given there has been free of charge and

can be viewed electronically by anyone without registration.74

68

69

70

71

72

73

74

ECJ C 245/20, paragraph 9.

See ECJ C 245/20, paragraph 13.

Recital (EG) 20 sentence 3 GDPR.

See ECJ C 245/20, paragraph 24.

The ADHGB already points this out, see Art. 12 ADHGB: “At every commercial court
to keep a commercial register in which the entries stipulated in this code
are to be included. The commercial register is public. The insight of the same is
permitted to everyone during normal working hours. Also can of the
Entries against payment of the costs, a copy can be requested, on request
is to be certified."

See RegVBG of December 20, 1993, Federal Law Gazette I, p. 2182 et seq.

See Section 10 (2) of the German Commercial Code (HGB); implemented by the federal legislature
of the European Digitization Directive (EU) 2019/1151.

In the course of this, many of those affected have checked the entries about themselves and
found that information that was not required there - such as some private addresses,
ID card copies and signatures - have been saved and published
are. We have received numerous submissions from citizens, which we will forward to the
Responsible body, the District Court of Charlottenburg as the Berlin Register Court,
have referred. There are limits to our supervisory activities where the independence
pendency of the courts could be affected. Although an entry in the commercial
gister no adjudicatory activity in litigation, but she excels in her
Affiliation to the voluntary jurisdiction in that it is administered by judges

is carried out.75 The judicial activities of the courts are subject to our

excepted.76

If the problems cannot be clarified in the first contact, we recommend

fenen who conduct a data protection review of the procedure within the

court, contact the President of the District Court of Charlottenburg

to turn. He supervises the register judges. A special

their office for supervising data processing operations in judicial activity,

as provided for by the GDPR,77 has unfortunately not yet been set up.

It is easy for us to understand that those affected are concerned about the abuse of their

data in view of the now easier electronic access.78

Restrictions on the free availability of all register data - in particular the

Entry of data not required in the specific case - should therefore be in the interest

of the persons concerned with the persons responsible and by the legislator

be done quickly.

75

76

77

78

Section 25 (1) sentence 1 of the Commercial Register Ordinance (HRV).

See also 3.1.

EG 20 sentence 3 GDPR.

See also 10.3.

3.3 Confusion before the Federal Central Tax Office:

Not a fun case

For the control of federal offices such as the Federal Central Tax Office (BZSt)

are not us, but the Federal Commissioner for Data Protection and Information

tionfreiheit (BfDI) in Bonn.79 In the present case, however, asked

Complainant why a Berlin bailiff seized his accounts, because

he was not aware of any open guilt. The error was quickly found: Not

he was the debtor, but a namesake with whom he not only shared the pros and cons

surname shared, but also the date of birth. They were to be kept apart

Data twins only based on their place of birth - but the bailiff had

are not asked for when querying an account with the Federal Central Tax Office.

Do creditors have open claims and the hope that there is something else

to collect them, you can contact the local bailiffs.

those who then set everything else in motion. With a so-called garnishment and

In the case of a directive, these come quickly, provided there is an enforceable title

to the accounts of the alleged defaulters. If an account is not known, an inquiry will help

at the BZSt as part of the so-called account retrieval procedure. That is where information

together to account master data of all bank customers. What used to be an exam

income from capital assets was introduced, is now widely used

dung, etc. in foreclosure.80

However, the account master data often does not give the current address

Account holders. It is not uncommon for the bank to apparently only save the address

chert under which the account was opened. In the present case, neither of

retrieving bailiffs nor the creditors from the data records,

that may be considered two different people from different places

Account holders could come into question. To make matters worse, that at the

There is no possibility of using a place of birth as a search criterion when querying the BZSt

to specify. The place of birth is also not included in the search results. In this

our false debtor and his data twin would have clearly differed.

In this case, the bailiff was obliged to give the creditors the

79

80

Section 9 (1) sentence 1 of the Federal Data Protection Act (BDSG).

See Section 802l (1) of the Code of Civil Procedure (ZPO).

communicate the data determined even if he had doubts as to their correctness

had. He may only withhold them if he is aware of the inaccuracy of the data.81

In the end, against some resistance and with great

ßen effort to reverse the garnishments of his accounts. The BZSt shared

also informed the BfDI that a list of doubles is now being kept in which

Corresponding cases would be included after they became known. By legal

Adjustments would now stand for a clear identification for tax purposes

identification number available, also the automated plausibility

checks have been improved by manually processing doubtful cases.

3.4 Extract from the Federal Central Register

Public prosecutor

One complainant wrote to us that a court had in a family court

Proceedings with the help of the Berlin public prosecutor's office a federal central

register excerpt instead of applying for an excerpt from the Federal Office of Justice (BfJ)

train to request.

The public prosecutor's office had responded to a letter from the court with a corresponding

Demand - it is in a family court procedure the educational ability of the

to examine the complainant - for himself information from the Federal Central Register

drawn up and sent to the court. The public prosecutor's office at the

Query at the BfJ as intended purpose, an investigation is running against it

the person concerned, which was not the case.

After the complainant's representation to the public prosecutor's office

rightly doubts as to the admissibility of the query under false conditions

and transmission to the court. The public prosecutor's office demanded the move out

then back from the court; an unusual process, but after it has already taken place

Information now the only one remaining. The court refused a return

however off.

81

See District Court (LG) Würzburg, decision of July 29, 2014, 3 T 773/14.

The Attorney General agreed to our request for the assessment of the

public prosecutor's office and also saw in the transmission an unauthorized purpose

change.82 She assured us that the prosecutor's office in general

It is routine to register extracts when sending files to other places that are not included

are directly involved in the criminal proceedings, and withhold information from the

to apply for registers only for their own purposes, which the Senate Department for Justice,

Diversity and anti-discrimination as far as confirmed. The incident was taken as an opportunity

been, compliance with data protection issues separately in view

take. We have the procedure with a finding of deficiency towards the State

attorney completed.

The question of whether the court, in response to its own request from the BfJ,

would have received in the future must remain unanswered due to a lack of responsibility. The

The court would have to carry out the purpose of its request 83 and the BfJ the request

with a view to issuing an extract to the court. Both is

not done here.

3.5 May the public prosecutor's office provide data information

Request ID card copies?

Citizens should also exercise their right to information vis-à-vis the public prosecutor’s office

can effectively assert.84 Since it is usually a piece of information

of protected data,85 the public prosecutor’s office makes high demands

to the identification of applicants if there are any doubts in this regard

consist.

The procedure in which the request for information is processed86 is graded and sub-

resigns i.a. according to whether certain identifying features from the

existing files. Only if there are reasonable doubts about the person

82

83

84

85

86

See Section 500 of the Code of Criminal Procedure (StPO) i. V. m. §§ 49, 47 No. 2, 3 BDSG.

§ 41 paragraph 3 sentence 1, 2 BZRG.

See AGM 2021, 3.2.

See Art. 10 GDPR.

See § 500 Para. 1 StPO i. V. m. §§ 59, 57 BDSG.

identity, the public prosecutor's office may request further information from the applicant

person themselves.87 This is where the request for a copy of an ID card comes into play

Game, which, however, is also a hurdle in asserting the right to information

can represent.

The public prosecutor's concerns are basically understandable: Straight out

Unauthorized requests for information come from close family or domestic areas

into consideration, as there may be strong interests in information about life partners,

bar: inside or children exist and access to the mailing with the information

is easily possible. From our point of view, the copy or even the scan of the personal

wise but just in these cases hardly suitable, the personal identity between

the person to whom the information relates and the applicant

prove. It is precisely those people from the immediate vicinity who can also access ID card

have documents, so that requesting a copy of them does not secure them

would scare. Instead of the information from an identity document, its copy

in addition, it is likely to be partially blacked out, as can often be seen from the files

other, more reliable identifiers.88

On our doubts about the ID copy as an effective and permissible means of

reliable identification in the scenarios outlined, we have the state

advocacy advised. About the right to information from the public prosecutor

only in exceptional cases can a copy of your ID be submitted

a sensible measure. In principle, an informal application is sufficient for the application

Write; the information is free of charge.89

87

88

89

See Administrative Court (VG) Berlin, judgment of August 31, 2020, 1 K 90.19.

For obtaining copies of ID cards in the area of the GDPR, see JB 2018,

9.2.

Section 59 (3) sentence 1 BDSG. A sample application can be found on our website

https://www.datenschutz-berlin.de/buergerinnen-und-buerger/ selbstdatenschutz/

verification-of-your-data/internal-security/public prosecutor's office.

3.6 Principle of data minimization also in legal briefs

We regularly receive complaints about the processing of personal data

Data by lawyers in the context of civil law disputes

events or legal proceedings. Those affected often complain that

in the pleadings and statements of claim their personal data to the

court, the opposing party or other recipients are transmitted,

although these do not or not to the extent necessary to exercise the legal

interests appear necessary.

Lawyers are in legal or judicial matters with regard to their presentation

Process fundamentally responsible under data protection law.90 As an independent

They support organs of the administration of justice in their capacity as legal advisers

Representatives themselves are responsible for the content of the pleadings, even if they

act to protect the legal interests of their clients.

Insofar as they receive personal data from third parties in the exercise of a mandate

process, they also decide on the purposes and means of the processing

these data and are in this respect not processors 91 for the clients,

but self-responsible. It follows that they process data only then

may, if there is a legal basis for this 92 and the data protection principles 93

be granted.

As far as the processing or transmission of personal data for the purpose of

Legal prosecution and defense are based on a legal basis

can,94 the data processing in terms of type and scope is governed by the statutory

Requirement limited that processing for those purposes be “necessary”.

must. When determining the necessity, the principle of

Data minimization to be observed, of the lawful purpose and consequently

also limits the necessity of data processing. The Principle of Data

90

91

92

93

94

They are so-called responsible i. S.v. Art. 4 No. 7 GDPR.

I.S.v. Art. 4 No. 8 GDPR.

See Art. 6 Para. 1 GDPR.

See Art. 5 GDPR.

For example Art. 6 Para. 1 Sentence 1 lit. f GDPR.

minimization requires that only data serving the specific purpose, and also

only as much data as is necessary to achieve the purpose is processed

may.95 From this it follows for the data processing in the context of the exercise of the mandate,

that lawyers must always check whether personal data, e.g.

significant for the assertion of a claim in court or to safeguard

the plaintiff's burden of proof for the facts justifying the claim

are done. Unnecessary data are to be omitted or made unrecognizable.

This can be done with a reference to data protection obligations towards the

court to be justified. In case of doubts whether a factual presentation through the teaching of the blackened documents is sufficiently substantiated, can be asked if the full copy is required by the court should be.

The principle of data minimization is also applied by lawyers to are for their clients and in particular in the context of judicial Enforcement of claims or legal defense to be observed. On the transmission of unnecessary data must be waived.

95 Article 5(1)(c) GDPR.

4 Youth and Education

4.1 Implementing regulations for youth welfare in the Criminal proceedings - data protection from the start thought along

Due to numerous changes in the law, it was necessary to to update publications for youth welfare in criminal proceedings (JuHiS).96 In this In connection with this, an adjustment to the provisions of the data protection General Regulation (GDPR). The competent Senate Department for Education and Youth and family involved us in the process early on and asked for our advice asked.

In a very constructive exchange with the youth administration, we have ours Proposed changes and additions. In detail it was z. B. um Adjustments with regard to the information obligations existing under the GDPR ten. Another aspect were regulations on the forwarding of personal Data by JuHiS to the probation service for young people or to independent organizations

of youth welfare, where special attention is paid to the transparency of data
processing for the young people was to be addressed. Since the JuHiS
processed personal data is social data that is subject to a
subject to their protection, it is particularly important that the implementing regulations
the sometimes very abstract legal regulations in a practical way
concretize.
It has been shown that appropriate votes can be taken in a short time
can, if we are involved at an early stage and the Senate Department for Education,
Young people and families can advise in good time. For the JuHiS, explanations could
regulations come into force that are both practical and data protection
are compliant.
96
Available at https://www.berlin.de/sen/jugend/recht/220501-av_jgh.pdf.

if there is a suspicion of endangering the welfare of the child
The Senate Department for Education, Youth and Family is developing an action
guidelines to inform childminders about how to deal with and
to support the driving process if there is a suspicion of a child endangerment. We
advised the Senate Administration on individual issues.
Do childminders suspect that one of them is being cared for
If there is a threat to the child's well-being, it is important that they know
what to do. In addition to the professional, personal and emotional challenges
ments in such a situation, the childminders also have data
to clarify legal questions. Because personal data of children and

Persons with custody may only be regularly transmitted to the youth welfare office
if there is a legal basis for this. As a rule, a
Distribution to the youth welfare office only come into consideration if the endangerment is not
can be averted otherwise.
Part of our consultation therefore concerned the question of what legal basis for the
Data transfer to the youth welfare office can be considered. So in case of one
child welfare endangerment, childminders can also act with legal certainty,
the federal legislature has adapted the provisions in children and youth law.
The circle of those institutions that have a protection order in the event of a child
have been expressly expanded to include day care workers. So it is-
more regulated that childcare workers are also more important when they become known
indications that a child you are caring for is at risk.
have to make an assessment. A specialist with experience in this respect - a
Person qualified to assess child endangerment - advisory
consult.97 Furthermore, the legal guardians and the child are to be put at risk
to include the child assessment, insofar as this provides effective protection for the child
is not questioned. Child day care workers must in principle
an "original-own" assessment of the hazard risks and situation of them

97 Section 8a (5) of the Eighth Book of the Social Code (SGB VIII).

child being cared for. The use of advice by an insofar
experienced specialist is therefore of particular relevance.
Day care workers are also obliged to inform the legal guardians
work towards the use of assistance if they deem it necessary.

If the hazard cannot be averted in any other way, there is also a

obligation to notify the youth welfare office. This means that the involvement of the youth

office - as well as specialists from other institutions and services - in the

This is usually only possible if this is absolutely necessary to avert the hazard

is. In order to create transparency for the legal guardians, we have

It is recommended that these legal obligations already be met at the beginning of childcare

point out care.

The risk assessment of day care workers with clues

for a child endangerment can be difficult in individual cases, so that the

consultation of a qualified specialist is of particular importance.

It is important to give the day care workers support as they feel in the

should behave in the event of important indications of a child endangerment

also to be on the safe side in terms of data protection.

4.3 Say Cheese! – Image, sound and video recordings in day care centers

Taking photos is part of day-to-day life. Regarding the to be observed

However, data protection framework conditions arise again and again

Questions. This year we again received various inquiries from

day-care centers and affected persons, under what conditions photos,

Videos and sound recordings made by children in the day-care center and

may be passed on.

As a rule, the production of image, sound and video recordings requires

children and their disclosure, publication or other use

the effective consent of the child's legal guardians. has consent

to be guided by the requirements of the GDPR.98 This means that the

Consent must be informed and voluntary. In the declaration of consent should

in addition to a description of the purposes of the recordings 99 that is as specific as possible

be explicitly defined in which way the recordings are used or (further) processed

who applies 100 and who they are shown or given to. In practice

it makes sense for the individual types of recording (image, sound or video recordings)

to provide checkboxes in each case. In addition, the day-care center should point out that the

legal guardians have the right to revoke their consent at any time with

to revoke this right for the future. The consent should be given in writing by the day-care center

must be obtained before the recordings are made. The ones of us together

published with the Senate Department for Education, Youth and Family, already in

2nd edition brochure "Data protection for image, sound and video recordings" 101

continues to offer assistance for day-to-day daycare.

When passing on recordings to the legal guardians, it should also be noted that

technical and organizational measures for the protection and security of the

to take measures: If the recordings are distributed, for example, using a data carrier

are to be recorded, e.g. B. be protected by encryption,

that in the event of the loss of the data medium no third parties gain knowledge without authorisation

can. Especially when using communication services, such as when

sand via messenger service, the day-care center must ensure that

these can be used in accordance with data protection regulations. This is not always the case in practice

the case.

The creation of image, sound and video recordings in a day-care center

nothing stands in the way if effective consent of the legal guardians of the

children are caught. When using messenger services must in advance

It can be checked whether the use can be made in compliance with data protection.

98

99

100

101

See Art. 7 GDPR i. In conjunction with Art. 4 No. 11 GDPR.

For example, taking photos on trips or events, showing film sequences

at a parents' evening, creating teaching materials, etc.

For example for publication on the website, for print publications, as notices in the

premises etc.

Available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/

brochures/2020-BlnBDI-Datenschutz_Bild_Ton_Video.pdf.

4.4 School digitization and data protection

As in previous years, we were there with different topics this year

the digitization of schools. After we also from last year

were able to report positive developments, e.g. B. from the amendment of the data

protection regulations of the Berlin School Act (SchulG), in which we

have extensively advised the House of Representatives,102 this year was largely

marked standstill. The education administration has our advice on many data

intellectual property issues are either not obtained or our recommendations are not

recorded.

4.4.1 Legal bases

We have pointed out several times that the ongoing

Revision of the School Data Ordinance 103, which has been in force since 1994, and now also the

Creation of the ordinance on the use of digital teaching and learning materials at last

must be completed. In addition to those that came into force in October 2021

School regulations must have a concrete form of the statutory

Framework conditions in the interest of school practice in the regulations mentioned

be done promptly. We have been supporting the process since 2018, but we have to

that still not all data protection requirements are taken into account

have been.

On a positive note, the Senate Department for Education, Youth and Family

from their position, which was still held in the middle of the year, that it would be sufficient simply to

to amend the data regulation, has moved away and in the autumn presented us with the draft of a

Digital Teaching and Learning Aids Ordinance. Since the school data regulation

rather on the processing of personal data in the administrative area of the

schools is applicable, we think it is very important that all related

data processing related to the digitization of schools in everyday school life, e.g. B.

when using learning platforms and video conferencing systems and when using them

digital end devices or in electronic communication, in a separate

Regulation to be regulated. Such an ordinance can then also be applied at any time

102

103

See 2021 Annual Report, 1.2.1.

See 2021 Annual Report, 1.2.2.

be adapted to a changing technology. Unfortunately, those from the educational

management proposed regulations in the draft are still too vague to

to provide schools with practical assistance. We have this opposite of

Senate administration problematized and a tightening of the regulations recommended. The

We will continue to accompany the process.

4.4.2 Berlin school portal

Last year, the Senate Department for Education, Youth and Family

portal as the central switching point for a large number of different services and

publicly announced in the school context. Via this school portal, for example, the

Registration of teachers and students in the learning management systems "Lern-

raum Berlin" and "itslearning" as well as other learning platforms that schools are provided with by the

educational administration are offered. Already in school

portal for some of the teachers, access to the e-mail accounts integrated via the

official e-mail communication is to be conducted. The Senate administration plans

for the future a significant expansion of the functions of the school portal. So should

legal guardians can also register there in order to use certain services,

such as B. the issuance of school certificates.

Since central services are made available via the school portal and access

to the personal data of a large number of different users

user groups, which is to be further expanded in the future, it is necessary

that the school portal is operated securely.

So far, we have not been sufficiently involved in the development of the school portal.

gen. The documents handed over to us, such as the data protection and IT security concept

showed serious deficiencies in terms of compliance with data protection law

regulations and in particular with regard to IT security. Already in the novella

tion of the SchulG, we have pointed out that for the operation and also the

Functionalities of the school portal in view of the large number of personal

son-related data of students: inside and teachers a legal basic

location is required. So far, such a system only exists for the subarea of identity

management. We have this to the Senate Department for Education, Youth

and family also made clear. Unfortunately, the school administration has us in the further

Process no longer included.

In addition to creating the missing legal basis, the education administration must

advance the IT security process in particular and determine which measures

measures are necessary to secure the school portal, then immediately

to be able to implement. This would take the form of a data protection impact assessment

start of operation must happen. Since the school portal is already productive

is used, such must be made up for urgently.

4.4.3 Devices and email addresses for teachers

The Senate Department for Education, Youth and Family has mobile

End devices procured and these have already been issued. The devices become central

managed. Registration takes place via a separate user ID for teachers

from the school portal. The teachers also receive business information via the end devices

Email addresses provided. Again, we were not in the conception

integrated. A data protection impact assessment is also not yet available.

4.4.4 White List

The Senate Department for Education, Youth and Family is legally obliged to

increase which digital teaching and learning materials are suitable for schools.104

This positive list is intended to make it easier for schools to select suitable software by

the products have already been tested by the Senate Department for their educational suitability

and checked from a data protection and legal point of view. In the preparation of

our authority has not been involved in this list so far. Since the test criteria up to us

was not available at the time of going to press and was also not publicly viewable

The process of evaluating the educational administration is incomprehensible to us. Ground-

In addition, we consider it problematic that the list is not publicly accessible

is. We are also not aware of the criteria by which the Senate Administration

Checks the data protection compliance of the products. In this respect, we cannot assess whether the

examination can lead to a result that schools can use. it is crucial

that the schools fulfill their obligations as controllers under the GDPR

can.105 The Senate Administration is therefore obliged to provide them with the results of their

to provide information.

104

105

§ 7 para. 2a sentence 2 SchulG.

See Art. 4 Para. 7 GDPR.

We would have the education administration in this so central point of the examination of the data

protection compliance of digital products used in schools.

However, our expertise was again not used. Granted-

In the future we will review the list as part of our supervisory responsibility and

evaluate.

4.4.5 Devices for students

At the end of the year we found out about the Senate's plans for future students

to be equipped with digital end devices across the board. After the one presented to us

The concept should be these devices, which will be available to the students of the

7th grade to be issued to tablets from a US vendor

act. The problem is that the use of these devices requires personal data

must be sent to the manufacturer. It is not transparent in which

Personal data of students would also be affected. In addition

the devices should be managed centrally, including a so-called mobile device management
(MDM) should be used. Such an MDM allows extensive access options
abilities to the devices: Many MDMs enable remote location data
retrieve and install software; with some MDM can even be made from the
Create remote video and audio recordings.
Since the education administration did not involve us here either, we have no information
information that enables us to make an assessment. Due to the available to us
However, based on the information provided, we must assume that the operation
of these devices cannot be carried out in compliance with data protection regulations. This applies in particular in
Case of private use of the devices by the students. The education administration
must take steps to minimize the risk before purchasing these devices,
that personal data of students is transmitted to the device manufacturer
become. In addition, it must be ensured that the devices are not used for monitoring
children and young people can use. We also have the same
as part of the hearing on these plans in the Education Committee of the MEP
tenhauses and recommended a device and operating system independent
solution to consider.

4.4.6 Berlin teacher teaching school database

The consultation process between the education administration and our authority for
liner teacher teaching school database (BLUSD or LUSD) was also included in this
year continued. We perceive a very constructive exchange here. Our return
wise are accepted by the education administration and usually implemented.
A specific problem at the moment is that schools are forced to use the LUSD
are legally obliged, but this regulation does not apply to the school authorities. While

Although most school boards now use the LUSD to carry out their duties

use, the education administration pointed out to us that individual districts only

reluctantly from the unencrypted, i.e. non-compliant e-mail transmission

want to move away from the processing of personal data in the training and retraining process.

There is a need for action on the part of the legislator here. We are willing to give us

to advise on a practical solution.

With the exception of a few areas, we must again note that significant

Significant deficits with regard to the data protection-compliant digitization of schools

consist. These are also due to the fact that the educational administration

our advice either too late or not at all or our recipient

fails to pick up. Once the course has been set, it can often be changed later

Project progress either not at all or only with difficulty and with considerable (financial)

correct effort. However, data protection is not an obstacle. early thought,

it also opens up new possibilities. We continue to stand with constructive advice

available and expect that our recommendations will be followed in the interest of all those

be accepted by the Senate Administration.

54

5 health

5.1 Order processing in hospitals -

Amendment of the state hospital law

(a continuation)

In 2020, the legislator had set the requirements for order processing in health

hospitals in the State Hospitals Act (LKG). Dem was a perennial

Coordination process between the responsible Senate administration, Senate Chancellery,

kenhäuser and our authority.106 The regulation should only be two

Years later, in October of this year, come into force. Just before that date

the coalition factions then presented a completely new draft.

In the course of the amendment of numerous state laws in 2020, the LKG, the

contains special data protection regulations for hospitals, the necessary adjustments

Amendments to the General Data Protection Regulation (GDPR) have been made.107

The 2017 amendment to the Criminal Code was taken into account

a general right of disclosure for the use of service providers

introduced for order processing. Accordingly, the for the hospitals

very practice-relevant regulation on order processing in the LKG adapted.108 By 2020

hospitals could only process data from patients themselves or

have it processed by another hospital on behalf of you. In addition, a

Processing by processors is possible if the data to be processed

were changed before the handover in such a way that the service providers do not recognize them

could identify which patients they refer to. Presented this scheme before 2017

an exemption from the duty of confidentiality that goes beyond federal law

it was then perceived as restrictive by many hospitals. In the course of

106

107

108

See 2020 Annual Report, 5.1.

See Art. 5 of the Act on the Adaptation of Data Protection Provisions in Berlin

Laws to Regulation (EU) 2016/679 (Berlin Data Protection Adaptation Act EU)

from October 12, 2020, GVBl. 2020, p. 807, 818 f.

See § 24 Para. 7 LKG.

digitization, they saw an urgent need to open up the restrictive

Regulation on the use of service providers.

The result of a detailed consultation process with our authority

then a draft regulation that gives the hospitals new opportunities for the

would have opened up the processing of patient data by also accessing this

own subsidiaries or other group companies or those of other health

houses could have resorted to. Shortly before the adoption of the corresponding

draft law, the House of Representatives, however, decided this regulation only two

years later, in October 2022. Significant under data protection

tete this, that without a special regulation in the LKG, at least for the two-year-old

Transitional period, only the general provisions of the GDPR on the

processing were to be observed. A disadvantageous situation for the patient,

that of the federal legislature within the framework of its legislative competence for others

professional groups had avoided.

But things turned out differently than the 2020 version of the law intended.

Shortly before the October 2022 date of entry into force, the coalition factions

present a new draft. The reform carried out in October 2022 had

The aim, on the one hand, is to allow hospitals to process orders on a larger scale

enable when the temporarily suspended regulation allowed, but on the other hand

to close the gap in protection, particularly in the case of careless use

global service providers are threatening. Because while in Germany about the

Regulations on the protection of secrets ensure that processors

have to guarantee the same protection as their clients and themselves

would otherwise make it punishable,109 this no longer applies if the application

area of the German penal code is left. It must therefore be governed

It is guaranteed that only such services will be used

are provided abroad, the processed data are subject to the same criminal

experience legal and procedural protection as in Germany. In addition, one must

Access by parent companies from third countries to patient data

be closed, regardless of whether this is for the purposes of product development

or the fulfillment of orders from the authorities of unsafe third countries.

109

See § 203 Para. 3, 4 Penal Code (StGB).

We discussed these considerations in the consultation on the draft law submitted to us

throw forward.

The version of the regulation now passed by the House of Representatives bears the

Data Protection Requirements Bill.110 Opposite the rule adopted in October

Should come into force in 2022, the regulation is more extensive, since it also includes data processing

services that are not carried out by a hospital or a company of a health

be perceived as a house group. By doing so while European cloud solutions

possible, but at the same time companies are excluded which, due to the

applicable law in third countries may be required to provide personal data

Releasing data to authorities in third countries became a workable compromise

found. We welcome the fact that the regulation expressly provides that the

work may only be carried out by persons who, according to the law applicable to them

a duty of confidentiality corresponding to German criminal law and a

subject to the right to refuse to testify.

Since patients usually have no choice as to whether they go to a hospital

go or not, it is necessary that their data are regulated by law

be adequately protected. With the revised version of the regulation for the order

processing in the LKG, the legislator has set the conditions for this in a way

regulated, which meets the special need for protection of the data of patients

carries. We will monitor the implementation of the regulation in practice.

5.2 Where is the responsibility? handling of Health administration with data from in Vaccination centers vaccinated people

For the online booking of appointments for vaccination against SARS-CoV-2 in the

The responsible Senate administration used the vaccination centers set up by the State of Berlin

for science, health, care and equality also in 2022

the services of a processor. To schedule a vaccination appointment online,

the citizens had to create a user account with the processor and

110

See § 24 Para. 7 LKG.

enter into a contractual relationship with them for this purpose. Many citizens were also

surprised by an e-mail from the processor after the vaccination in which they

was informed that their personal vaccination documents (including the completed medical

nesebogen) had been uploaded to their user account. When viewing the

Some Berliners did not find their vaccination documents uploaded to the Zerkonto

own documents, but the documents of other people.

That a processor processes the personal data that he has for the responsible

should process it, not for its own purposes - specifically for a between him and

the contractual relationship to be entered into - may process, we have the

Health administration explained several times since the end of 2020. We demanded

they repeatedly take steps to maintain a privacy-compliant state

to manufacture. The health administration has not complied with this request.

Instead, she entered into the contract with the processor without the data protection legally required adjustment extended. Consequently, citizens who online wanted to make an appointment in a Berlin vaccination center, also in 2022 Set up a user account with the processor and a contractual relationship for it enter into with this. We have urged the Senate administration to ensure that the contractual relationships with the processor - if the Berliners do not want to keep the user accounts - are automatically terminated as soon as the Accounts no longer required for scheduling appointments at Berlin vaccination centers- are.

In addition, we cannot see any legal basis for the health administration to the vaccinated persons a copy of the vaccination documents in their user accounts used in the agreement. This processing is in Connection with the vaccination not absolutely necessary. Unless the vaccinated People should be provided with their health data in this way, that's just it with their express consent and under special safety precautions allowed. The Senate administration sees this differently and sticks to the ten data processing. The risks of this unnecessary data processing have been in the cases before us, in which the documents are wrong people were clearly shown.

After all, we were able to get data from people who agreed to a have not noticed the vaccination date, now according to the Senate Administration be deleted at regular intervals. In view of the previously presented Deficiencies in the design of the order processing relationship, which related data including the health data of a large number of citizens

ger:innen concern us, the topic will continue to occupy us.

Personal data may only be processed by processors on instruction

of the person responsible are processed. Breach processors

here against, those responsible must ask them to submit a data protection

into a compliant state and, if necessary, terminate the cooperation. We

the responsible health administration has referred to this requirement on several occasions

pointed out. People expect the public sector in particular to

Data security-oriented, data-saving and in strict compliance with the purpose

binding processed.

5.3 Appointment Reminder - Medical Offices

send messages to wrong people

Also this year we received many inquiries and complaints from patients

who use an appointment management system of a service provider by medical

general practices. The service provider will u. insofar as a processor for

Physicians working throughout the Federal Republic when he ordered from the practices

Appointment confirmations and reminders via SMS or email to the patients

sent. In some cases, however, such messages did not come from the right ones

patients, but with other people.

The sending of appointment messages by medical practices to patients

only permissible if the patients have expressly consented to

their telephone number or e-mail address can be used for the appointment message

may.111 In addition to obtaining the patient's consent, the practice

employees: make sure that they enter the e-mail address or telephone number,

111

See also JB 2019, 6.3; JB 2021, 6.5.

to which the appointment message is to be sent correctly. Because a single

ger small transposed letters or numbers can lead to a person who

has nothing to do with either the practice or the appointment, to an appointment with someone else

is remembered.

However, since the news often contains neither the contact details of the practice nor a

unsubscribe link, it was for the recipients of those messages

almost impossible to delete your e-mail address or your tele-

phone number that was processed without your consent. Since only the

name of the service provider emerged from the messages, the affected

to people with a request to delete their e-mail address or telephone number

this company. This informed the persons concerned - as from those with us

submitted complaints - but neither the contact details of the actual

responsible practice, nor did it inform the practice of the misguided one

Appointment message and the corresponding deletion request from the recipient. The

data subjects whose e-mail address or telephone number has been unlawfully

was used, this procedure means that both the medical practices,

who initiate such appointment messages, as well as by the processor

left out in the rain by the service providers used.

Medical practices not only have the technical and organizational measures

to meet people who want to send messages to wrong recipients.

prevent. You should also include an unsubscribe link in the messages,

through which those affected can refuse to receive further messages.

5.4 Vaccination invitations from the health senator to minors

In July 2021, the former Senator for Health, Nursing and Equal Opportunities

shipped. As part of our supervisory activities, we received numerous complaints

those of people who object to the invitations addressed to their children

judged In order to be able to investigate the matter, we asked

responsible senate administration to answer a series of questions. the us in

The answers finally communicated this year indicate that the substantive

We do not meet the requirements for data protection information prescribed by law

were taken into account.

In the letter of invitation from the senator, the requirements of Art. 14 GDPR

not considered. Since the personal data (names and addresses of the

children and young people) who are assigned to the Senate Administration by the State Office for Citizens

and regulatory affairs (LABO)112 for communication

should be used with the persons concerned, the health administration

held responsible, at the latest at the time of the first notification

to comply with their information obligations towards the data subjects.113

Corresponding data protection information is more precise for the data subjects,

transparent, understandable and easily accessible form in a clear and simple

chen language.114 This applies in particular to information that - like

here - aimed specifically at children.115

In the senator's letter, the children and young people addressed were

neither precise nor transparent nor in an easily accessible form about the processing

informed of their personal data in connection with the letter. It

rather, there was no such indication at any point. In addition, there were none

Contact details of the official data protection officer of the responsible Senate

administration included. Furthermore, there was also a lack of information on the legal basis

location for data processing, information on how long the data will be stored,

the indication of the source from which the address data originates, as well as the information about

the rights of data subjects.

We expect that the requirements for data protection information to be provided

be observed in the future. We have informed the Senate Administration of this. On our

Asked when exactly the data of the data subjects was deleted

us that the data records already after the invitation campaign under consideration

were deleted after inspection of returns.

112

113

114

115

According to § 34 of the Federal Registration Act (BMG).

See Article 14(3)(b) GDPR.

Art. 12 para. 1 sentence 1 1st clause GDPR.

Art. 12 para. 1 sentence 1 2nd clause GDPR.

Are personal data necessary to communicate with the data subject

person are to be used, not collected from the data subject himself,

but e.g. B. at LABO, the data protection information must later

test at the time of the first notification to the data subject.

Especially when the group of people addressed is

Minors are acting, it is necessary that special attention to understandability

the information is respected.

5.5 Open archive doors in the hospital

We were informed by a resident living near a clinic that

Dropped unknown medical records in their mailbox. In parallel

we received a data breach report from the clinic, according to which approx. 300 patient files

had been stolen. We have asked the clinic to ensure the safety of their

secure files.

Every medical treatment, whether outpatient or inpatient, must be documented

become. This documentation serves both as a source of information for the ongoing

Treatment as well as the proof of the procedure of the treating physicians

after completion of treatment. Files from the outpatient treatment to which it

in this incident are to be kept for ten years.[116] In the present

In this particular case, the management of the clinic decided to keep the files longer

as prescribed - a procedure that is regularly not classified as lawful

is—and, over the years, apparently control of file archiving

lost. The files were not kept sufficiently protected - the doors to the

Archive rooms were also open to unauthorized persons - there was still an overview of

which files were actually in what number and where.

This led to unauthorized access of an unknown extent. An unauthorized person

repeatedly got into the archive and took out bundles of files, which she

boxes and distributed at several locations near the clinic. The files became the

Clinic probably largely returned. The clinic can give an exact figure

116

Section 630f (3) of the German Civil Code (BGB).

however, only the number of files returned. How many files forever

have disappeared is unknown to her. An unsatisfactory one for the people concerned

Condition. The case shows the effects of mismanagement in the field of architecture

verification of files can have. We have asked the clinic to ensure their safety

to ensure files, to catalog the files completely and files for which

There is no specific reason for storage beyond the regular statutory period,

to destroy.

Like all carriers of health data, patient files are particularly protected

to keep. Storage must be organized so that it can always be traced

can be drawn, which files are available and which at what time

are destroy. The retention period should vary depending on justified individual cases

apart from the regular legal retention periods. currency

During the entire storage period, the confidentiality of the files is ensured by effective

to ensure technical and organizational measures.

63

6 Integration and Social Issues

6.1 Advice on consent and confidentiality

declaration of release for applications after

Severely Disabled Persons

The State Office for Health and Social Affairs (LAGeSo) and the Senate Administration

for integration, work and social affairs intend to apply for

to revise disability rights. With regard to the consent and confidentiality

In the declaration of release from duty, we have pointed out that it should be noted that

that the information in the application is as precise as possible before any

Information and documents can be obtained from doctors and other offices.

Every year, several thousand applications are submitted to the pension office after the

Disability Law 117 a. As part of these applications, which concern the determination of the

The presence of a disability and the degree of disability are specific

processed the protected health data of the applicants. Applicants must

sen provide information about health restrictions and treatments.

If further information is necessary to process the application, it can

be required, information and documents can also be obtained directly from the attending physician:

be requested to decide whether or to what extent a severe disability

change is present. In order for this to be legally possible, LAGeSo obtains consent and

Declarations of release from confidentiality from the applicants.

The revision of the forms was a consulting project that started in 2018

cess with our authority. It was about the question of whether the LAGeSo

the medical profession the declarations of consent and release from confidentiality

patient has to submit. This is usually not necessary unless the

Physicians require the submission of a corresponding declaration.118 In particular

If documents are obtained from hospitals, they usually require

moderate the template. It is important that the LAGeSo then also the explanations quickly

117

118

In accordance with Section 152 of the Ninth Book of the Social Code (SGB IX).

See Annual Report 2018, 7.2.

makes accessible. When revising the forms currently in use

we advised the LAGeSo and urged this in the interest of transparency

to be as precise as possible.

Consent must be informed, specific and given voluntarily as well

the person concerned will be informed of their right of withdrawal for the future.119

The data subject must be aware of the data that is processed on the basis of their
Consent may be processed and which persons and bodies they from
releases confidentiality. If in the release from confidentiality and consent
declaration waived the naming of all doctors and in this respect
the information provided in the application referred to under the Severely Disabled Persons Act
be sure that the information in the application is as accurate as possible before
appropriate information can be obtained from doctors and hospitals.
As part of the application process, the responsible clerks are responsible
to check that the application submitted by the applicant is as accurate and complete
dig has been filled in as far as possible. General information in the application for a residence
halt in a specific hospital without further details are not enough to
of a legally effective declaration of consent and release from confidentiality
to go out
So that the pension office can provide information and documents to the treating
Physicians and other bodies in the context of an application after the severe disability
can be obtained, it is necessary to obtain consent from the applicants.
to obtain declarations of release from duty and confidentiality. They have to
Information given in the application about the doctors and hospitals treating you
be as precise as possible so that it is clear what information is being referred to
Declaration of consent and release from confidentiality.

6.2 Proof of entitlement instead of Berlinpass

Because of the closures due to the corona pandemic, the district offices
not issue Berlin passes for a certain period of time, which the recipients

119

Art. 7 General Data Protection Regulation (GDPR) i. In conjunction with Art. 4 No. 11 GDPR.

of social benefits allow the use of benefits. This
led to the persons concerned during controls in public
verkehr (ÖPNV) and at other places their notification of benefits as proof of their
authorization had to be shown. Now the Berlin Pass should be completely abolished and through
a proof of eligibility as well as a carrier card of the Berliner Verkehrsbetriebe
(BVG) are replaced.

The Berlin Pass enables people with little or no income to do so
discounted access to education, sports, culture and local transport. The mountain
linpass provides a discrete means of credentialing, as there are no closer ones to it
Information on the specific eligibility grounds can be found. Such
Reasons only have to be given when applying for the Berlin Pass by presenting the
corresponding social benefit notifications to the district offices
be sen.

The social benefit notifications contain data that is particularly worthy of protection, such as
Reason for eligibility for social benefits, e.g. unemployment, the asylum
status or the status as a victim of SED injustice, and beyond that a variety
number of personal data such as name, address, date of birth and marital status.
It is not compatible with the requirements of data protection that authorized persons
to oblige customers to use their services when using discounted offers
notification of inspectors in public transport, cashiers at theater box offices
etc. to submit. In 2020, the Senate had those people who had a Berlin
passport because of the pandemic, although they are entitled to do so
would have been, referred to, the performance notice in the event of any checks
to submit. Those affected complained to us about this and asked for data protection
legal review.120

We investigated these complaints and contacted the BVG and the

responsible Senate Department for Integration, Labor and Social Affairs. are there

we countered in particular the argument of the Senate administration that affected

fene people would have the choice between purchasing the regular offers or

to decide whether to disclose their data, since they are currently on the perks

120

See JB 2020, 12.1.

are dependent. Data protection must not depend on the income of the persons concerned

be dependent.121

In March, we were informed by the Senate administration about a Senate resolution

informed, after the Berlin pass in its previously known form abolished and

through a new proof of entitlement in combination with a BVG carrier card

is to be replaced. We were asked for assistance in developing the new

Proof of eligibility requested. We complied with this request and have

the Senate administration later this year will advise how the new proof will be discreet

and can be designed in compliance with data protection regulations. This should go through directly in the future

the responsible service points are issued and only the

Last name, first name, date of birth and the duration of the benefit approval

of all entitled persons of the respective need or household community

shaft included. File number or other identification numbers (such as housing benefit number

mers) should not be recognizable. Finally, the new credential

with the exception of the job center, not the respective service point, but only

lich identify the state of Berlin as the responsible body, so that no conclusions can be drawn about the

Type of service can be drawn. As far as the job center due to federal law

regulations must be shown, this should be done in as discreet a form as possible

happen.

We also support the Senate Administration and the BVG in introducing the

new BVG carrier card. This should be designed in such a way that it is not obvious at first glance

can be distinguished from other BVG plastic cards. In the application process,

Finally, data are collected that are necessary to check whether the

Applicant also includes the person listed on the Proof of Entitlement

is. Both the Senate Administration and the BVG are also concerned

ensure that any service providers used also act in compliance with data protection.

Offers of public and cultural participation for those entitled to social benefits

must be designed in accordance with data protection regulations. Since the use of a

speaking authorization always the disclosure of specially protected persons

121

See also our press release of March 1, 2021, available at

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/

20210301-PM-berlinpass.pdf.

related data, priority must be given to protecting that data

lay. The danger of possibly even public stigmatization of the

affected persons when making use of the offers is under all circumstances

to avoid.

6.3 Malfunction in the elections of the senior citizens' representation

the districts

It happened this year as part of the elections for the senior citizens' representation of the districts

to a major breakdown that affected thousands of Berliners. Us

received numerous complaints. We have cleared up the case and

responsible district office Reinickendorf warned.

The law to strengthen the participation rights of senior citizens

social life in the state of Berlin 122 promotes the active participation of the

seniors and also aims to improve the solidarity community

away. For this purpose, so-called senior representatives are set up as bodies for senior citizen participation

elected at district level. Almost 70,000 seniors experienced this year

in the districts of Friedrichshain-Kreuzberg, Pankow and Charlottenburg-Wilmersdorf

a surprise: at the beginning of January you received mail from the district of Reinickendorf,

with which they were invited to the local election of the district senior citizens' representation.

Many of those affected could not understand the reasons for this

District Office Reinickendorf was in possession of their personal data and used them for the

letter of invitation, even though they lived in a completely different district.

In the course of pursuing the complaints submitted to us, we were able to resolve the case

clarify: The cause of the breakdown was a technical defect in the inserting machine

of the IT Service Center Berlin (ITDZ). The ITDZ took over the printing and the

Dispatch of the election notifications centrally for the district offices and was involved

with regard to the personal data used as a processor for

this active. On the evening of January 6, 2022, a problem occurred in the ITDZ with the envelope

animal machine so that production had to be interrupted. When rebooting

122

Berlin Seniors Participation Act (BerlSenG).

During production there was an error in the operation of the software for the

Linking the cover letter with the address data. This led to the text of

district office Reinickendorf accidentally with the address data from the districts Fried-
richshain-Kreuzberg, Pankow and Charlottenburg-Wilmersdorf. From
a total of 910,000 letters sent were for the district of Friedrichshain-
Kreuzberg 19,123, for the district of Pankow 25,000 and for the district of Charlottenburg-
Wilmersdorf 25,000 faulty. To a disclosure of the data to third parties is
it didn't come.
We have compared to the seniors department of the district office Reinickendorf, the
responsible for data protection, issued a warning.
The reason for this was the failure to have an effective order processing contract with
to close the ITDZ. The department of the district and the ITDZ have promised
to make up for this immediately and to take all measures to achieve comparable
cases to avoid in the future.
In the course of fulfilling their duties, public bodies allow personal data
Process data by IT service providers such as the ITDZ, this is a rule
moderate to see an order processing. This must be in accordance with the specifications of
DSGVO must be legally secured,123 which in particular by a
Order processing contract can take place. If this is neglected, there is a data
breach of protection.

123
Art. 28 Para. 3 GDPR.

7 science and research

7.1 Digital study aptitude tests - really one
Alternative to presence?

At first glance, digital study aptitude tests seem to be uncomplicated
solution for the selection of applicants for study places. on the two-

When carrying out such tests using your own devices, you should be careful

of the applicants in their apartments, however, significant data protection

Questions.

We have the Senate Department responsible for science, health and care

and equality as well as representatives of the universities at the beginning of the year

Requirements for digital aptitude tests for university admission

advise. The idea of one of the universities represented was to

to monitor the conduct of a study aptitude test using so-called proctoring software

to be installed on the private devices of the applicants. purpose should

be able to detect attempts at fraud at an early stage; an understandable concern.

In detail, however, significant data protection issues arose: During the

During the conduct of the digital tests, image and sound recordings should be

men of the test participants: inside as well as an automated monitoring of the

other programs running on the devices. the software

goods should for this u. a. evaluate the browser history and configuration settings

How to change the privacy settings in the browser. in their range of functions

the software thus resembled more malware (so-called Trojans) than software

that users would install voluntarily. In addition, there was the problem that

with the use of this software also biometric data - such as facial features

and eye movements - as well as other personal data - such as the equipment of the

Apartment or the documents stored on the devices used - recorded

became. We discussed the fact that the use of such software is significant

Interventions in the right to informational self-determination entails and their

legal admissibility must be examined in detail. Because a corresponding right

basis in the higher education regulations is currently missing and otherwise on-

Due to the considerable depth of intervention also with the requirements of necessity and

proportionality of such data processing is not readily in line

would be to bring, the implementation of appropriate tests using a

do not display such software on a legal basis.

Also for obtaining consent from applicants

we have no way without alternative test offers. Consent can only

be considered if the applicants are specific and transparent about the

data processing will be informed. This also includes the criteria for automatic

tized evaluations, which, however, can be changed without exact knowledge of the

used algorithms are difficult to describe. In addition, there is consent

only be considered if this is given voluntarily. Besides the possibility

required to carry out the aptitude tests using the monitoring software

there is therefore an alternative possibility of taking the tests in person at university

own devices.

In view of the considerable interventions that are associated with the use of such software products and

the automated evaluations would be connected, but it would also be required

a consent solution, initially a legal regulation in the Berlin university

law (BerlHG), which defines the legal framework for data processing

shows. In addition, it can be assumed that the regulations of the telecommunications

cation Telemedia Data Protection Act (TTDSG) for individual processes in any case

require consent that is not covered by an alternative legal basis

can be replaced in the BerlHG.124 We have the Senate Department for Science,

Health, Care and Equality and the university concerned from the assignment

the software when conducting study aptitude tests is discouraged. The involved

ten have followed our recommendation.

From both a legal and a technical point of view, the conduct of studies

aptitude tests, but also digital exams using software for

monitoring raises significant questions. In view of the requirements for a data

protection-compliant procedure, it is necessary to precisely explore the extent to which this is necessary

124

See § 25 TTDSG.

in university practice consists in using the monitoring software, and then

to precisely define the legal framework. We are happy to stand for this

available for advice.

7.2 What exactly did the person want? And what not?

A lot of data processing is justified by the fact that the data subjects

persons have (allegedly) consented to the processing. They check

However, it is often not sufficient for those responsible to know which processing operations are carried out by a

declaration of consent are actually recorded and thus allowed and which are not.

We received a complaint about a self-help organization that

who were subjected to problematic educational measures in their childhood.

In addition to offers of help for these people, the organization is also involved in

Area of scientific research into these educational measures and their

(mental) consequences for those affected. To this end, the organization led

a list with contact details of data subjects who had agreed to

To be available for surveys for research purposes.

The organization passed this contact information on to a university. The affected

should be contacted for the collection of data as part of a master's thesis.

The master's student then sent her questionnaire to almost 200 contacts

in an open e-mail distribution list. This means that all recipients of the e-mail did not have
only access to each other's e-mail addresses, they also got knowledge about it,
who in detail was also affected by educational measures, because of which
Follow the organization committed. The Master's student made a special contribution
protected data of the persons concerned openly.
One of those affected complained to us about this situation. For the
The university, which is not based in Berlin, was responsible for the disclosure itself
and therefore does not fall within our area of responsibility. However, we checked
whether the disclosure of the contact details by the organization was lawful.
This requires a voluntary and unequivocal declaration of intent
of the persons concerned. These had been compared as part of a questionnaire

the organization made the following statement: “I consent to a
The self-help organization and the team of experts contact the scientific
scientific processing.”
This statement does not imply any unequivocal authority that the data also
disclosed to persons or entities outside the organization
may. Nor can the explanation of this meaning be taken from the context
be taken, because in the present case it was stated in the introduction to the questionnaire
explicitly that the data would not be passed on to third parties. the consent
The declaration of consent therefore only referred to contact by the organization
itself. This meant that the organization had no effective consent to the transfer of the
contact details to external institutions. Already the transfer of the data was
lily unlawful. We have received a warning from the organization because of this
pronounced. The organization responded to our speech and revised

the declaration of consent.

The transfer of personal data to third parties involves risks, since responsible

Literally giving control over the data out of hand and those affected

cannot understand to whom the data is passed on. If the

disclosure is based on consent, those responsible must check whether

the declaration of the consent of the persons concerned with the disclosure of their data

to third parties can actually be unequivocally inferred.

73

8 Employee data protection

8.1 Camera surveillance in the workplace

Employees can hardly avoid video surveillance at work,

which is why high demands are placed on the operation of such monitoring

are. Under no circumstances should there be a comprehensive control of the activities of the employees

come.

In principle, personal data of employees may only be processed

if this is absolutely necessary. For the legitimacy of surveillance

of workplaces using video cameras, special circumstances must exist, such as

e.g. a high risk for the property of the company. past thief

steel or attempted break-ins can be clues. But even then it is

Not every camera surveillance is allowed: In principle, no

Total surveillance can take place. In particular, the production

area where the work is mainly carried out, by means of cameras permanently

be monitored. Changing rooms, break rooms and toilets are also not allowed to be

be monitored.

In one case we examined, a company monitored the kitchen that

central production site, with a camera showing what was happening around

recorded the clock. The company was made aware of the ban, whereupon
the camera was switched off during the day and is now only used outside of the
times is active. In another case, although not the jobs themselves,
but with the corridors through which the offices of the employees could be reached
eight cameras filmed. The camera surveillance was justified with past
attempted burglary and property damage. It is also in cases like these
not sufficient if the company merely has the record by means
Video cameras informed. It must also be considered whether milder measures
can be implemented that serve the security interests of the company as well
satisfy. It would be e.g. B. to think about whether an alarm system
enough to ward off break-ins. In the present case, the eight cameras should

Monitor side entrance doors located at each end of each corridor.
As a result, it was actually not possible for the employees to watch the cameras during the
Avoid working hours because access to the workplace was directly monitored.
Here we recommended the positioning of the cameras as part of the investigation
and to reconsider their use. The company ultimately made its decision
for a new security concept that requires significantly fewer cameras,
whereupon most of the cameras were turned off and the cameras that were no longer needed
could be dismantled.
It should be noted that dummy cameras or deactivated cameras can also be an intrusion
can display in privacy. The jurisprudence is based on this
an associated pressure to monitor an intervention in the personality
Rights of the data subject.125 Even if the lack of data processing here
The scope of the General Data Protection Regulation (GDPR) is not open,

may take civil action against replica cameras or inactive cameras

ras may lead to elimination.

In principle, there must be extensive surveillance by means of cameras

be fully enlightened. A recording should usually be made after 72 hours

to be deleted. In companies that have a works or staff council,

whose consent to camera surveillance is required. It also has to

always be checked whether minor interference with the personal rights of the

employees adequately meet the security needs of the company.

Under civil law, even with deactivated cameras or dummy cameras,

claims for payment or injunctive relief exist.

8.2 Deletion of application documents

Applications for a job usually contain a lot of personal data.

Understandably, many applicants therefore ask for the completion of the

application process, a deletion of your data or the destruction of your

lay. If the application is withdrawn, the situation is simple: there is none

125

See Federal Court of Justice (BGH), judgment of March 16, 2010, VI ZR 176/09; District Court (LG) Berlin, judgment of August 14, 2018, 67 S 73/18.

Legal basis for further processing of the data, the application documents

are to be deleted immediately.

If the application is withdrawn, it is advisable to delete the data

to apply. There is a sample form on our website with the request

request to delete the personal data.126 It should be noted that the

responsible body has a period of one month to respond to the deletion request.

The situation is somewhat more complicated if the application is not withdrawn, but was rejected by the authority or the company. Applicants could appeal against the refusal. The authority or the company must then be given the opportunity to take legal action against such to defend a lawsuit. The application and also documentation of the application process including the evaluation. It applies to this a period of up to six months. This results from the relevant Appeal deadlines of the General Equal Treatment Act (AGG) and the Labor Court Act (ArbGG) and any delays caused by delivery a lawsuit.

In some cases, however, employers also have a much more extensive storage assurance intended: In a case examined by us, a company commissioned a recruiting agency to carry out the application process. That can in be generally in order within the framework of order processing. In this situation However, the agency required applicants to have an unlimited Agree to storing the documents for further application procedures, otherwise your application cannot be considered. An applicant then drew his application and lodged a complaint with us. The commissioning company parted with the agency very quickly due to our intervention, which unlawfully wanted to store employee data.

In another case before us, a complainant wondered why asked about a supposed salary requirement in an application process chen, which he had not transmitted. After acquaintances drew his attention to it

126 Available at https://www.datenschutz-berlin.de/buergerinnen-und-buerger/self-privacy/review-of-your-data.

had done that his address including phone number was published on the Internet

light, he got to the bottom of the matter: via the result display of several search

machines were his application documents on a company's website

fully visible, to which he had applied in 2019. The company

has the application documents after our intervention from its own web

site removed, but the data was cached by the search engines

still available for a while. In this context, it is helpful to know that the

Responsible body according to the case law of the Berlin Court of Appeal (KG) also for the

responsible for deleting the data still in the search engines

can be.127

If it is no longer necessary to store application data, these must

to be deleted. If applicants request deletion, it happens in practice

often cause problems because companies exceed the one-month deadline for responding to the deletion

exceed order. On the other hand, we receive many submissions in which the

Those affected have not waited for the one-month period that the company

answering the deletion request. Here we point out that the deadline

is to be awaited at first.

8.3 Need for a new employee data protection act

The social changes in connection with the increasing digital

talization also raise questions when dealing with employee data, which are

legislators must be answered.

A separate employee data protection law has been under discussion for decades.

kiss. The conference of the independent federal data protection supervisory authorities

and the countries (DSK) demanded a new one at the beginning of the year

Employee Data Protection Act repeated.128 The social change caused by the

Digitization influences the employment relationships in many respects and

127

128

See KG Berlin, judgment of November 27, 2009, 9 U 27/09.

DSK resolution of April 29, 2022: "It's time for an employee data protection law

is 'now'!', available at https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.

Vulnerabilities in the protection of employees' personal data. At

many of the problems currently arising are subject to legal uncertainty; open

In case of doubt, questions will not be interpreted in favor of the employees. problem

It is matic when employees, out of fear of professional disadvantages, violate

their right to informational self-determination during the employment relationship

assert. Notifications of violations often only reach us after the end of the

employment relationship and is therefore greatly delayed.

Of great practical importance for the protection of employee data is the

storage of work in the home office. However, this restructuring does not result in

that the need of the authorities and companies to control the work processes

decreases. Rather, we receive requests for advice, according to which the interest in over-

surveillance is so far-reaching that even a comprehensive inspection of workplaces in

the apartments of the employees is still considered appropriate. Also become

Not all employees are provided with separate devices for working in the home office

ment. It is not uncommon for people to work on private devices there, which is why not only

the database from the employment relationship, but possibly also the privacy of the

Workers beyond the employment relationship is affected, even if the

Employers are only checked on a digital level.

In the complaints we received from employees, the

Handling personal data on application portals on the Internet

role on which those affected had previously published their data. Also the one

rate of artificial intelligence is used in the placement of employment

will gain in importance in the future. This makes it possible to collect a large amount of data

to process the initiation of an employment relationship and personal assessments

to create forecasts, profiles, which may not be transparent or

are difficult to trace, resulting in potentially deep invasions of privacy

employees can lead.

Social change and digitization are posing the working world in general and

especially employee data protection faces major challenges. Here are

specific legal regulations in the form of a new employee data protection

required by law.

8.4 Particularly sensitive data in personnel files

In employment relationships, too, it applies that personal data that are particularly worthy of protection

related data may only be processed in narrowly defined exceptional cases.

This data includes information that can be used, for example, to draw conclusions about the health

security status or political convictions of employees or

points for religious defamation or racial persecution. Also

Information about trade union affiliations is subject to this special

Protection.129

Civil servants of the State of Berlin can, according to the Special Leave Ordinance (SUrlV) for

apply for vacation days for special purposes. Special occasions include: state

political, religious, professional, trade union and sporting purposes. After Bean

The documents are transferred to the State Administration Office (LVwA) for the special leave

attached to the personal file of the applicant. This allows personal

related data on religion, party or trade union affiliation input in

find the personnel file.

We had a complaint about this, which we took as an opportunity to increase the practice of the LVwA

check over. In fact, it was common for personnel files to be specially protected

enclose personal data in connection with special leave.

The processing of these special categories of personal data is only

narrow limits allowed. From the requirements of the SUrlV, after which special leave only

is to be granted in certain cases is determined during the examination of the application

although the necessity, in case of doubt, of data that is particularly worthy of protection

to process employees. However, it cannot be concluded from this that

this data may also be stored permanently in the personnel file.

Beyond checking the requirements for special leave, there are none

Legal basis for the storage of specially protected data in the

personnel file. As elsewhere in employee data protection, it must be checked here whether the

data processing is required.130 Due to the time limit of the special

vacation it is necessary to save the approval for the file in order to be traceable

129

130

Art. 9 Para. 1 GDPR.

Here according to § 14 Berlin Data Protection Act (BlnDSG) i. V. m. Art. 9 Para. 2 GDPR.

to determine the extent to which special leave has already been granted. not necessary

However, the justifications or evidence for the justification of the

respective special leave, on the basis of which conclusions can be drawn about the specially protected ones

data can be pulled.

In the course of our audit, the Senate Department for Finance, in its function as

Technical supervision for the LVwA announced, in future in connection with the

taking special leave does not contain any specially protected personal data

more to take over in the personnel files and a deletion concept for existing ones

to prepare files.

In the personnel file, information about the duration of the approved

reserved special leave are stored, but not information about the type

of vacation or the respective justification, provided that these conclusions can be drawn

specially protected personal data.

80

9 housing

9.1 Duplicate health data excess at the

Meeting of a homeowners association

A property management had for the meeting of an apartment owner

community laid out a list for the participants, which also included the vaccination status

should be specified. A participant photographed this list.

The contact protection measures introduced due to the pandemic

In many cases, restrictions also provided for attendance documentation. The

Infection Protection Measures Ordinance (today Basic Protection Measures Ordinance)

of the State of Berlin also contained restrictions on visiting public

locations or gatherings in larger groups for people who do not have sufficient

have been able to demonstrate vaccination protection against COVID-19.

The facilities, catering establishments and otherwise for the organization

responsible for gatherings of people trod different

Ways to document attendance. Purpose was in each case, a subsequent

To enable tracking of infections that may occur. For this reason

vation, a property manager decided to carry out a

Meeting of the homeowners association available list of parts

participants to a query field on the vaccination status of the participants

expand. It should be entered there whether and to what extent participants

vaccinated against COVID-19 infection. The participants came:in-

partly also after. One of the members photographed this list after the end of the

Assembly.

The processing of personal data by means of a list of participants

people is common at meetings of homeowners associations and

serves the purpose of proving who actually attended a meeting

and, if applicable, which voting rights exercised. Like many other data processing

within homeowners associations, such a purpose-bound

Documentation not objectionable. The data on the vaccination status is

but about health data. This data is not related to the

Carrying out the administrative order that the property management receives from the housing

owner community has received, or with the attendance documentation for

tracking infections. Their processing is also subject to special hurdles

because it is information about a person that is particularly worthy of protection.131

The query by the property management found no legal basis - neither

in law still in the Infection Protection Measures Ordinance - and was lacking

Consent of data subjects to the processing of their health data

unlawful.

Within a homeowners association, there are due to members

due to the close contractual relationship, comparatively far-reaching insight

rights into the documents of the community, which also contain information about the other

can give limbs. In this respect, there is often the transmission of copies of

Ownership share lists, statements or similar. a right of members to receive them

Information. Photographing a list of participants by one of the members

that of the community can also be justified. However, this only applies to the extent

the list only contains data that is necessary for the implementation of the contract

community of owners are required. This was with the one in question

list is not the case, so that photographing the list also involves data protection

constituted a serious violation. The acting property management and the member concerned

of the homeowners association were informed by us about the legal situation

and pointed out their wrongdoing. The deletion of the unlawfully collected or

photographed data was arranged.

Also extensive rights of inspection within the framework of close contractual commitments

Apartment owners' associations do not justify the query

of health data by a property management and certainly not the Ver-

processing of this data by a member of the community. unlawfully

The data obtained must be deleted immediately and this deletion is the responsibility of the person concerned

also to confirm.

131

See Art. 9 Para. 1 General Data Protection Regulation (GDPR).

Joining a homeowners association causes far-reaching

rights of other community members to view their own data. will be one

property management entrusted with the business of the community, it is a separate

permanent responsible body with all the corresponding rights and obligations.

Homeowners associations are contractual between the members

justified, often with the administration of the common property third parties

instructed. Many property management companies have even specialized in the management of residential

property on behalf of homeowners associations. the pro

Scriptures of the law on home ownership and permanent residence (WEG)

contain numerous regulations specifically geared to this type of housing.

First of all, every member has a broad right to insight into the company

were the other members. This follows primarily from the WAY: Within

of homeowners associations is to check their own accounts

Regular inspection of the documents of the other members is also required.132

This right of inspection also includes, for example, lists of participants in meetings of the

community, all billing documents relating to the community

matters or information about house money arrears of individual members. Over

the jointly concluded contract can also include further insight

rights are agreed.

With the advancing digitization, file inspections are shifting more and more

to the Internet, homeowners associations are no exception: portals,

through which the property management fulfills its information obligations with regard to the

community requirements online are widespread. That too

proactive provision of documents about the postal dispatch was already the subject

of inputs; both are fundamentally not objectionable in terms of data protection law.

This is how a property management company processes personal data from tenants

Owners on the basis of Art. 6 Para. 1 Sentence 1 lit. b GDPR. After this may

those data are processed that are required to fulfill, for example, a rental contract or

132

See § 28 WAY.

of a contract of homeowners associations are required. operator:in-

Creation of portals for administration and communication with the residents of the

managed apartments are contract processors for the respective house processing

to involve administration. The digital provision or the postal dispatch

of lists and bills do not contain any further information

encroached on the rights of the persons concerned, than anyway through the right of inspection

of the other members of the community provided by law, provided the

necessary technical and organizational measures to protect the data

complied with.

Members of homeowners associations, on the other hand, have no entitlement

to the receipt of personal data of the other members, if not hereby

the fulfillment of the contract of the community is intended. For example, if not in the contract

it is explicitly stated that e-mail addresses from people who are not in the house

administration or the community advisory board, may be used

the other members also have no right to receive the e-mail addresses.

Advisory board members are also only allowed to use the addresses to fulfill their tasks

use within this committee. The same applies, for example, to the telephone numbers of others

members; there is no right to communicate with any members outside

the bodies provided for by law and contract.

It is often underestimated how far the obligation to disclose one's own

usage or billing data within a homeowners association

shank is enough. The use of online portals for the management of residential property

is generally not objectionable if the required data security

is guaranteed.

84

10 economy

10.1 User-friendly data disclosure:

Please complete and understandable!

We are regularly contacted by people whose requests for information are incomplete

or were answered incomprehensibly. The right to data information is that

The heart of the rights of data subjects: the information should allow data subjects to

be put in a position to understand the processing of the data concerning them

and to be able to check the legality of the data processing.133

The right to data information is also of central importance because it

enables the targeted exercise of other data subject rights, such as the right to

Correction or deletion of the data.134 It is all the more important that the data

future is granted in full and at the same time precise, transparent, understandable and easy

is accessible.

Complete information does not only contain the master data from the customer

database, i.e. name, address data and date of birth, but everything about the person

stored data, such as u. Order history, credit ratings, log-in, click and

browser data or communication with the data subject. Over and beyond

the data subject must be given further information (so-called meta information),

so e.g. B. where the data came from, who it was shared with or for how long

they are stored.135 If individual points are not relevant in the specific case

because the data has not been passed on, for example, the persons responsible may

not simply remain silent about it, but must provide appropriate negative information

grant.136 Otherwise, the data subject would not be able to tell whether it was actually

no corresponding data processing took place or the data information only

is incomplete.

133

134

135

136

See Recital (EC) 63 General Data Protection Regulation (GDPR).

See Art. 16, 17 GDPR.

See Art. 15 (1) lit. a to h GDPR; Art. 15 para. 2 GDPR.

For example in the form of: "Your data has not been passed on."

When providing data information, some companies simply refer to the

Statements in their data protection declaration. Such a reference can be the individual

However, it is not a substitute for information. While fulfilling the privacy policy

serves general information requirements before data processing,137 the

Information in the case of a request for information tailored to the data subjects

be. The unchanged adoption of text parts from the data protection declaration in

data information is only possible if the information remains the same,

such as with regard to the right of appeal to a supervisory authority

Case is.138

A data disclosure is more precise, transparent, understandable and easily accessible

form in clear and plain language.139 For controllers who

process a large amount of personal data, this is not always easy to implement.

Zen. In the case of a confusingly large amount of data, those responsible can

proceed in stages, d. H. first the relevant for their average addressee

communicate the data and at the same time inquire about the level of detail in the content of the

further data is desired. However, this form of information is not permitted

lead to a restriction or aggravation of the right to information.

If the data disclosure contains internal abbreviations or codes, it can be difficult

be to understand this. Here, those responsible must at least provide additional information

provide information. However, these must not lead to the affected

person has to do tedious translation work to get the data information

to understand and verify. The visual form is also part of comprehensibility

the presentation of a data report. With a responsible person checked by us

could the information in the data report be due to the selected presentation

wise with many table columns and a minimum font size neither digitally nor

Can still be printed out in the regular DIN A4 format when considered legible as a whole. In

this case we were able to convince the company to form an alternative

to choose the representation.

137

138

139

See Art. 13 or Art. 14 GDPR.

See Article 15(1)(f) GDPR.

Art. 12 para. 1 sentence 1 GDPR.

Data information must be complete and understandable for the person concerned

be processed. The European Data Protection Board (EDPB) has

draft guidelines on the right of access, which will be published after their finalization

offer additional clarity for companies and those affected.140

10.2 Objection of abuse of rights

request for information

Some companies refuse to provide information to affected persons

sons. They argue that there is no obligation to provide information and

Data copies, e.g. in the form of telephone recordings, exist if the

affected person with the assertion of their right to information data protection

pursue foreign purposes. We received several complaints in which companies

asserted the objection of abusive behavior 141 and

have brought that information need not be provided.

In a case before us, there was between one complainant and one

Undertake a dispute as to whether a contract agreed by telephone is valid

came about or was terminated. The complainant did that

Right to information against the company and demanded in this

connection also the delivery of a copy of the telephone recording. The

Company refused the complainant the relevant information and

stated that with the request for information, they are pursuing non-data protection purposes

would. She just wanted evidence of a civil dispute

to back up.

The Federal Court of Justice has the scope of the right to information under the GDPR

(BGH) submitted questions to the European Court of Justice (ECJ).142 The BGH doubts

that the tracking of other than data associated with the request for information

140

141

142

See EDPB Guidance 01/2022 of 18 January 2022: "On Data Subject Rights - Right

of Access (Version 1.0)", available at https://edpb.europa.eu/our-work-tools/documents/

public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

Art. 12 (5) sentence 2 lit. b GDPR.

See BGH, decision of March 29, 2022, VI ZR 1352/20.

protective purposes automatically to an exclusion of the right to information

leads.143 According to the wording of the GDPR 144, the existence of the right to information is not

linked to the motivation of the person concerned, so the

future requests are also not justified. This indicates that the Union

legislature basically wanted to leave it up to the person concerned whether and off

the reasons for the request for information. Therefore, should not solely due

the fact that a request for information on the transmission of a copy of the data

non-data protection reasons, it can be concluded that this

manifestly unfounded or excessive 145.146

Taking into account these views of the Federal Court of Justice, in our case there was nothing obvious

unfounded or excessive request. Neither was the request for information frequent

repeated, there were other reasons for abusive behavior.

An intention to damage on the part of the complainant was not recognizable in the present case.

bar. We have the company with reference to the referral order of the BGH

informed that the information is to be given to the complainant and

There is a right to the transmission of a copy of the data.

Those responsible are obliged to provide data subjects with the desired information

grant and to transmit data copies, such as telephone recordings. On off-

future request cannot be made with the objection that it serves non-data protection purposes,

be denied unless a manifestly unfounded or excessive request

or improper conduct.

143

144

145

146

Ibid., No. 16 et seq.

See Art. 15 GDPR.

I.S.v. Art. 12 para. 5 sentence 2 GDPR.

See BGH, decision of March 29, 2022, VI ZR 1352/20, para. 18.

10.3 I want to know! Information obligations at Data retrieval from the commercial register

Again and again we receive complaints from people who use their personal data

Data surprisingly reproduced in commercially operated public platforms-

find. The commercial register often turns out to be the source of the data. Purchase-

people and commercial companies are required to include certain information in the

to be entered in the commercial register. This also applies to personal data

natural persons, such as the date of birth or the private address of

Company founders. The entries in the commercial register are - since August of this year -

res free of charge - publicly visible on the Internet.147 Commercial platforms are taking hold

the data and use them for their own purposes. In none of the cases known to us

The persons concerned were informed about this by the platform operators

informed.

Whether a data retrieval from the commercial register for the purpose of commercial publication

publication on another portal is lawful, within the framework of an interest

on the one hand, it must be taken into account that the data on

must be published in the commercial register on the basis of legal regulations.

With every further publication there is a risk that the data will be uncontrolled

reproducible and can thus also be falsified. On the other hand acts

This is data that is already publicly accessible via the commercial register, d. H.

a retrieval is generally not limited to specific purposes. The processing

in some portals, it also serves to provide transparency about possible interdependencies

Company. The balancing of interests must therefore be carried out in each individual case.

It is also crucial whether those responsible can ensure that the

data was accepted without falsification and is also kept up-to-date in the long term.

On the other hand, the obligation of those responsible is regularly non-negotiable

data subjects about the collection and the planned publication of their personal

personal data.149 Those responsible come to this information

tion obligations towards the persons concerned are often not fulfilled, but instead called upon

147

148

149

See 3.2.

See Art. 6 (1) sentence 1 lit. f GDPR.

See Art. 14 GDPR.

refers to the exception of the "disproportionate effort".150 For this

etc. pointed out to the large number of people to be informed or in case

address data that is only available by post, also ensure that the information is sent by post

more cumbersome and more expensive than email. The burden of proof for the disproportionate
The amount of effort lies with those responsible. These must present their processes
set and explain why the effort for the notifications versus the
Gaining knowledge among those affected would not be proportionate. The aspect that
sending by post is more complex and expensive than sending by e-mail,
cannot be asserted. For the calculation of the effort for your information
information obligations, those responsible cannot rely on the most favorable option for them.
ness as a presumed normal case. In addition, data collection and
Data processing within the framework of such a business model is digital, so that a
collective postal mailings also to a large number of addresses on a regular basis
is possible without much effort.
Anyone who chooses the business model of publishing mass data must
also fulfill the resulting obligations. Such a company can
generally do not refer to the exception of disproportionate effort.
Against the application of the exemption to such commercial processing
The rule examples listed, the processing purposes, also speak for processing purposes
subject to public interest. Ultimately, the decisive
facilitating data subjects' control over their personal data:
If the operators of platforms do not notify the persons concerned
, they do not learn about the dissemination of their personal
gene data. They are also denied the opportunity to exercise their rights
in particular the right to information, objection and deletion, against the Ver-
exercise responsibly.
The retrieval of personal data from the commercial register by commercial
platforms may be lawful in individual cases. The people concerned are
to be informed about this on a regular basis.

150

Article 14(5)(b) GDPR.

10.4 Attention online trade: guest orders must be offered as a matter of principle!

The conference of the independent data protection supervisory authorities of the federal and of the federal states (DSK), with its decision of March 24 of this year, has information on published data protection-compliant online trade via guest access.151 Core What the decision says is that controllers who sell goods or services in Offer online trade, their customers basically a guest access for the Must provide order, regardless of whether they also next to them provide a customer account. The background is that those responsible do not per se can assume that customers in any case have a continuous Wanting to have a customer account is a conscious declaration of intent necessary.

So far, it has been common practice in online retail that setting up a customer account was required in order to place an order. These customer accounts can be used to simplify new orders from the same online shop.

An order history can also often be viewed in the account. Over and beyond However, online shops often also use the data stored in the account for profile education and for promotional purposes.

The principle of data minimization applies in data protection law.152 This means that that the data processing - also in online trade - is based on the purposes of Processing must be limited to the extent necessary. Does the data processing take place? for the performance of a contract,153 the processing must be limited to what is

Fulfillment of the contract or contract processing is necessary, whereby the term of the

is to be interpreted narrowly.154 The establishment of a customer account and the

The associated further data processing is regular for the fulfillment of the contract

not mandatory. As a rule, a company may therefore only open an account

151

152

153

154

Resolution of the DSK of March 24, 2022: "Privacy-compliant online trade using

Guest access", available at https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.

Article 5(1)(c) GDPR.

Art. 6 (1) sentence 1 lit. b GDPR.

See EG 39 sentence 9 GDPR.

directed if the data subject effectively, i.e. in particular voluntarily and informed,

agrees.155

In order for the criterion of voluntariness to be guaranteed, the fulfillment of a contract

not linked to a request for consent to data processing

the one that is not required for the fulfillment of the contract.156 From the voluntary nature of the

Consent to setting up a customer account cannot be assumed,

if the customer has no possibility of a guest order or no equivalent

Order option is offered. An order option is then to be regarded as equivalent

hen if it does not entail any disadvantages for the customers, i.e. in particular

Order effort and access to these options of ordering with a customer account

are equivalent to. Fortunately, more and more companies are offering nationwide and also in Berlin

accept their customers the alternative in the form of a guest access.

If personal data from the customer account is used for advertising purposes

should be evaluated or processed, companies should also note that

that your own consent related to these purposes must be obtained. Advertising

represents data processing that goes beyond the mere establishment and management of a

continuous customer account and from the relevant consent

is not covered.

10.5 Secure Authentication

In a data breach report we received, a company informed us that

that his employees' passwords were disclosed in plain text, which they used to log in

tion to the company's IT systems, which also used personal data

data are processed.

Anyone who processes personal data must ensure that only legitimate

people can access the data. The prerequisite for this is that this person

identify them to the systems and services. The process for this is called

155

156

Article 6 paragraph 1 sentence 1 lit. a GDPR i. In conjunction with Art. 4 No. 11, Art. 7 GDPR.

See Art. 7 Para. 4 GDPR.

Authentication.157 Classically, this is done by entering a user name and

a password. The password may only be known to the person using it.

Protection is no longer guaranteed if passwords are known to other people

become. An essential protective measure is therefore, among other things, passwords not in plain text

save. A check of the correct input by the registering

person is also possible in another way: a cryptographic procedure can be used for this.

contact, which clearly derives a value from each password, which instead of the password

is saved. The method is chosen so that it is complex, from the

derived value back to the password.

Part of the calculation should be outsourced to the device that is itself

registering person uses. In this way, the password is not transmitted in plain text via the

binding sent to the server. This is extra protection in case the

Encryption of the connection, which is of course still necessary, fails or a

gives another person access to the IT system that receives user input

for their authentication. This IT system is often necessary

accessible via the Internet and is therefore particularly at risk. The review of

Users should be reserved for another IT system that itself is in front of a

direct access from the Internet is protected. This eliminates some weaknesses of the

Authentication with passwords weakened. In particular, the probability

significantly reduced that incidents - such as the data breach mentioned at the beginning -

unpleasant consequences for the users and those people whose

data are processed.

Nevertheless, residual risks remain. Safer procedures are available and cause

generally no great effort. They are based on the person posing as

legitimately wants to identify owns a device (such as a smartphone) that has a

complex cryptographic secret.158 This secret remains

finally in the device and is used to, at the request of the server,

157

158

The terms "authentication" and "authentication" are commonly used in language

use often used synonymously, but describe different sub-processes

Registration process: Users “authenticate” themselves on a system using

clear login information (such as a password or chip card). The system

then checks the validity of the data used, it "authenticates" the

users. See https://www.bsi.bund.de/dok/ 11693908.

A common procedure is described in the FIDO2 standard.

those responsible to carry out a calculation, the result of which can only be obtained with knowledge of the

secret can be determined, but which can also be determined by the server without this secret

nothing can be checked. Therefore, companies must check whether such a suitable

wordless authentication procedure under the circumstances of the specific processing

can be implemented and the effort required for this, taking into account the risk, is

authorized knowledge of password data within a reasonable framework. Are

Given these two factors, purely password-based authentication is not

more allowed.

Anyone who processes personal data must ensure that only legitimate

people can access the data. Verification of authorization with

Username and password are no longer state-of-the-art. who that

method still uses because alternatives cannot be implemented, must

prevent passwords from being stored in plain text. Preferable

and possibly mandatory are passwordless procedures.

10.6 Help, my customer account was hacked!

What to do against identity theft and Account takeover?

Identity abuse in online trading is a major annoyance for those affected

Persons. Again this year we have some complaints about this

topic received. The good news is that affected people are taking action themselves

to protect themselves against identity abuse. But also the companies

are obliged to take measures to protect their customers.

This year, the unauthorized takeover of existing customer

accounts are increasingly the subject of complaints procedures. The acquisition of a customer

denkonto by unauthorized third parties, also known as account takeover, typically takes place

wisely using the actual log-in data that the owner

of the affected customer account.159 Behind the account takeover

often so-called credential stuffing. This is a cyber attack method

159

This usually means email address or user name and password.

in the case of access data, in the case of other data breaches or data breaches

skimmed off can be automatically tried out with other services. The

Attack method is based on the fact that many users of online services use the same

Use access data (credentials) for several services. speculate on it

the attackers - unfortunately often with success. Attackers can use lists with

acquire a number of log-in data, e.g. in the Darknet. The access data can be from a

individual, but also from different sources. Contrary to the usual

Expectations are that the passwords don't have to be bad or weak, even as

strongly valid access data can be affected if they are used in a previous

past data breach were disclosed.

For the account holders concerned, the takeover of their customer account is included

associated with unpleasant consequences. Not only can the data stored in the account

can be viewed, e.g. the address, the date of birth or the purchase history.

In some cases processed by us, the e-mail address stored in the account could

address can be changed using the log-in data, so that the account holders

no longer have access to their account. If there is also a goods

order, for the account holder: inside mostly an intensive correspondence with

necessary for the company to clarify the facts and possible purchase

fend off price claims. Was the information stored in the customer account before the order

exchanged e-mail addresses, there is also the fact that the account holders may only

found out about the order with a considerable time delay, because any

sent order confirmations were sent to the newly stored e-mail address.

Companies are required to do this, taking into account various factors

such as the state of the art, the cost of implementation and the severity of the risk

appropriate technical and organizational measures for data subjects

take to ensure the security of processing and against the

to prevent data processing that violates the GDPR.160 A measure to

To thwart dental stuffing is to contribute to the use of passwords

to refrain from authentication and instead to use cryptographic

160

See Art. 32 GDPR; see also the orientation guide of the DSK of March 29, 2019:

"Requirements for providers of online services to secure access", available at

https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.

key to set 161 or, in addition to using a password, authentication

tion with a second factor. Attackers are gaining with the currently

common attack methods usually only passwords, but not the crypto

graphical key of the users: inside or other (second) factors.162 Second

factor is usually the possession of a device that has a letter that is only valid for a short
displays a username or number combination that customers use in addition to their password
indicate. The combination is either generated on the device or by
the company via a separate transmission path to the device and thus
transmitted to the customers, whereby the production takes place on a specially prepared
standing device is preferable.
At least for data processing with a high risk, such as online
banking, two-factor authentication is not just a recommendation, but
Achieving an appropriate level of protection is necessary. In the area of conventional
chen online shopping, two-factor authentication is not yet customary in the industry,
Username or e-mail address and password are usually sufficient to log in. Comes
when it comes to credential stuffing, companies can take over the account as such
difficult to prevent. When logging into customer accounts using the
actual access data, companies can usually not recognize
whether the log-in by the real account holders or by unauthorized persons
he follows. A higher total volume of login attempts can be a problem for companies
be an indication of credential stuffing, but even if an increased login volume
is detected, companies find it difficult to stop an attack without the
Registration process as a whole, d. H. for all customers.
Therefore, companies must check whether a passwordless or two-factor authentication
tization procedure can be implemented under the circumstances of the specific processing
and the effort for this, taking into account the consequential risks, becomes unjustified
Keeps registrations within reasonable limits. If these two factors are present,
then a purely password-based authentication is no longer permissible.163 Above
In addition, companies must take action to make the impact more successful
Contain attacks on data subjects. In this respect, companies have to check

161

162

163

See 10.5.

For two-factor authentication see also https://www.bsi.bund.de/dok/11693908.

See 10.5.

which measures are suitable and appropriate in the specific case, in order to

avert damage. For example, the blocking of a (presumably) affected customer

denkontos represent an effective measure. Regardless of whether it exists

obligation to notify after an attack164, companies should

also notify customers about important events in the customer account

For example, changing the e-mail address stored in the customer account counts.165 It stays

However, there is a risk that customers will not receive notification emails, for example

because of an overflowing inbox, or they do not read the e-mail or do not read it immediately

and therefore not react immediately. Whether a notification by itself

is already a sufficient protective measure, must therefore be checked in each individual case.

If orders can be placed via the customer account, which

no further interaction on the part of the customer to initiate a payment

obligation should require the change of e-mail address from the confirmation

be made dependent on the account holder. This can e.g. B. by sending

a confirmation link to the email address originally stored in the customer account

take place. In this way it can be ensured that the change of the e-mail

address is made by the actual account holders. Also become

any order confirmations sent by e-mail to the actual account information

haber:innen dispatched, which in turn means that in the case of an order an immediate

intervention enabled. This measure only fails where the attackers also

have the access data for the e-mail account.

The good news is that account holders are at risk of attacks like credential

tial stuffing can be reduced by preventing multiple use of passwords

consistently avoid. We therefore strongly recommend account holders for

create a separate, sufficiently long password for each service. For the usable

We recommend using a secure password manager. Besides that

account holders should do this wherever possible, but especially

for accounts that are particularly worthy of protection, such as e-mail accounts or customer accounts

Activate online shops, passwordless or two-factor authentication.

164

165

Art. 34 GDPR.

See also point 2.5 of the DSK guidance of March 29, 2019: “Requirements

to providers of online services for access security”, available at

https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.

10.7 Publication of signatures on the Website of a public company

A shareholder complained to our authority about the complete publication

ing of his handwritten counter-motions to the Annual General Meeting including

his signature on a public company's website.

According to the GDPR, personal data must be processed lawfully

works.166 Personal data is any information relating to a

identified or identifiable natural person.167 This also includes the

signature of a person. The processing of the data is u. a. lawfully when they go to

Fulfillment of a legal obligation is required, which the responsible

body.168 It must be proportionate and relevant to its purpose and

limited to what is necessary.169 Personal data should therefore

only be collected and processed to the extent necessary to achieve the purposes

is necessary for the data processing and with regard to the purpose of the processing

has relevance. In addition, personal data should only be processed

if the purpose of the processing cannot be reasonably attributed to other, milder,

the informational self-determination right of the persons concerned is less

medium can be achieved.

According to the German Stock Corporation Act (AktG), the board of directors of a stock corporation

obliged to make motions from shareholders accessible.170 The subject of this

These so-called disclosure requirements are in addition to the justification for the application and any

Opinion of the management of the joint-stock company but only the names of

Shareholders including their first names, but not their signatures. That is

texts sent by shareholders can be made available in scanned form for retrieval

being held. However, if counter-motions exceed the statutory mandatory information

contain additional personal data, these are unrecognizable in each case

close.

166

167

168

169

170

Article 5(1)(a) GDPR.

Art. 4 No. 1 GDPR.

Article 6 (1) sentence 1 lit. c GDPR.

Article 5(1)(c) GDPR.

See Section 126 (1) Sentence 1 AktG.

In the present case, the original signature of the shareholder was published

on his counter-motions to the general meeting of the stock corporation by a

are not required on their website to fulfill the aforementioned disclosure requirements.

dumb. His signature could have been blacked out. Likewise would be

a copy of his countermotions and their disclosure limited to

the legally prescribed content of the responsible body possible and also

been reasonable. We have the established violation of the law by the joint-stock company

sanctioned with a warning.

The publication of the original signatures of shareholders on countermotions

to the general meeting of a stock corporation is not required and violates

thus against the GDPR.

10.8 Old bank statements and the right to information

One complainant had asked his bank to submit the transaction data free of charge

nes credit card account from the years 2010 to 2016 as part of a data protection

legal request for information. The bank initially rejected this by reference

to the archiving function in the online account management area and referred to

Query from the complainant, who does not archive the bank statements in question

had, on a provision in their general terms and conditions. She offered that

Complainant to send him a copy of his bank statements against payment

payment of a specific fee.

According to the District Court (AG) Bonn, bank customers have a right to their

Bank has a data protection right to information 171 about all account

movements in their bank account. The bank fulfills the customer's right to information

but not yet if it only provides the account statements. With it

only their obligations under the payment service contract have been fulfilled. The data disclosure

should primarily be the legality control with regard to the processing of

personal data,172 enable the pursuit of a

the purpose or for another purpose (e.g. the preparation of court proceedings

171

172

Art. 15 para. 1 GDPR.

See EG 63 sentence 1 GDPR.

or strengthening one's own position vis-à-vis third parties) does not justify it

the objection of abuse of rights.173

The right to information under the GDPR includes all data that is held by those responsible

available. An exception for only part of the data is not provided for.174

The scope of the right to information is therefore the data stock at the time

of the request for information. The person concerned always has one

Right to complete and correct information about the specific

worked data. The EDPB guidelines on the right to information under Art. 15 GDPR

provide that the notion of copy applies solely to those information

refers, which are to be granted according to the provisions of the GDPR.175 These give the

responsible bodies a leeway as to how the information is to be provided in a specific individual case

most expedient can be implemented. In this respect, there is for data subjects

no blanket claim to the sending of a complete copy of the account statement.

Nevertheless, there is a right to complete information. In practice, the

In many cases, the simplest way to obtain a right to the future is to list the sales (accounting

gen) of the respective account. We are talking to the responsible bank

pointed out in order to use a modified and data protection-compliant website in the future

contribute to the information process.

Banking institutions are obliged to inform data subjects as part of an information

requires at least the transaction data of a bank account to be made available free of charge

deliver.

173

174

175

See AG Bonn, judgment of July 30, 2020, 118 C 315/19, para. 33 sentences 3, 4 and 5, available at https://openjur.de/u/2271642.html.

See Art. 15 GDPR.

See EDPB Guidance 01/2022 of 18 January 2022: "On Data Subject Rights - Right of Access (Version 1.0)", paragraphs 22 and 23, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en (in the consultation process).

10.9 No abuse of rights when requesting information for the preparation of civil proceedings

An insurance company refused to provide information under data protection law

to fulfill a data subject's claim because, in their opinion, they

Information abusive to prepare a claim against the insurance

pending civil process.

The GDPR enables responsible bodies to take action against the abusive

to defend the exercise of data subject rights such as the right to information.176 In doing so

two case constellations can be distinguished in which there was abuse

gene: On the one hand, there is a case of abuse that is obviously unfounded

application.177 However, unfounded applications usually only require

a negative response,178 which usually does not give the responsible

effort required. A case of abuse in such case constellations is therefore

only if the processing of the application is far above average

would require effort, although its unsuccessfulness a priori unquestionable

fixed. On the other hand, a case of abuse in the case of an excessive application

are available.179 An application is not excessive simply because it has a high

Processing effort triggers at the responsible departments. Rather, it is required

abusive behavior on the part of the applicant. For interpretation

the aim behind the respective law is important.180

The guidelines of the EDPB on the right to information according to Art. 15 GDPR see a relevant

speaking stipulation that motives of data subjects to assert

of data protection requests for information in principle for responsible bodies

are not queryable and also the intention to use the information received

176

177

178

179

180

See Art. 12 Para. 5 Sentence 2 GDPR.

See Art. 12 Para. 5 Sentence 2 Alt. 1 GDPR.

Art. 12 para. 4 GDPR.

See Art. 12 Para. 5 Sentence 2 Alt. 2 GDPR.

For example, in the case of the right to information in accordance with EG 63 sentence 1 GDPR: "A data subject should

a right to information regarding the personal data concerning you that has been collected

have been granted and have this right without issue and at reasonable intervals

can perceive to be aware of the processing and its lawfulness

to be able to check."

to assert legal claims against the responsible body

use, does not represent an abusive exercise by data subjects.181

Motives of data subjects to assert data protection laws

Requests for information cannot be queried by the responsible bodies. information

requirements are to be met, regardless of whether they are also used to prepare for

civil lawsuits against the responsible authorities.

10.10 Pseudonymization for data export

A trading company approached us with a request for an assessment of a

Procedure that should enable him to transfer data to his customers without risks

Processing to export to the USA. According to the ECJ, the USA offers

no adequate protection of personal rights in the processing of personal

related data. Unfortunately, the proposed solution proved to be unsustainable.

In 2020, the ECJ found that the US did not have an adequate level of

protection of personal data.182 This is primarily due to the

opportunities for US authorities to access data processed there,

without data subjects having sufficient legal remedies against it

stand. The EDPB reacted to this judgment with recommendations with which additional

Any measures of a legal and technical nature nevertheless provide sufficient protection

be guaranteed for data exports to an insecure third country such as the USA

183 One of the recommended means is to pseudonymise the data

before their export.

181

182

183

See EDPB Guidance 01/2022 of 18 January 2022: "On Data Subject Rights - Right

of Access (Version 1.0)", paragraphs 13 and 187, available at https://edpb.europa.eu/

our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-

rights-right_en (in the consultation process); see also 10.2.

See CJEU, judgment of 16 July 2020, C-311/18 ("Schrems II"); see JB for details

2020, 1.2.

EDPB Recommendations 01/2020 of 18 July 2021: "Measures to supplement

Transmission tools to ensure the level of protection under Union law for personal

related data (version 2.0)", available at https://edpb.europa.eu/our-work-tools/

our-documents/recommendations/recommendations-012020-measures-supplement

-transfer_de.

Pseudonymisation changes personal data in such a way that

they are no longer individual persons without consulting additional information

can be assigned.184 This assumes that everything from the original

data must be removed, which uniquely identifies the person. play at it

initially clearly identifying information such as the name of the person, their birth

date or your address matter. This is also what the trading company intended,

who contacted us. It wanted a service provider to handle the

use transactions of his online shop. This service provider is based in

USA and mainly processes the data entrusted to him there.

On the way from the customer via the online shop to the service provider, the

Data are changed in such a way that the customers are neither for the service provider nor for

Authorities who could have requested the delivery of the service provider's data,

are recognizable.

Here are the ways the US authorities to detect

Persons in databases are available and from which are suspected

that they are actually used should not be underestimated. It is not

unlikely that the strategy of some of these authorities is to get data

from many sources initially in stock and, if necessary, to combine

net. For example, the data streams that come from payment processes come into consideration

come. Many payment service providers are based in the USA. The ones of them

processed data are subject to access by US authorities. Also the

Society for Worldwide Interbank Financial Telecommunication (SWIFT) based in Bel-

gien, which handles a particularly large number of transactions worldwide, is to issue

Committed to data.185 Trades that are paid for electronically, such as those from

the business of the company we advise, can be

signed transactions and thus the identity of at least part of the

Uncover customers.

In its recommendations, the EDPB therefore stipulates that none of the

additional information related to the assignment of pseudonymised data

184

185

See Art. 4 No. 5 GDPR.

In relation to data processed by SWIFT in the European Union (EU).

the request for data is regulated by an agreement between the EU and the USA,

see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22010A0727(01).

may serve individuals, may be available in the country to which they go

be exported. Otherwise there would be no effective protection for the data. We

The measure planned by the company therefore had to be considered insufficient

deny.

To export data to a country that does not have sufficient protection of personal

rights, far-reaching technical measures are necessary that

Prevent misuse of exported data. Pseudonymization can do this.

However, all possibilities must be considered, pseudonymised data

reassign to individuals.

10.11 Apps and Web Services Data Breaches

A not inconsiderable proportion of the data breaches reported to us is due to

ensure that data protection and IT security are not already in the design phase

Apps and web applications are consistently considered.

When people interact with mobile applications (apps) and web applications,

a large amount of personal data is generated, e.g. Data on the type and

way of using the application as well as personal, sometimes particularly sensitive

valuable data that is stored in the application. If users register at

must identify themselves to the application when registering, is used as a user

name often uses your own email address. Vulnerabilities can these

Disclosing data, with sometimes annoying, sometimes downright unpleasant consequences for

the affected. Therefore, the operators are obliged to use the applications and

design the underlying services securely. Breakdowns are to the competent

to report to the data protection supervisory authority. In the case of high risks for those affected

these are also informed. It's best if it doesn't even have to be such

data breach is coming.

Nevertheless, we often receive reports of security gaps, be it from companies

themselves, be it because security researchers have found vulnerabilities.

The reported vulnerabilities mostly affect one of the typical classes of

Vulnerabilities identified by the Open Web Application Security Project (OWASP), a

non-profit foundation dedicated to improving software security

uses, regularly in a list of the most common and riskiest vulnerabilities

be listed.186 The list published in 2021 contains for the first time the

elongated access control in the first place. What is meant by this is that for certain

Access to data actually involves identification and authentication of the query

which would have to take place, but this either does not take place at all or fails, so that

data to be protected is delivered to unauthorized persons. Also in ours

work, these cases, in addition to attacks by malware, make a significant

proportion of security incidents that have serious consequences for a large

Number of people affected may have.

In various cases that have become known to us, for example, communication

a smartphone app with the associated server systems is not sufficient

secured. The assessment of the developers was apparently: Since the

App comes from us and only this one speaks with the servers, it is sufficient to

to encrypt the connection. A check of the admissibility of the respective query

then only took place to a limited extent, because it was assumed that their own app

would only make legitimate inquiries. Inquiries from other sources fell completely

out of sight. This view is wrong: the application can also contain errors

ten and enable the query of such data, to which the respective user

shouldn't really have access. In addition, there is also the more serious

Possibility for third parties to use the communication interface without the application

and contact the server directly. Encryption only helps to a limited extent here.

It makes it difficult to determine how and via which interfaces

the application interacts with the servers of the background system. Yes she can

usually easily bypassed if the attackers control the end system,

on which the application is running. It is therefore only a matter of time before it is known which

accepts and executes commands from the server via the application interface,

without verifying the entitlement of the requester. Personal

Genetic data are disclosed. By skilfully varying the queries,

also often maximize the data yield.

186

See https://owasp.org.

105

Chapter 10 Economics

Specific data breaches based on the problem described included:

the following incidents:

• The server interface of a campaign support app 187 not only gave how

provided the top 15 election officials in an area from, but as many as

were requested. Since far more data is available per dataset than necessary

were completed, extensive data of all election workers could be viewed.

In a vulnerability that arose later, all the data of the

call street campaign. The anonymity of the persons concerned was

so insufficient that at least in individual cases their identification is possible

could be.

• A pharmacy delivery service enabled its ordering app via the interface

used, the retrieval of the entire order data of all customers.

• A practice management software supplied a list of those being looked after via the interface

practices. The data records contained access data to other systems. patient

data from other patients including invoices and laboratory results

and call up sick notes, since only the basic access authorization

was checked, but not whether it was based on data from your own or someone else's account

was accessed.

Other data breaches were based on access keys to interfaces from

other services (e.g. for sending e-mails) in the program code of a website

placed goods that could be called up unprotected by third parties. Such mishaps

ten, for example, in an application for posting and sending results for Corona express

test centers and a web shop.

Frequently occurring errors in web applications are also insufficiently

secure links used to retrieve invoices, order confirmations or corona

Test results 188 can be used. There are often ongoing customer or order

numbers that can be changed in an existing link to the respective

Retrieve other people's documents. A safe implementation would det

187

188

See JB 2021, 15.1.

See JB 2021, 1.4.

output the corresponding document only if further checks are successful

fen. Possible conditions may be that the person concerned is in the

Application to be logged in or other parameters identifying the document

must state, which is not known to third parties and cannot be guessed.

If we are informed of security gaps such as those described, we will contact you

us immediately to the company responsible and request that they be removed

the vulnerability. We request more information to assess whether

the measures taken are sufficient to make data processing more secure in the future

design. If the person responsible can be proven to have breached their obligations,

can also result in sanctions.

Anyone who operates apps and web applications must ensure the security of the

worked data worries. To find vulnerabilities, application and

underlying server services are examined in detail for vulnerabilities.

Protection measures that work independently of the specific application - how

e.g. B. Encryption, firewalls, proxy servers or automated investigations of

Source codes for more formal errors - are not enough.

11 Transport and Tourism

11.1 Tesla's Sentinel Mode

This year we received a large number of complaints in relation to the so-called

Get Sentry Mode, which Tesla has available in its vehicles

puts. We also get press inquiries about this topic again and again.

Since Tesla moved its German headquarters from Bavaria to Ber-

lin, we are the data protection supervisory authority for Germany within Germany

responsible for receiving complaints against the processing

personal data by Tesla for its own purposes. The pan-European

However, Tesla's main office is in the Netherlands. Therefore enough

the complaints we receive against Tesla within the framework of the European

Cooperation procedure 189 to the competent Dutch supervisory authority

processing continue.

However, the majority of the complaints we receive have not changed

directed against the company Tesla itself, but against the

testify built-in guard mode, with which the environment video technically

can be monitored. Was Sentinel Mode enabled in its previous form

several cameras continuously record what is happening around the vehicle. The

Recordings were only overwritten after an hour. Then realized that

vehicle a threat, the last ten minutes of recording were continuously

stored on a USB stick if it was connected to the vehicle.

In the event of a significant threat, the alarm system and the

Owners were notified via a mobile phone notification. One

A significant threat was identified, for example, when a window was smashed.

However, there are indications that it has already been assessed as a threat if

a person merely moved past the vehicle.

189

Art. 60 General Data Protection Regulation (GDPR).

The use of the guard mode in this form was usually not data protection-

compliant: The production and storage of video recordings of people or

License plates in public spaces are generally only permitted if they come from a

sufficient cause takes place. In any case, this is without a concrete threat scenario, for example

if persons or other vehicles merely move past a vehicle

gen, not the case. The interests of the persons concerned then prevail in the

rule those of the keeper.190

Since the end of 2022, sentinel mode has been significantly data-

designed to be more protective. In particular, the cameras are now standard

disabled. The holders can set themselves whether permanent video recordings

should take place. If the cameras are disabled, threats are only through

Sensors detected only when touching the vehicle, no longer during activities

around the vehicle - for example when just passing by - react. Will a threat

detected, the cameras are also no longer activated automatically,

more, the owners receive a notification by mobile phone whether video

recordings are to be made. In addition, Tesla has the duration of the video recordings

reduced to one to ten minutes - depending on the settings of the holder: inside.

Both the cameras and the overall sentry mode are standard

switched off and must be activated manually. The video recordings take place

for the owner's own purposes, e.g. to protect against theft. Holder: inside of

Tesla vehicles are therefore initially self-sufficient to operate in sentinel mode

responsible and have the prerequisites for the preparation and storage

observed from video recordings. In any case, like companies, they

operate the video surveillance technology, obliged to notify the persons concerned

appropriate way to provide data protection information.191 If video surveillance

carried out by means of a vehicle, there is usually an imprint here

on the vehicle. This should draw attention to the fact that and by whom

video surveillance takes place, as well as contain a link or QR code that points to

refers to a website with further data protection information. We are not aware of any case

in which owners of Tesla vehicles actually use the guardian

mode have given required data protection information.

190

191

Art. 6 (1) sentence 1 lit. f GDPR.

Art. 13, 14 GDPR.

Should we come across illegal video surveillance by a vehicle
activated sentinel mode or lack of information about the video surveillance
are made aware of, especially in the case of repeated
violations, the possibility of supervisory measures up to the imposition of a fine
to grab money. This can particularly affect holders who do the above
have not installed the software update, d. H. the sentinel mode in its earlier
use shape. Tesla vehicles are basically also without activated sentinel mode
Lily protected against theft, for example by the also installed in the vehicles
alarm systems.

For Tesla, we are the responsible supervisory authority within Germany. As well
we are responsible for all owners of Tesla vehicles who are based in Berlin
are signed Will the sentinel mode installed in Tesla vehicles or its
Cameras activated must be ensured that other people and vehicles
only be recorded with sufficient cause. In addition, the affected
persons are provided with the necessary data protection information.

11.2 Submission of photocopies of ID for booking of vacation rentals

Booking vacation rentals via online platforms or apps is easy. little
ger convenient it is to register on such a platform or claims on
to assert data information or deletion if unredacted information

white copies are requested. This is now a decision of the Irish

Data Protection Authority (DPC).

An online platform for booking holiday accommodation has its German branch

leave in Berlin. This has been for years for both registration and

for cases in which customers obtain information about the data processed about them

or wanted to have them deleted,192 requested unredacted ID copies

that. Because of this practice, there have been many complaints against the company since 2018

received by our authority. We have reported about this before and

192

See Art. 15, 17 GDPR.

set out the requirements for requesting copies of ID cards. In

As a result, we have recommended the data subjects to oppose the lump sum

to resist requests for unredacted copies of ID cards.193

The company's European headquarters are in Ireland. Ultimately responsible

dig is therefore responsible for processing the content of the complaints we receive

the DPC. A complaint filed in autumn 2019 is now pending

the first final decision of the DPC. The person making the complaint

wanted the company to delete their data. The company for-

initially requested a copy of his ID card for this purpose, whereupon the person refused to give it

to submit and lodged a complaint with us. The DPC has the person in their

Core concerns upheld and ruled that the company was unlawful

acted. The company requested more data than needed to identify

tion would have been necessary.194 In addition, the company did not have sufficient

Doubts about the identity of the person presented and probably did not have.195 The DPC

has accordingly taken action against the company.

It is regularly unlawful for companies to send unredacted statements

Request white copies if data subjects have the rights to which they are entitled under the GDPR

existing rights. The future will tell if the Irish

Data protection supervisory authority also based its decision in this regard on the

Registration process of the online platform transfers.

193

194

195

See JB 2020, 12.4.

See the data minimization imperative i. S.v. Article 5(1)(c) GDPR.

See Art. 12 Para. 6 GDPR.

111

12 sanctions

12.1 Contact Tracing of the Unwanted Kind

In the second year of the pandemic, too, we had to stop improper use of contact

data collected in shops or restaurants for the purpose of documenting attendance

tation were raised, sanction.

To contain the corona pandemic, the various SARS-CoV-2

Infection control measures ordinances, the collection of contact data such as name,

telephone number, address or e-mail address. In a case before us,

which such data is used by an employee of a sporting goods store to

To contact the customer several times privately and to e.g. to invite to a meeting.

The repeated unwanted contact by e-mail was fined

sanctioned by us. In another case, a restaurant guest received unwanted

Promotional e-mails after he entered his contact details in an attendance list

had gene. The restaurant used his alone for contact tracing

e-mail address provided in the event of a corona infection without his consent

for sending newsletters. Even as he had already informed the restaurant

that he did not want any more advertising, he received another undesirable

th newsletter. We also have a fine against the restaurant

enacted

In the meantime, attendance documentation for the purpose of contact

Tracking for infection protection reasons is no longer provided for by law.

12.2 Privacy for the bin

If you want to do a corona test in a test center, you have to do one regularly

Provide a range of personal information. In doing so, the collection of

Data either analog in paper form or digitally via a web application. The

Four fine notices issued by us against operators of test centers

show that breaches of data protection law depend on the format chosen

can occur in different forms.

A company that operates several corona test stations and a digital data

survey via its own internet portal, did not have its registration form

designed in compliance with data protection regulations. The mandatory information on the form was the vaccination status

intended. Neither was there a legal obligation for this information

to carry out a corona test, nor were corresponding consents

ments obtained. In addition, see the online form for specifying nationality

a default preset in the shape of a Germany flag, though too

this information was not required for the purpose of the tests.

In the case of optional information in online forms, the default should always be

be an empty field. Preselected settings (in this case the German national

affiliation) usually violate data protection in the case of optional fields

through data protection-friendly default settings (so-called privacy by default).196 The affected

Because of this pre-selection, fenen people are in the sense of a so-called opt-out

forced to correct the default. With an empty standard field as tech-

niche default would ensure that the optional specification of customers

is only charged if the customers actually want to do it. A

Opting-out, on the other hand, can lead to customers choosing the default setting for convenience

change, or because they overlook it.

In a similar case, we have a company that also

operates corona test stations, issued a fine because this i. a.

the ID or passport number, the vaccination status and the nationality at the

Online registration for a corona test as mandatory information. Another sub

take, which operates corona test stations, had to a complainant who

initially registered for a test, but did not take it,

Various information is continuously stored in our own web portal. That was

despite a request for deletion by the complainant and our intervention as

Regulatory authority not changed. In another case, data of the customers

collected in paper form. The company sanctioned by us disposed of the Anmel

196

See Art. 25 Para. 2 Sentence 1 General Data Protection Regulation (GDPR).

debogen not properly. Instead, completed registration

sheets - in garbage bags together with used corona tests - on the open street

found. There was also no corresponding data breach report by the

Company at our authority, which we sanctioned with a legally binding fine

have functioned.

Use of test center services was limited during the

pandemic is the prerequisite for participation in many areas of society

life. In doing so, we have a wide range of data breaches

identified, where sanctioning with fines was often necessary.

12.3 Penalties for Unauthorized Use of

police database and contact details

from the police service

This year, too, we conducted many fine proceedings against police officers who

unauthorized, d. H. without official reason, personal data from the police

retrieve internal POLIKS database or contact information obtained in some other way

use data for private purposes.

POLIKS is one of the most important electronic information systems in Berlin

Police and accordingly contains extensive data sets. Become in POLIKS

in particular data from suspects, criminals, victims and witnesses

saved. This includes information such as names, dates of birth, addresses,

but also previous convictions and witness statements. The police use POLIKS as information

tion system for their statutory tasks in the area of criminal prosecution and

ren defense. Police officers are regularly informed about data protection

legal regulations informed and instructed that they expressly

is prohibited, data from POLIKS and other police information systems for

use for private purposes. Nevertheless, access to POLIKS is becoming more and more of a problem

abused, people - for example from the personal environment - without official

cause to request and in particular information about their life

to learn circumstances. For example, a police officer asked for information

her new life partner to check whether the police have made an appearance

had kicked.

As part of their daily work - for example during operations or the interrogation of

Witnesses - police officers regularly gain knowledge of the contact details

of people. We have sanctioned several cases in which this was obtained officially

th information then for private purposes by the police officers

were used. In a case before us, a police officer has the

phone number of a burglary victim, which he received as part of a police operation

had learned in his private mobile phone to the woman

then to contact sexually motivated. In another case, a police officer

ter the cell phone number of a woman that he knew from his emergency call service

was also used for private contact.

We initiated 18 cases against police officers this year and

16 fine notices with a total of 124 fines against police officers

enacted Although for many years we have obtained unauthorized use on business

sanction personal data, we unfortunately continue to observe legal

harassing police officers.

12.4 Unauthorized Database Queries

Employees of the job centers

We regularly conduct fine proceedings against employees of the job centers who

have access to various databases as part of their activities, these access

possibility but use for non-purpose queries.

In one case, an employee repeatedly and unauthorizedly provided information about her

Neighbor queried in the job center's electronic information systems. In

In another case, we waived a fine because an employee in the

central process support portal used for online registration information

(OLMERA) requested information about a colleague for private purposes.

115

Chapter 12 Sanctions

This year we have a total of 6 procedures against employees of job

centers, state and district offices initiated and 4 fines with 171

waive fines.

12.5 The Two Eyes Principle: Conflict of Interest

a company data protection officer

within a group structure

We have a fine against the subsidiary of a trading group

in the amount of 525,000 euros due to a conflict of interest of the company

data protection officer imposed. The company had a privacy

commissioner appointed to independently control decisions that

he himself had met in another capacity. The fine is not yet

final.

Company data protection officers have an important task: They advise you

companies with regard to data protection obligations and monitor them

Compliance with data protection regulations. This function may only be

carry out tasks that are not subject to a conflict of interest due to other tasks.197 A

A conflict of interest would exist, for example, in the case of people in managerial positions who themselves

applicable decisions on the processing of personal data in

meet companies. The task must therefore not be performed by people

which would thereby monitor themselves.

Such a conflict of interest existed in the case of a data protection officer of a subsidiary

parent company of an e-commerce group. The person was also business

manager of two service companies, which on behalf of the company

mens personal data processed, for which he acts as data protection officer

was named. The service companies he manages are also part

of the group, include customer service and fulfill orders. the data

The protection officer therefore had to ensure compliance with data protection law by the im

monitor service companies active in the context of order processing,

197

Art. 38 para. 6 sentence 2 GDPR.

which he himself managed as managing director. There was thus an interest

conflict and consequently a violation of the GDPR.

As a supervisory authority, we therefore initially issued a warning in 2021

against the company. After a re-examination earlier this year,

because the violation persisted despite the warning, we imposed the fine.

When calculating the fine, we took into account the three-digit million turnover

of the e-commerce group in the previous financial year and the role of

Data protection officer as a contact for a large number of employees

and customers. The intentional renaming of the

Data Protection Officer over the period of almost a year despite the already

warning issued by us. Among other things, classified that that

Company cooperated extensively with us and the breach during the

ongoing fine proceedings.

This fine underlines the important function of data protection officers

In companies. Data protection officers cannot on the one hand ensure compliance

of data protection law and, on the other hand, have a say in it. One

such self-regulation contradicts the position of data protection officers as

independent authority within the company on compliance with data protection

should work towards. To avoid data breaches, companies should

any double roles of the company data protection officer in group

check structures for possible conflicts of interest. This applies in particular when

if order processing or joint responsibilities between the

Group companies exist.

12.6 The man with the 13th birthday

Incorrect entries and delayed information led to the operator of an inn

credit agency on two fines totaling EUR 46,500.

Contrary to the legal requirements 198 were in the relevant business information

shared a total of 27 incorrect addresses and 13 incorrect birth dates for more than two years

stored data on one of our complainants. The storage of a

Small "data cocktails" in a credit agency poses a significant threat to

the persons concerned in terms of their economic capacity

large amount of incorrect data suggested in the specific case that the complaint

führer has already resided at over two dozen addresses, which means that third parties who

received the entry in the credit agency, a negative impression

can arise.

Only in the context of the request of the data subject for information about

the data processed by the operator of the credit agency were the

incorrect information corrected. In addition, the information was provided on the basis of internal

ner assignment problems first wrong as negative information and then also

late with a delay of more than three months. Because the company

had previously been repeatedly warned by us for relevant violations,

we decided in this case to impose fines that have already been

are strong.

It is essential that the personal information collected by a credit agency

related data can be correctly and clearly assigned to a person. Straight through

In this respect, credit bureaus must also create internal structures in the company

who ensure that information 199 is given truthfully and in a timely manner 200

can be granted.

198

199

200

According to Art. 6 Para. 1 Sentence 1 GDPR i. V. m. Art. 5 Para. 1 lit. d GDPR.

According to Art. 15 Para. 1 GDPR.

Within the one-month period in accordance with Art. 12 Para. 3 Sentence 1 GDPR.

12.7 Publication of sports photos of minors for online sales

In a serious fine case, a sports photographer released over 16,000

Photos of minors participating in a swimming competition in swimwear

taken for sale on a freely accessible website. the minor

could be categorized by country and age groups.201

The company that runs the website in question offers sports photography across the EU

from competitions on. However, it was not possible to obtain effective consent from the photo

signed minors nor their parents for the inclusion and publication of the

photos. Even an appeal to press privileges on the part of the company

mens failed because the images had not been edited, nor one

restriction of their further use for journalistic purposes

is. The fine we imposed is not yet final.

For the commercial use of photos without editorial-journalistic reference

requires the consent of the persons photographed or, in the event that these

are minors, the consent of their legal guardians.

201

See also the comments on the associated administrative case in JB 2021, 3.7.

119

13 Telecommunications

and media

13.1 Fonts on everyone's lips

Triggered by a judgment of the Munich Regional Court (LG) on Google Fonts

Fonts on websites have received a lot of attention recently. caused resentment

a plethora of attempts at civil law warnings. Many operators have the uproar

taken as an opportunity to redesign their websites. It's not just external

embedded fonts, but also the other

to critically review the third-party services set.

The operators are responsible for the visual and functional design of websites

often prefabricated elements that are available from external service providers

be asked. This is particularly common for photos, videos, logos or country

cards. This year the focus has shifted to a service that seems inconspicuous,

for many, however, is indispensable: fonts. As well as other external

Elements can use fonts dynamically or locally. at the dyna-

Mix Embed the fonts simultaneously each time the website is accessed

loaded from the servers of the service providers into the browser of the users. here at least the IP address is transmitted to the external service providers who possibly located outside the European Union (EU).

In order to spare these streams of data that require justification, fonts instead stored on the website operator's own servers and then be delivered locally. The implementation of such a local solution can ber:innen with the help of instructions freely available online and without much effort do it yourself. However, we find that many operators do not is aware of which elements are integrated into their website - especially with website Builders come with many services pre-installed by default. Website can also do this Check operators themselves using a network analysis, which is carried out using the in developer tools included with all web browsers.

In January, the LG Munich dealt with fonts and with a Google Fonts' judgment drew attention to the issue.202 The court constituted a violation of the right to informational self-determination and the personal rights if website operators use the dynamic IP address send messages from third parties to Google automatically and without their consent, as soon as the website is accessed. A legal basis for the transfer of the IP addresses are not available because Google Fonts are also used without a connection to a Google server when the website is accessed is established and the IP addresses of the website users are transmitted Google takes place. The core criticism of the court was therefore the transfer of data in the USA without a legal basis, although this can be avoided without necessity or effort were. The plaintiff was then awarded damages of 100 euros by the court

awarded.

As a result, not only did we receive many complaints about the use of

Google Fonts on websites, but also requests for advice increased significantly

at. The reason for this was an abundance of campaign-like warning attempts. tenthous

Sending website operators were civilly prosecuted for using Google Fonts

received a legal warning, and they were also asked to pay damages. Because of

our original task assignment of the control of data protection

We cannot provide legal advice on how to deal with such warnings.

write done. To website operators when designing their website

but to support data protection law, the German supervisory authorities have

the guidelines on the subject that have already been published in the past. This counts

etc. the guidance of the Conference of Independent Data Protection Supervisors

Federal and state authorities (DSK) for providers of telemedia,

all potential problems related to the use of third-party services on websites

addressed.203

202

203

See LG Munich I, judgment of January 20, 2022, 3 O 17493/20.

See DSK: "Orientation aid from the supervisory authorities for providers of telemedia

December 1, 2021", available at https://www.datenschutz-berlin.de/fileadmin/

user_upload/pdf/orientation aids/2022_OH_Telemedien.pdf; to update the

For guidance after a consultation process has been carried out, see 13.2.

With all the commotion surrounding fonts, it's important to keep in mind that

for most websites, more extensive aspects for a data protection compliant

operation are to be clarified as the use of a single font service. independent

Depending on potential warnings, website operators should use the current

cause a stir to find out which third-party services actually

are actually integrated into their websites. The critical review should be

not limited to the use of fonts, but always the others as well

third-party services used.

13.2 Results of the first DSK consultation process

for guidance for providers of

telemedia

In December 2021, the DSK published a new guide for providers of

Telemedia passed.204 Following the publication, concerns were raised

Stakeholders are given the opportunity as part of a consultation process to

comment on the content of the guidance. All comments received

have been evaluated in the meantime and an updated version of the orientation

published. As a result, individual legal views were specified

and two chapters with practical additions added.

Based on the practice of the European Data Protection Board (EDPB).

the DSK decided to do so, with regard to the orientation aid also interested parties

to include The consultation process serves to review and, if necessary, to

development of the guidance, but is not intended to determine its validity and application in the

touch practice.

A total of 14 statements were received within the two-month consultation period.

gone.205 These were viewed and evaluated and checked to see whether

there is a need for change for the publication. The evaluation was in one

comprehensive report recorded by the DSK on December 5 of this year

205

See JB 2021, 14.2.

These are available on the DSK website at https://www.datenschutzkonferenz-online.de/

consultation procedure.html available.

122

published together with the updated version of the guidance.206

The changes made essentially specify or concretise

some statements on the legal views and assessments of the supervisory authorities.

In addition, two new chapters were added for designing consent banners

as well as the rights of data subjects in connection with the use of cookies

added. Both chapters are of great practical relevance, since complaints

Regulatory authorities often opposed the design of banners and - recently

increasingly - against unfulfilled requests for information in connection with cookies

judge.

We recommend website operators to familiarize themselves with the two new ones in particular

Chapters of the "Orientation Guide for Providers of Telemedia" trusts

make. These deal with the specific design of consent banners

as well as the observance of data subject rights in connection with the assignment

of cookies.

13.3 Online Games: Lawful Change of Address

or secret account transfer?

We get a lot of complaints about online games. In practice, there are often

the legitimate interests of the providers in effective enforcement

of the rules of the game the interests of players when asserting their

rights towards those affected.

In one case, a player wanted to change the email address on their player account.

The player claimed that he has the right to have his data corrected. The

offering companies suspected, however, that the player his account with this

transfer change to another player. This was by the rules of the game

forbidden. The background to these rules is that players can determine their game progress themselves

to achieve in order to enable honest competition. The company

initially denied the player the change on the grounds that it was technical

not possible, but then admitted during the procedure that the change

206

Available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/

orientation aids/2022_OH_Telemedien.pdf.

123

Chapter 13 Telecommunications and Media

the e-mail address is possible, but involves a great deal of effort. It

must be ensured that the new e-mail address is actually the same

person. The company believed it was the change

an e-mail address does not involve a correction of the data, since the old e-mail address

continues to be valid and therefore not wrong.

This objection could not hold: In principle, every person is free to develop

decide which e-mail address they use for which communication purpose or for

which communication partners would like to use. In particular, everyone has to

person may be permitted to gradually remove a specific email address from the

to pull back in order to be able to switch it off at some point, e.g. B. because the person den

wants to switch email providers or because they have too many unsolicited emails

reach a specific address. The correctness of an e-mail address depends on

after not only that they are objectively assigned to the person concerned

can. It is also required that an e-mail address of the data subject

intended for the specific communication purpose. This determination

the data subject may also change over time. So can a former

correct e-mail address becomes incorrect. A company is then fundamentally

obliged to change these upon request. However, the company is allowed to do so

take steps to ensure that the new email address is actually

belongs to the same person. We have a deposit against the company

statement expressed, since this the request for correction without further examination

rejected and the player initially given an incorrect reason for the rejection

named.

If a person wants to change their email address on an online account,

this regularly a request for correction of the personal data

If there are doubts about the legality of the correction, the company

take action to verify.

13.4 Collection of the telephone number as a mandatory field

A company offers the use of digital media content over the Internet within the

sign up for a paid subscription. We received a complaint that

the company of customers who use the paid version of the offer

dialed, collected a telephone number as mandatory information.

According to the company, the collection of the telephone number for the contract

Fulfillment 207 required: If customers have a problem using the offer

have that cannot be solved by e-mail or chat, the employees of the

company that supports customers personally on the phone. In addition, the knowledge

registration and use of the telephone number also for the prevention of misuse and fraud

manoeuvrable: In the event of suspected third-party access to the customer account or

incorrect debits and corresponding blocking of the account the customers

be notified by SMS. Alternatively, the compulsory collection of tele-

phone number and its use for the above Purposes also on legitimate interests of

company.208

The mandatory indication of the telephone number for service purposes or for

Use and fraud prevention is responsible for the conclusion and implementation of user

contract with the company within the meaning of the GDPR is not required. For

the implementation of the customer service is sufficient for the company

available communication channels, in particular through the possibility

the use of the present e-mail address and through the offer to those concerned

People to call the company's customer service themselves.

For fraud and abuse prevention, there are other options than use

the telephone number, such as the e-mail notification for log-in

Try or use a dedicated app.

The compulsory collection of the telephone number cannot be attributed to authorized persons either

interests of the company are supported: 209 Although this has in principle a

legitimate (economic) interest in the collection and processing of the data

207

208

209

Article 6 paragraph 1 sentence 1 letter b of the General Data Protection Regulation (GDPR).

See Art. 6 (1) sentence 1 lit. f GDPR.

See ibid.

the customers. However, there is no compulsory collection of the telephone number

here, too, by the necessity stipulated by law: customer satisfaction

Security and effective prevention of abuse or fraud can be just as good

This ensures that the company provides its customers with the information

a telephone number for the purposes mentioned, so that those customers

Those who want to make use of the service offer their telephone number

can specify, while those customers who want to do without it, none

have to provide information. As a result, the compulsory collection and further

Processing of the telephone number of the persons concerned is not necessary in order to

safeguarding the interests of the company.

As part of a weighing of interests with the interests of the persons concerned

NEN would also be the contrary will of those people considerable, the

do not wish their telephone number to be used for the stated purposes. Simultaneously

a compulsory collection of the telephone number violates the obligation

for data minimization.210 For the collection of the telephone number, the

Obtaining consent is necessary.211 In the case of consent within the meaning of the GDPR

it must be a voluntary “for the specific case, in an informed manner

and unequivocally given declaration of will".212 Voluntary

However, there is no reliability if the telephone number is designed as mandatory information

is. As a result of our intervention, the company has the phone number of the

deleted and we were also informed that in the future we would

not to use telephone numbers as a mandatory field. We have a warning

pronounced.

The collection of telephone numbers as a mandatory field in Internet offers must

neither for the fulfillment of the contract with the persons concerned nor for authorized persons

interests of those responsible may be necessary. Where this is not the case,

those responsible for a (voluntary) consent from their customers to the survey

and obtain the intended use.

210

211

212

Article 5(1)(c) GDPR.

Article 6 paragraph 1 sentence 1 lit. a GDPR.

Art. 4 No. 11 GDPR.

13.5 Amendment of the RBB state contract

The State Chancellery of the State of Brandenburg and the Berlin Senate Chancellery work

ten currently working on the amendment of the State Treaty on the establishment of a

joint broadcasting corporation of the states of Berlin and Brandenburg (RBB State

bear). According to the currently known draft status, e.g. planned to control

compliance with data protection regulations also in the so-called economic-administrative

to transfer the strategic area to the RBB data protection officer.

So far, the control has been subject to compliance with data protection regulations

the processing of personal data for journalistic purposes of data

protection officer of the RBB, while the control in the economic-administrative

Area - this mainly affects the data of broadcasters for moving in

of the license fee and the data of employees of the RBB and its auxiliary

and associated companies - is assigned to our authority. This division will

also practiced in Brandenburg, Bremen and Hesse. In the other states

the control for both areas is the responsibility of the data protection officer of the respective

broadcaster. The current draft for the amendment of the RBB state contract provides for

that in the future the control for both areas will also be carried out in Berlin and Brandenburg

the RBB data protection officer should take place.

In a joint statement with the state commissioner for data

protection and for the right to inspect files (LDA) Brandenburg, we have

dere noted that the proposed full transfer of the

Data protection control of the RBB data protection officer

is compatible with the provisions of the GDPR: Derogations from Chapter VI of the

GDPR, which contains regulations on the independent supervisory authorities, are only

permitted if this is necessary in the processing of personal data for journalistic purposes

Purposes is required "to exercise the right to protection of personal data with

to reconcile freedom of expression and freedom of information

gen".213 This does not apply to the processing of personal data in

lich-administrative area and in particular not for the processing of personal

drawn data from license fee payers and employees of the RBB and

213

Art. 85 para. 2 GDPR.

its auxiliary and affiliated companies. The transfer provided in the draft

the control of compliance with data protection regulations on one or an inter-

NEN broadcasting data protection officer: n also for the processing of personal

Data in the economic-administrative area therefore violates the regulations

of the GDPR and is therefore contrary to European law.

The procedure provided for in the draft for the appointment of a

radio data protection officer for the control of the processing of personal data

We consider data outside of data processing for journalistic purposes to be

contrary to European law: According to the version available to us at the time of going to press

new state treaty, only the Broadcasting Council or the

Intendant of the RBB with the approval of the Board of

works. According to the GDPR, however, the appointment is the responsibility of the parliament, the government

tion, the head of state or an independent body acting under the law

of the EU Member State is entrusted with the appointment.214 The appointment by a

independent agency such as B. an electoral commission, can only be admissible if

this body in turn has sufficient democratic legitimacy.

The broadcasting and administrative boards of the RBB are due to the

seen (and previously practiced) naming procedures for their

Members, however, are not independent bodies within the meaning of this provision. Of the

then 33 members of the broadcasting council, only seven become members of the state parliament

Brandenburg and sent by the House of Representatives, at the suggestion of the respective

Parliamentary groups are elected.215 The majority of the members of the Broadcasting Council

on the other hand, not elected, but by the many named in the state treaty

Institutions and bodies (e.g. churches, business associations, trade unions

ten and other social groups).216 The board of directors in turn

consists of seven members elected by the Broadcasting Council and one member

rat delegated member.217 Broadcasting Council and Board of Directors do not have

sufficient democratic legitimacy within the meaning of Art. 53 Para. 1 GDPR for

the appointment of members of an independent supervisory authority for data

protection. Nor does the appointment presuppose a proposal from the government or any of its members

214

215

216

217

Art. 53 Para. 1 GDPR.

This corresponds to the previous regulation in § 14 Para. 1 No. 24 RBB State Treaty.

See § 14 Para. 1 RBB State Treaty.

See § 19 Para. 1 RBB State Treaty.

128

members, of Parliament or a Chamber of Parliament, as is the case in the GDPR

is provided.218

The supervisory structure practiced so far in Berlin and Brandenburg has proven itself

according to our authority in consultation with the LDA Brandenburg for the supervision

on the processing of personal data in the economic-administrative

Area is responsible while supervising the processing of personal

Data for journalistic purposes by the data protection officer:n des

RBB takes place. In our view, there is no reason for a change.

The control of compliance with data protection regulations in the economic-administrative

nistrative area of the RBB should as before by our authority in consultation

be perceived with the LDA Brandenburg. A transfer to the or

the data protection officer of the RBB is not possible under European law.

218

See recital (EG) 121 sentence 1 GDPR.

129

14 political parties

14.1 The purchase of addresses does not release from obligations

A citizen complained to us who had received personally addressed election advertising from the

of the Association of Political Parties found in his mailbox. He had the advertising

neither gave the party his address nor was he otherwise in contact with her.

The information in the imprint of the advertising brochure did not get him any further, because she only led to an address dealer.

Our complainant therefore wrote to the party and asked them about it. Man initially saw himself as not responsible and took the position that one bought the addresses and the advertising via a so-called letter shop from the address have had the service provider send it. You never have the addresses in your own hands had, but only contributed content. As part of our test, it turned out that the party had commissioned the list owner in particular to sen that corresponded to certain selection categories: So should the For example, those addressed have “performer-like characteristics”, “[party] affinity and younger than 60 years”. In addition, certain political cal attitudes and belonging to certain social milieus become.

We have warned the national association of the party for several reasons: In this case, the dealer and the party were jointly responsible, since neither the Address dealer nor the party without each other's part on the selection of Addresses could finally decide. For this it does not matter whether the party had direct access to the data.219 The data had no legal basis been processed because the person addressed did not consent to the receipt of

219 See European Court of Justice (ECJ), judgment of July 10, 2018, C 25/17, para. 68 f.

party advertising.220 At the same time, the party was committed to its information and obligations to the future.221 The party appealed against our warning A complaint has been filed with the Administrative Court, which has not yet been decided.

14.2 Fake testimonials in the election campaign?

In September 2021, citizens received personalized letters in which they

Personalities from politics and business were called upon to

to elect the tenth Bundestag candidate. The letters mediate in the absence of others

Information gives the impression that it was sent directly from the people who advertised it

stand up for the candidate.

Even if the content of the letter is in agreement with the supposed sender:in-

were designed, the addresses of those addressed came from the reporting

register and were retrieved from there by the district association of the party being advertised.

fen. The retrieval was made on the basis of the specifically regulated for parties

Authorization in the Federal Registration Act (BMG).222 The district association transmitted the addresses

then an advertising provider 223 and commissioned them with the mass mailing

of recommendations (testimonials). Despite corresponding requests for information on our part

the district association of the party could not submit an order processing contract 224,

which already made it inadmissible to pass on the addresses to the advertising provider. Also

there is no legitimate interest in the processing of the data by the district

connected, if those affected are left in the dark about who the author

of election advertising. Furthermore, the district association of the party through the design

of the letter violate its information and transparency obligations. For the

However, this is important information for the recipients - such as: Where did the party come from

220

221

222

223

224

In principle, according to Section 50 of the Federal Registration Act (BMG), parties may use addresses from the

received registration register. There is a right to object, but not

regarding the purchase of addresses. In addition, § 50 Para. 1 BMG only allows very much

limited selection criteria (e.g. age group). Advertising that goes beyond § 50 BMG

Permissible goes beyond that is only permitted with consent.

See Art. 14, 15 General Data Protection Regulation (GDPR).

See § 50 Para. 1 BMG.

In the so-called letter shop process; see 14.1.

According to Art. 28 Para. 3 GDPR.

131

Chapter 14 Political parties

my data? Who processed my data? What legal remedies do I have

Disposal?

In view of the high number of people affected and the seriousness of the violations, we

hand over the process to our sanctions office for further processing.

132

15 Europe and International

15.1 Uniform guidelines for calculating fines

In May, the European Data Protection Board (EDPB) issued new guidelines on

resolution of fines.225 The European data

safety supervisory authorities agreed on a uniform fine practice.

Our authority has the Conference of Independent Data Protection Authorities

of the federal and state governments (DSK) in the EDSA working group "Fines".

and played a key role in developing the guidelines. The guidelines see a five-step process

existing assessment procedure that reflects the nature and severity of the violations and

taking into account the turnover of the companies concerned:

In the first step of the assessment procedure, it is determined whether the case in question

sanctionable actions and to what extent these have led to violations.

It is clarified whether all or only some violations will be punished with a fine

can become. In the second step, a starting amount for calculating the money

repentance, which now takes place according to a uniform model. The third step will be

aggravating or mitigating factors that affect the amount of the fine

can increase or decrease. The guidelines see a uniform interpretation for this

before. In the fourth step, the statutory maximum amount of the fine pursuant to Art. 83

Para. 4 to 6 General Data Protection Regulation (GDPR) determined and ensured that

the amount is not exceeded. Finally, in the fifth step, it is checked whether the

calculated final amount meets the requirements of proportionality and effectiveness

suffices or further adjustments to the amount are required.

After the guidelines were approved, they were subject to a six-week public review

Consultation. The feedback was taken into account in the final version

and the guidelines around a reference table with starting points for calculating the

225

EDPB Guidelines 04/2022 of 12 May 2022: "On the Calculation of Administrative

Fines under the GDPR", available at https://edpb.europa.eu/our-work-tools/documents/

public-consultations/2022/guidelines-042022-calculation-administrative_en.

fine added, which the severity of a violation with the turnover of a company

correlates.

The guidelines increase the transparency of the procedure of the data protection

supervisory authorities when imposing fines. Since her adoption

the guidelines form the basis for the fine calculations made by our authorities.

15.2 Privacy Certification

This year, certification according to Art. 42 GDPR has gained significant momentum.
to. The first German certification program for order processing called
EuroPriSe was approved by the supervisory authority in North Rhine-Westphalia, after-
which it goes through a process of inner-German and European coordination
in which our authority was also actively involved. With three further certifications
tion programs that have been submitted to other German supervisory authorities
den, we have also contributed to the domestic German vote. underneath
was a certification program for order processing by cloud service providers
ter: inside. Another generic certification program for managers and
We will continue to present processors in the future in the role of co-reviewers
accompany the EDPB.

The aim of the certifications is to increase transparency and ensure compliance
GDPR by providing a quick overview of the level of data protection
relevant products and services. As part of certification
procedure, an accredited certification body checks a specific data transfer
working process for compliance with previously defined certification criteria.
If the test is positive, the certificate is issued for three years and can be used in the
connection to be renewed. Within the three-year period, the certification
also obligated to carry out random checks.

With the help of data protection certificates, citizens can easily
identify friendly services for private use, companies will e.g. B.
the selection of processors easier. The duty of the responsible

chen for the careful selection of reliable processors: inside 226 can in the
in practice mean a considerable amount of testing and primarily represents small and medium-sized

ere companies sometimes face challenges. Certificates can choose
suitable services for order processing. to note
remains that not the company as such, but a specific processing
development process is certified. So it always has to be done by those responsible
be checked whether the specifically planned use of the respective providers: inside the
certified processing.
The certification criteria, which further specify the requirements of the GDPR, are
an essential part of certification programs and must be prior to their use in the
practices are reviewed and approved by the relevant regulatory authority. In addition
contain the certification programs application notes and test methods that
also examined by the supervisory authority as part of the program review
become. This year we were actively involved in examining the certification
experience gained in the context of the DSK working group
"Certification" in the new version (2.0) of the "Requirements for data protection
lic certification programs", which was adopted in June.227
We also have this together with the other German supervisory authorities
improved the internal German coordination processes. Likewise this year
work on the two test programs submitted to our authority
set. Overall, the inner-German cooperation this year has
increase in practical experience with data protection certification
programs, which will facilitate future program audits. After
EuroPriSe, the first German certification program for order processing
a process of domestic German and European coordination of the supervisory
authority in North Rhine-Westphalia in 2022, we assume that
soon a certification body will be accredited and the first certificates will be issued
can.

The first German data protection certification program (EuroPriSe) was established

after internal German and European coordination by the supervisory authority in

226

227

Art. 28 Para. 1 GDPR.

Available at https://www.datenschutzkonferenz-online.de/media/ah/DSK_

Certification criteria_V2_0_Stand_21062022.pdf.

135

Chapter 15 Europe and International

North Rhine-Westphalia approved. We assume that certification will soon

agency is accredited so that processors in Germany

country for all types of processing according to this program

sen to show to those responsible that the processing

GDPR compliant. Based on the experience of this and other certification

DSK has met the requirements for data protection certification

fication programs further specified.

15.3 International Traffic: Scheduled

US adequacy decision

Awareness and attention to the transmission of personal

In the second year after the "Schrems II" judgment of the European

European Court of Justice (ECJ) increased sharply. We get more and more complaints

against companies from various sectors in which complainants

Transfers of your data to countries outside the European Economic Area

(EEA) reprimand.

After the ECJ on July 16, 2020 the adequacy decision of the European

had declared invalid for the USA by the European Commission,228 existed for companies

and those affected have great uncertainties when it comes to the transmission of personal data to the USA.229 On October 7 of this year, US President Joe Biden has a new one Executive Order issued, which the ECJ's criticisms of the US to invalidate the right to watch. On this basis, the European Commission plans to able to adopt a new adequacy resolution 230 for the United States.

With such a decision, the European Commission attests to a third country an adequate level of data protection outside the EEA, which allows companies men from the EEA is enabled to collect personal data without the further measures 231 to that third country. A new Appropriate

228

229

230

231

CJEU, judgment of July 16, 2020, C-311/18 ("Schrems II").

See 2020 Annual Report, 1.2.

See Art. 45 GDPR.

See Chapter V GDPR.

security decision for the USA must therefore in any case the criticism of the ECJ from the Clear up the "Schrems II" verdict. Specifically, this means that for government access on data from the EEA clear and in accordance with the principle of proportionality Appropriate rules and effective legal protection options against official access must be created for data subjects from the EEA. After introducing one concrete draft for an adequacy decision by the European Commission, the EDPB will carefully analyze the draft and issue an opinion

hand over. We are accompanying this development intensively and are also bringing ourselves to the fore
Work in the EDPB working groups when evaluating such a decision
and its consequences. Only with the full implementation by the US side
planned changes and the adoption and entry into force of a
adequacy decision for the USA, the concrete legal situation regarding
Lich transatlantic transmissions. Until then, companies must meet the requirements
from the "Schrems II" judgment continue to be fully observed.
We observe that the attention and awareness of the issues of the
International data traffic strong for companies and complainants
have increased. This is also reflected in the growing number of complaints
visible, the alleged illegal data transfer to third countries to the content
have or in which the transmissions, in addition to other violations, as supplementary
the point of objection to be reprimanded. The corresponding complaints are addressed
against companies and institutions from various sectors such as medicine,
Financial products, delivery services, legal advice, therapy, education and public
databases. The international data traffic is thus increasingly the
role of a cross-cutting issue, since hosting, order processing and
commercial data exchange in many cases to transfers to third countries
comes.
Those companies that recognize data exports in their own area of responsibility
now base their data transmissions to the USA on for the most part
so-called Standard Contractual Clauses (SCC) as suitable guarantees.232 Through the assistance
of the German and other European data protection supervisory authorities 233

232

233

See Art. 46 Para. 2 lit. c GDPR.

the central requirements of the ECJ in this area could be specified.234

In many cases, however, companies are still not taking adequate

the additional measures required by the ECJ. Therefore we carry out our test

80 companies' data exports as part of website and

e-mail hosting.235 A large proportion of the procedures have now been

sen as the controllers will terminate the processing in question

or a more legally secure solution for hosting their website or email server

have chosen verse. However, a few responsible persons continue to rely on the

Transmission to third countries without the requirements of Chapter V of the GDPR and the

adequately implement the requirements of the ECJ. We are in talks about this

with the companies, but are also examining the seizure of supervisory authorities

Remedial Powers.

If companies have compliance with data protection regulations through a certification

236 striving for verification and in this context also transfers of personal data

in third countries, applicant companies must prove that they

comply with GDPR transfer requirements. Appropriate

Specifications must therefore be included in the corresponding test programs for certification

places to be included. Our authority accompanies such a program before the EDPB

and also checks its conformity with Chapter V of the GDPR.237

As can be seen from the increasing number of complaints from all economic

areas shows that there is still a great need for advice in the area of

national traffic. We bring ourselves within the framework of the German and European

intensive cooperation in the clarification of remaining questions and the

enforcement of the requirements of the ECJ. Any future appropriate

The security decision for the USA must meet the requirements of the "Schrems II" judgment of the

234

235

236

237

See EDPB Recommendation 01/2020: "Measures to supplement transmission

Tools to ensure the level of protection under Union law for personal data

data", available at https://edpb.europa.eu/our-work-tools/our-documents/

recommendations/recommendations-012020-measures-supplement-transfer_en;

see also the DSK report on US surveillance law by Stephen I. Vladeck,

available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/

publikationen/DSK/2022/2022-Vladek_Rechtsgutachten_DSK_de.pdf.

See JB 2021, 1.1.

I.S.v. Art. 42 GDPR.

See 15.2.

138

Chapter 15 Europe and International

fully implement the ECJ in order to protect personal data

corresponding foreign connection as well as legal certainty for companies and

to ensure citizens. Until an offer finally comes into effect

measurement resolution for the USA, those responsible must refer to other instruments

ments from Chapter V of the GDPR and these in accordance with the specifications

from the "Schrems II" judgment.

15.4 European Cooperation

The GDPR provides for close cooperation between the European supervisory

authorities before. In particular, this involves cases involving a cross-border

involve the processing of personal data.

A case is cross-border if the data processing takes place either in several

branches in various member states of the European Union

(EU) or if the processing takes place in only one branch

has or are having effects on data subjects in more than one Member State

can.238 Our authority takes the lead in processing those cases in which

the responsible company has its headquarters in Berlin. Is the

Headquarters of the company in another member state of the EU or the EEA,

we transmit the cases we receive to the supervisory authority of the respective

member state. In this case, we are only the supervisory authority concerned.

The lead supervisory authority investigates the case and is in constant contact

Exchange with the supervisory authorities concerned.239 As soon as the lead supervisory

If the supervisory authority has identified a case, it presents it to all the supervisory authorities concerned

a draft resolution for a vote. Accordingly, our authority

again this year the draft resolutions of other leading supervisory authorities

reviewed and objections lodged in the case of deviating positions. On this way

we have commented on a large number of issues between the European

European supervisory authorities require coordination.

238

239

Art. 4 No. 23 GDPR.

Art. 60 GDPR.

In those cases in which the lead authority responds to the objection of a

If the authority does not wish to follow, it contacts the EDPB for dispute resolution.240

The German authorities first agree on the content of such objections among themselves

away. This year, for example, we have dealt with four objections that have been agreed within Germany

against draft decisions of the Irish Data Protection Authority (DPC).

involved in large Internet companies, which then went into the dispute settlement procedure.

For example, an objection to a draft decision by the DPC on data

processing for behavioral advertising by a major social media

service, against which other European supervisory authorities

Germany under the leadership of the Hamburg Commissioner for Data

protection and freedom of information objected. The objection to its creation

we were significantly involved, complained that the media service

processed data unlawfully,241 as he has no legal basis for the

extensive processing of the data,242 including some that are particularly worthy of protection

Data,243 features. A general reference to the fulfillment of the user agreement 244

is not sufficient in this case. Although the consent of the person concerned

obtained, but a refusal would result in the complete refusal of the offer

and is also inseparable from consent to other matters.245

It was also objected that the resolution had legal consequences for the company

not specified clearly enough. The appeal asked the DPC to

instruct responsible person to delete the unlawfully processed data, future

to prohibit current data processing without a legal basis and an appropriate

and to impose a dissuasive fine.246 Regarding these appeals

the EDPB on December 5th of this year the binding decision 3/2022: 247

Although the EDPB does not follow all the arguments in the objections, in the present

sible case that the person responsible in the case of behavioral advertising

240

241

242

243

244

245

246

247

Art. 65 GDPR.

See Article 5(1)(a) GDPR.

See Art. 6 GDPR.

See Art. 9 GDPR.

Art. 6 (1) sentence 1 lit. b GDPR.

See Art. 7 Para. 2 GDPR.

In accordance with Art. 58 (2) lit. c, f and i GDPR.

Available at https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_bg.

not to the fulfillment of his contractual rights from the contract of use against

about the person concerned.

In addition, as part of the DSK working group “Organization and

Structure" to improve the inner-German coordination of such objections

contributed: Last year we reported that one of our objections to

Dispute settlement proceedings had gone.248 Together with our colleagues

Lower Saxony and Hamburg, who also have experience with dispute resolution procedures

have, we offered a workshop for the German supervisory authorities on the subject

which was received very positively. In addition, we also have our own

Drafts coordinated in the cooperation process. In 15 cases we were able to reach consensus

adopt final decisions with the concerned supervisory authorities in Europe and

thus creating clarity for data subjects and those responsible.249

Overall, the increasing experience of all supervisory authorities with the European

European cooperation procedures to an ever smoother process, the one

productive exchange of content with the aim of finding a consensus.

248

249

See JB 2021, 16.2.

See 18.6.

16 Freedom of Information

16.1 Developments in Germany

The Conference of Freedom of Information Officers in Germany (IFK)

this year under the chairmanship of the State Commissioner for Data Protection Schleswig-

Holstein passed three resolutions.

With a resolution, the IFK called on those involved in the coalition negotiations

after the state elections in Lower Saxony, the enactment of a transparency

law in the coalition agreement.250 A corresponding passage can be found

now in the coalition agreement between the SPD and Bündnis 90/Die Grünen.251 In a further

In its resolution, the IFK recommends that the administrations in the federal and state governments

Relevant official communication in embodied form - regardless of whether

communicated in paper form, as e-mail, via SMS or using social media

will - to document in order to grant access according to the freedom of information law

guarantee.252 The IFK refers to a judgment of the Federal Administrative Court

(BVerwG) on the disclosure of Twitter direct messages from the Federal Ministry

of the interior and for homeland.253 In a third resolution, the IFK considers

the handling of the state government of Mecklenburg-West Pomerania with access to

Information about the Foundation for Climate and Environmental Protection MV states that foundations

who perform public tasks, the public has a right to information

functions. The right to access information then exists regardless of whether

it is a foundation under public law or - as in the case of the Stiftung Klima- und

250

251

252

253

Resolution of the IFK of October 26, 2022: "Lower Saxony: The time for a transparency

law has come!", available at https://www.datenschutz-berlin.de/infothek/

decisions-of-ifk.

See lines 28-33 in the coalition agreement "Safe in times of change - Lower Saxony

future-proof and in solidarity" for the period 2022-2027, p. 102.

Resolution of the IFK of June 30, 2022: "SMS in the file: Official communication

is fully subject to the rules of freedom of information!", available at

https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk.

BVerwG, judgment of October 28, 2021, 10 C 3.20.

Environmental protection MV - is one of civil law.254 The elected

The organizational form must not undermine the state's duty of transparency.

16.2 But no transparency law for Berlin

In the last two years we have reported extensively on the efforts

the outdated Berlin Information Freedom Act (IFG) of 1999 with a modern one

to replace the Transparency Act.255

This year it was now clear that the corresponding statement in the red-green

red coalition agreement, 2022 a transparency law based on the Hamburg model

to introduce and thereby maintain the high standards of the IFG, not a priority

had.

16.3 Transparent Food Control

In the last two years we have been improving information for

Consumers through the introduction of the Food Control Transparency

law (LMÜTranspG),256 which we very much welcome. The law is now

known as the "Clean Kitchens Act" and will come into effect on January 1, 2023

Power. Details on the official procedure are contained in an implementing regulation

regulation,257 which was submitted to us for comment in the draft.258 You

contains the details of the rating system and the presentation of what is to be disclosed

so-called food monitoring transparency barometer.

254

255

256

257

258

Resolution of the IFK of June 30, 2022: "No circumvention of freedom of information by

Establishment of foundations under civil law!", available at https://www.datenschutz

-berlin.de/infothek/beschluesse-der-ifk.

See JB 2020, 19.2.2; JB 2021, 17.2.1.

See JB 2020, 19.2.3; JB 2021, 17.2.1.

So-called Food Monitoring Transparency Act Implementation Ordinance

(LMÜTranspG-DVO), GVBl. 2023, p. 7 ff.

The Berlin Commissioner for Data Protection and Freedom of Information is before the enactment of

Hear laws, ordinances and administrative regulations if they

concern freedom of information or the processing of personal data; please refer

§ 18 para. 2 sentence 3 IFG and § 11 para. 2 sentence 2 Berlin Data Protection Act (BlnDSG).

143

Chapter 16 Freedom of Information

Hygiene management in the company is responsible for 50% of the assessment,

while compliance with food law regulations is more likely at 6.25%

plays a minor role in the control result. It is the spirit and purpose of

new regulations required and appropriate that in favor of health

the consumer may not take final administrative measures

measures taken against the food company as a criterion for evaluating the "income

compliance with food law provisions" must also be taken into account;

the administrative measures themselves are not included in the transparency

rometer listed. However, we have spoken out in favor of

legitimate period of misconduct on the part of food companies at all

only be relevant, does not go back indefinitely, but to the last

is limited to six years. We consider this period to be appropriate because it

on the one hand takes into account the European requirements according to which results are made

earlier official controls are to be included,259 and on the other hand the federal

legally regulated control interval of three years for companies with a low

risk is taken into account.260 This ensures that even with these companies

be more than just an official control in the current surveillance measure

can flow in.

16.4 Transparent school system?

In 2020, in the course of the discussion about the numerous area exceptions

men criticized in a new transparency law that the entire school area of

was excluded from the scope from the outset.261 This was justified

in the Senate draft at the time that a ranking list for schools should be avoided.

As is well known, the intended law was not passed.262

At the request of a parliamentary group, the Scientific Parliamentary Service (WPD)

comprehensively examined the questions raised in accordance with the IFG and constitutional law and

259

260

261

262

Regulation (EU) 2017/625 of the European Parliament and of the Council.

General administrative regulation on principles for the implementation of the official

Monitoring of compliance with the provisions of food law […]

(AVV frame monitoring).

See AGM 2020, 19.2.2.

See 2020 Annual Report, 16.2.1.

an expert opinion found that there was a need for secrecy in relation to the collected

Statistical individual school data basically does not exist.263

16.5 Processing of IFG applications - Even without postal address!

We received several submissions from citizens because the one requested

Ask - especially the police - before you deal with the respective IFG application for the first time

requested the postal address of the applicant. The requirement

was pronounced regardless of the stage of the proceedings, i.e. even if

initially only preliminary information on costs was desired. The police reasoned

as follows: "The information is required in order to

to avoid issuing information to an anonymous application, as well as

to enable the decision to be made accessible in an identifiable manner." You

pointed out to the applicants that without an address no further processing

successes.

We have informed the police that an "anonymous application" is being considered

of the communicated name is not available and that the collection of the postal address

violates the IFG.264 According to this, the processing of personal data

permissible insofar as this is necessary to fulfill the tasks specified in this law

is. In addition, we have pointed out that inspection of files

according to the IFG orally, in writing or electronically.265 The

refusal or restriction of file inspection or file information is regular

be justified in writing or electronically.266 The extension of these provisions

the wording "or electronically" was made by Article 21 of the Act

to adapt the form requirements in Berlin state law (FormAnpassG).

263

264

265

266

WPD report of April 8, 2022: "Questions about the existence and scope of a

Right to information with regard to certain statistical data on individual schools

in the State of Berlin", available at https://www.parlament-berlin.de/media/download/2819.

See § 4a IFG.

Section 13 (3) IFG.

Section 15 (1) IFG.

145

The template for this was drawn up by the Senate Department for the Interior and Sport.267

After that, simple electronic communication in IFG cases is completely sufficient

from.268 We have informed the police that their view reflects the clear intention

the legislature: the postal address of IFG applicants

to demand as a prerequisite for the initial processing of the IFG application is not

required.269

Because the police didn't change their procedures, nor did they agree with our view

discussed, we at the Senate Department for the Interior, Digitization

tion and sport because of their fundamental responsibility for the right to freedom of information

a complaint and request for support due to incorrect application of the IFG

submitted by the police. The interior administration did not share our view and

primarily based on § 13 para. 1 IFG, which does not allow an anonymous application

provides. The interior administration did not respond to our argument that

the amendment to the law on the permissibility of simple electronic communication

initiated by herself and was found to be permissible at the time. we see

us in our opinion by the judgment that has been passed in the meantime

administrative court (OVG) of North Rhine-Westphalia,270 confirms the contrary

267

268

269

270

See Abghs.-Drs. 18/0420 of June 21, 2017; on p. 16 of this template it says: “With

This or a form requirement with the same meaning will be used alongside the traditional one

Written form also includes all electronic forms, including 'simple' electronic ones

forms allowed. The term 'in writing or' also refers to the electronic

Forms specified that the content/text must match that of the paper form. Short:

Whenever an email is sufficient, this form requirement should

to get voted."

See also the further explanations in relation to § 15 Para. 1 IFG in ibid., p. 18:

"According to the sense and purpose of the regulation in § 15, the applicant should

given the opportunity to review the reasons for the refusal. The font

required is used for textual fixation (exclusion of orality). on the special

Evidence and authentication mediated via the qualified electronic signature

function doesn't matter. The decision is also one

administrative act. According to Section 37 paragraph 2 of the Administrative Procedures Act, an administrative act

in writing, electronically, orally or in any other way. The simple

Electronic form without a qualified signature is therefore sufficient."

In this respect, we receive the opinion represented in the JB 2021 under number 17.2.3.1 that for the

"Proper delivery of a (fee) notice a deliverable

postal address" must always be given.

See OVG North Rhine-Westphalia, judgment of June 15, 2022, 16 A 857/21 (not

final).

146

Chapter 16 Freedom of Information

judgment of the lower court 271 in relation to the problem in question.

The fourth guiding principle of the Higher Administrative Court's judgment says: "Neither from the regulations

of the Freedom of Information Act nor from general procedural regulations

the general obligation of an IFG applicant to submit his postal

to indicate in writing." The Federal Administrative Court appealed to will provide clarification

bring about.

We appeal to the public authorities in the state of Berlin, the postal address of the

If possible, not to request applicants if they are responsible for processing the

IFG application, e.g. B. for the desired advance cost information, actually not

is needed.

16.6 Shadows and Lights in the Senate Administration

for education

A citizen applied to the Senate Department for Education, Youth and Family

Disclosure of the last tender and award documents for the "IT experts

Schools". He did not submit the application under his real name, but used

a pseudonym.

At his request, the citizen received information from the education administration that

there was an award document with several lots for all applicants in 2018

have given. However, the documents are not sent according to the IFG

provided, so that alternatively only a telephone file information or the inspection

on-site is possible; about the fee for this would depend on the chosen variant

decided. When in further communication it turned out that the citizen at

had given a pseudonym in his application, the Senate administration demanded that

Identification and the provision of a postal address in order to receive the approving IFG notice

to send.

Our examination has shown that the requested information was on the Internet at the time

was generally available. Against this background, we could the Senate administration

271

See Administrative Court (VG) Cologne, judgment of March 18, 2021, 13 K 1190/20.

finally convince the applicant to provide the desired, electronically

handene information to send free of charge, without the real name and the

to request a postal address. The message granting the application was for the citizen

not disadvantageous and could therefore be sent informally.

We welcome the result-oriented and citizen-friendly about-face of the Senate

administration for education, youth and family.

16.7 IFG refusal at the foundation supervision

A citizen complained to our authority that the Senate

The foundation supervisory authority responsible for justice, diversity and anti-discrimination

Statutes of a foundation under civil law did not want to disclose. The Foundation

supervision justified the refusal of access to information i.a. so that

the right to freedom of information does not apply without restriction, but rather (in addition to the

Restrictions in the IFG itself) “on the basis of general legal principles

Limits” experience. The apparently intended publication of the statutes on the

Online platform FragDenstaat would subject the foundation to publicity that

they are fundamentally not subject. The citizen objected to this

and asked us to support his request.

We have informed the foundation supervisory authority that the decision they issued

particular is unlawful because it contains no statement as to which

ches concrete exceptional circumstances of the IFG the access to information is denied.

Rather, the general statements made it clear that the supervisory authority for foundations

assumed that access to information on all companies under her

were excluded from the outset. However, as long as there is such a

If there is no area exception for the supervision of foundations, the authority in

each individual case and in relation to each requested document with the IFG exception

facts 272 and, if necessary, the statutory hearing

proceed with the affected foundation.273

272

273

§§ 5 ff. IFG.

Section 14 (2) IFG.

The foundation supervisory authority did not agree with our view and

finally rejected, this time u. a. on the grounds that the IFG

Application like any other legal claim "overarching legal standards as

Objection can be raised if these apply to the exercise of

contrary to the right made". This is z. B. in the case of "contradictions in

half of the legal system" is the case. Since these general statements

were not valid in our opinion and there are still no comments on

IFG facts limiting or excluding the claim were made

den, we could only recommend that citizens seek judicial clarification.

The IFG also applies to the supervision of foundations. She must like any other public

Offices of the State of Berlin Information access requests for foundation documents

based on the exceptional circumstances of the IFG and cannot rely on it alone

overarching legal standards.

16.8 Constitutional complaint of the Humboldt University of Berlin

In connection with the submitted by the Humboldt University of Berlin (HU).

Constitutional complaint to review whether the amendment to the Berlin High

School Act (BerlHG) 274, the legislative competence has been exceeded

was, a citizen applied for the disclosure of various documents. For this

included the statement of complaint and information on the contractually agreed

disclosed costs for legal advice. The HU rejected the application on appeal

on trade and business secrets worthy of protection and referred to them

beyond the lawyer's duty of confidentiality. The disclosure of the complaint

debriefing would also conflict with the ongoing court proceedings. Incidentally, be

he copyrighted.

We have informed the HU that it must be clarified in the objection procedure why in

Reference to the contract with the legal representative also a partial disclosure

274

The revised § 110 Para. 6 BerlHG regulates temporary employment relationships

the so-called follow-up commitment for scientific and post-doctoral employees.

149

Chapter 16 Freedom of Information

out of the question.275 Because not every piece of information in the contract is there from the outset

a trade or business secret worth protecting.276 Professional secrecy is also

secret of the lawyers commissioned by the HU does not access the information

in contrast to. As the "mistress of the secret", the HU cannot rely on the professional

the secret of the secret bearer she had mandated.277 Eventually

not sufficiently clear why by disclosing the complaint brief

adverse effects for the State of Berlin in the implementation of an ongoing

court proceedings are to be feared.278 The determination of the specific possibility

adverse effects on the part of the body responsible for information - here

missing - statement of facts from which an impairment arises

of the subject to be protected.279

The statement of complaint is also not to be protected under copyright law

work, because according to this only personal, intellectual creations enjoy copyright

legal protection.280 The required originality is lacking if the creation of a

subject by technical considerations, by rules or by others

constraints was determined. Amount of work or significant expertise involved in the

design are therefore not sufficient.281 This was therefore not the case

plausible that the complaint brief of the authors of the HU man-

dated law firm not according to the requirements of the HU - namely in relation to the

procedural result to be achieved and to be validly justified - was created. The

The creation of the complaint brief was therefore determined by the specifications of the HU,

so that the document is not a personal, intellectual creation,

therefore not a copyrighted work. In front of this background

For this reason, we recommended that the HU publish the complaint brief and

moreover - also in view of the public interest - even the proactive publication

on their website.

275

276

277

278

279

280

281

See § 12 IFG.

See § 7 IFG.

See BVerwG, judgment of December 15, 2020, 10 C 25/19.

See § 9 Para. 1 Sentence 2 IFG.

See VG Berlin, judgment of December 8, 2021, VG 2 K 48/20, citing BVerwG,

Judgment of November 27, 2014, 7 C 12/13.

§ 2 Para. 2 Copyright Act (UrhG).

VG Berlin, judgment of November 1, 2021, VG 2 K 142/20.

The HU did not agree with our view. The citizen has against the

Corresponding notice of objection of the HU complaint at the administrative court (VG)

raised in Berlin.

We welcome the clarification of the numerous legal issues initiated by citizens

the Administrative Court of Berlin.

16.9 Police publication as permanent classified information?

A citizen complained to us that in the database of a university

tätsbibliothek a publication by the police from 2005 about the residence ban

disposal was listed, but not as classified information by the police

was disclosed. The police justified this by saying that by disclosing

Conclusions about the tactical approach of the police could be drawn, what

would represent a serious disadvantage for the State of Berlin. Next was called

it: "Government action, especially that of the police, must not be calculable or

be foreseeable, otherwise the legally assigned tasks of the police

Averting danger and preventive criminal prosecution can no longer be fulfilled

to. There is therefore a risk that, in such cases, if third parties become aware of

obtained such information, which in future will relate to police actions

Art could set what an effective police task fulfillment essential

would complicate. The passing on of this document for further training to persons or

Positions outside of the Berlin police are prohibited."

We have informed the police that the relevant decision to the citizen

is unlawful. For it contains one known to us from numerous other cases

Standard text and does not deal with the fact that the coveted

document is now more than 16 years old. In this respect, we doubt that the

General knowledge is still suitable for drawing conclusions about the tactical approach

to the police, and therefore disclosure continues to have a serious

would represent a disadvantage for the State of Berlin.282 In addition, the

282

See § 11 IFG.

Decision no statement as to whether the reasons for the previous level of secrecy

"Confidential" have meanwhile been omitted. Despite two

not expressed from multiple memories.

We have to state that the police are here, but not in other cases either

or does not adequately deal with our legal opinion. At a

Amendment of the right to freedom of information, we will advocate that our

Recommendations to bodies responsible for information when making decisions about the

access to information must be taken into account.

16.10 Police Service Regulations on the police fitness

We received a complaint from a citizen of disclosure to the police

Administrative regulation PDV 300 required. This regulates u. the health

Aptitude test for police service. The police refused to disclose

and justified this with the fact that this could have a negative impact on the

concerns of public safety are to be taken care of.

The police explained that with knowledge of the regulation and existing illnesses

health symptoms could be tried, the symptoms during an examination

to disguise accordingly to contrary to the necessary requirement in the

to enter the police service and to be able to exercise it. In addition, they counted

Documents to protect the official decision-making process according to § 10 Para. 4

IFG: "By publishing them, the internal and inter-authority

process may be affected."

The refusal of access to information cannot be based on Section 10 (4) IFG

become: Because after that is only the discussion, deliberation and consideration, consequently

the actual process of deliberation, protected. On the other hand, the administrative

provision as the basis for forming a decision is not part of the scope of protection of Section 10

Para. 4 IFG. Section 11 IFG was also applied incorrectly. Because there were contrary to that

The wording of the law only "possible adverse effects" on the interests of the

public security adopted through the disclosure of the police service regulation.

These possible "simple" disadvantages already do not constitute valid arguments

are to be considered against disclosure are not sufficient: are required

according to the wording of the law, rather "serious" disadvantages for the well-being of the

federal or state. These were definitely not recognizable.

In this case, too, the police did not deal with our arguments-

set and the objection of the citizen against their decision with still

rejected without valid justification. The question arises

the meaningfulness of our legally standardized advisory authority,283 if our

Arguments regularly play no role in the decision on IFG applications.

16.11 district office submission in Mitte

A citizen asked the Mitte district office to forward the district office template

1400/2021 approving an addendum to a contract of sale

to the visitor and information center of the German Bundestag

has. The application was rejected on the grounds that it was an internal one

Document that the decision-making process and the consultation within the district

officials and is therefore not subject to the right to information under the IFG.

We supported the citizen's appeal against this decision. One

Access to files or information should be denied if the content of the files relates to the

process of decision-making within and between authorities.284 The right

access to files or information does not exist, insofar as files relate to the advice of the

Senate and district offices and their preparation.285 This provision

protects the core area of executive personal responsibility, i.e. the advisory

secret of said bodies. This includes only the discussion, consultation

and deliberation, hence the actual process of deliberation. Are not protected

in the case of both of the exceptions mentioned, the factual bases and the

Result of the decision-making process.286

283

284

285

286

§ 18 paragraph 2 sentence 2 IFG.

§ 10 paragraph 4 IFG.

§ 10 Para. 3 No. 1 IFG.

VG Berlin, judgment of August 25, 2016, 2 K 92.15.

Therefore, we informed the district office that a district office submission only the facts

forms the basis for the subsequent district office decision and is therefore fundamental
to be disclosed. The district office apparently kept other district office templates
moderately not in need of protection, because numerous templates are even proactive
published on the district website. So we made it clear that
Notice of objection may have to contain additional statements from which the
Need for protection, especially with regard to the district office requested in the present case
template results.
Due to our intervention, the Mitte district office ultimately did not have the citizen
only sends the desired document free of charge, but also records it
published on the district website.
We welcome the smooth communication with the district office and in the present
particular case that our recommendation was also taken up
The document requested is subsequently accessible to all interested parties on the Internet
close.

16.12 Food controls in Pankow

We received two complaints from the Veterinary and Food Inspectorate
Pankow. In one case, a citizen requested information about the latest food
controls in an organic market. In another case, a citizen asked given
of the automated references the file number and the place of jurisdiction of the model
procedures and instructions on how to deal with inspection report requests
regarding.
In the first case, the citizen received the on his numerous reminders each time
following standard message: "The pending test case at the administrative
the court has not yet made a final decision. Once a decision is made
will proceed accordingly. Until then, you are asked to
refrain from asking. Alternatively, we refer to our website […].” We had to

inform the citizen that we cannot mediate in this matter. Because ours

Authority has in matters of the law to improve the

154

Chapter 16 Freedom of Information

health-related consumer information 287 does not have the function of an arbitration

stop. This function was only given to us in relation to the IFG by the state law

geber.288 So we could not help the citizen here to ensure that the

District Office Pankow issued a substantive decision.

In the second case, however, we acted towards the district office of Pankow. Then

the district office failed to recognize that with the few information sought after, none

health-related consumer information is affected, but only general ones

Information was requested to which the IFG applies. The office then called us

the file number and the competent court, but also informed us that

that the requested instructions do not exist. It had this information

Citizens initially kept secret. Only after our notice that our authority only

as an arbitration body and not as a carrier of answers from the requested body

to the applicant, the office made up for its omission and

judged the citizen.

In the case of inquiries in connection with food controls, the requested

authority to check in each individual case which legal basis for the disclosure

information is considered.

287

288

Also known as the Consumer Information Act (VIG).

§ 18 IFG.

155

Chapter 16 Freedom of Information

16.13 IFG refusal at RBB

We received two complaints from citizens against Rundfunk Berlin-Branden-

castle (RBB). In one case, the position of the RBB was disclosed in advance

the drafting of the amendment to the state treaty with regard to the termination of the

restric or linear radio broadcasting via VHF, DAB broadcasting and

request the distribution of radio programs via mobile communications. In the other case

a citizen requested details on "ideas management" in the RBB, i. H. what

Suggestions for improvement submitted since 2018 and with a cash or non-cash prize

were rewarded.

Both requests were rejected by the RBB and the rejection as follows

Standard justification: "An obligation to provide information on the part of the RBB can only apply to the

There are areas in which the RBB acts as a sovereign in the narrower sense, e.g. B. in

As part of the collection of broadcasting contributions or when allocating broadcasting time

to parties." In addition, it was pointed out that the obligation to provide information

RBB basically the entire area of editorial-journalistic activity

taken and according to the IFG no information has to be provided

who in any way draw conclusions about editorial secrecy and the

Allow program order.

With regard to the complaint case "state treaty amendment" we have informed the RBB

shares that he cannot evade access to information here because the position

RBB's actions are not actually constitutionally protected journalism

table-editorial activity 289 and also not the editorial secret

regarding. Because this includes, above all, the secrecy of the information sources.

Such information was not affected here. Also a substantive reference of the

Request for information on program order 290 was not evident. We have therefore

asked to review the request for information, taking into account the

Possibility of only partial disclosure.291

289

290

291

This activity falls under the scope of Art. 5 Para. 1 Sentence 2 Basic Law (GG).

This is in § 26 Media State Treaty (MStV) and § 3 of the State Treaty on the

Establishment of a joint radio station for the states of Berlin and Brandenburg

(RBB state contract).

See § 12 IFG.

With regard to the "ideas management" complaint, we explained to the RBB that the

selected standard formulation as the sole justification for the information

refusal is not sufficient, but the concrete request of the citizen IFG-compliant

to be answered. The RBB finally informed the applicant that the

desired information is not available.

The RBB is also in principle to an IFG-compliant decision, possibly under

Consideration of the IFG exceptions,292 obligated. Will the informa-

denied access to the IFG, this decision is ultimately also judicial

easily verifiable.293

16.14 Access to information at Tempelhof

Project Ltd

A citizen asked Tempelhof Projekt GmbH for a 100% state-owned

nes company, an overview of all reports with environmental relevance

to the Tempelhof airport building. The GmbH informed her that she was not under

falls within the scope of the IFG. The citizen asked us to support her

concern.

We drew the attention of Tempelhof Projekt GmbH to the fact that although

not within the scope of the IFG with regard to general information

subject,294 however that access to environmental information such as that requested here

from the special regulations in § 18a IFG i. In conjunction with the Environmental Information Act (UIG)

is determined.295 Private bodies with an obligation to provide information can therefore be such,296

who perform public tasks or provide public services,

related to the environment, in particular those related to the environment

services of general interest, and thereby under the control of the state of Berlin or one

legal entity under public law subject to the supervision of the State of Berlin

292

293

294

295

296

§§ 5 ff. IFG.

See Art. 19 Para. 4 GG (guarantee of legal recourse).

§ 2 para. 1 IFG.

See § 2 Para. 2 IFG.

See Section 2 Paragraph 1 No. 2 UIG.

subject. Against this background, we asked the GmbH to submit the application again

to be checked and according to the specifications of § 18a IFG i. V. m. the UIG to be modest.

In addition, we have pointed out that in the present case the legal process

has been given to the Berlin Administrative Court.297 This means that the applicant

lerin can have the decision of the GmbH reviewed by a court if necessary, which we can do for her

also recommended. However, we had to tell the citizen that we

cannot continue to work for you because our arbitration board

Function formally only to authorities and other public bodies of the State of Berlin

extends.298

Disclosure of environmental information can not only be done by public bodies,

but in principle also required by private institutions.

297

298

Section 18a (3) IFG.

§ 18 para. 2 sentence 1 IFG.

17 From the office

Our office has experienced some fundamental innovations this year.

In addition to moving to a new office building, the choice and

Filling the vacant position of the Berlin Commissioner for Data Protection and Information

Freedom of mation crucial.

After Maja Smoltczyk left at the end of October 2021, the position was

Berlin Commissioner for Data Protection and Freedom of Information for over a year

occupied. During this time, the department was provisionally managed by Deputy Volker

Brozio directed. On October 6th of this year, Meike Kamp became the new Berliner

elected officer for data protection and freedom of information. with her assumption of office

on November 15, she took over the management of the department.

At the end of September, our authority moved from Friedrichstraße to new offices

Old Moabit drawn.

17.1 Cooperation with the Chamber of Deputies

The Committee for Digitization and Data Protection (DiDat) came into being this year

together 17 times and dealt with topics of modernization and digital

tal transformation of administration. The Berlin Commissioner for Data Protection and

Freedom of Information attended all meetings and provided extensive advice to the panel

together with their experts.

The implementation of the Online Access Act,299 the digitization of health

houses 300 and schools 301 were important items on the agenda at the

Committee agenda. In one of the last meetings of the year, Meike received

Kamp, the newly elected Berlin Commissioner for Data Protection and Information

299

300

301

See 1.2.

See 5.1.

See 4.4.

liberty, opportunity to give the committee their ideas for the coming term of office

to be presented.302

17.2 Cooperation in national and international

conferences

Also this year, our authority took part in the meetings of the Conference of Independent

pending data protection supervisory authorities of the federal and state governments (DSK) as well as

the Conference of the Freedom of Information Officers in Germany (IFK) and

worked intensively with colleagues from the other federal states.

The DSK met this year under the chairmanship of the Federal Commissioner for the Data protection and freedom of information from March 22 to 24 in Bonn and from 22 to 24 November in Koenigswinter. In addition, three interim conferences were held on January 27, June 22 and September 21 in Berlin. The DSK summed up during their meetings, numerous resolutions and resolutions on current data protection law common topics, e.g. on data protection-compliant online trading using guest access,303 to Facebook pages and to the processing of personal data for purposes of scientific research.304

The IFK met underground in Kiel from June 29th to 30th and from November 8th to 9th the chairmanship of the State Commissioner for Data Protection Schleswig-Holstein. There were passed three resolutions: on access to information on all official communication, access to information at foundations under civil law and Necessity of a transparency law in Lower Saxony.305

The Global Privacy Assembly (GPA) 306 took place as a two-day face-to-face conference from October 27th to 28th in Istanbul. The focus of the conference was the law Privacy in an era of rapid technological advances. beyond that

302

303

304

305

306

See https://www.parlament-berlin.de/ados/19/DiDat/protokoll/dd19-016-ip.pdf.

See 10.4.

All resolutions and resolutions of the DSK are available on our website at https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk available.

See 16.1.

Formerly International Conference of Data Protection and Privacy Commissioners.

160

Chapter 17 From the office

The institutional development of the GPA was again an important topic. The GPA adopted numerous resolutions and reports, including about the principles and expectations for the appropriate use of personal data in the Face Recognition Technology.307

17.3 Service point for citizen submissions

The Citizens' Submissions Service Center is the central point of contact for people to report a violation of your data protection rights to us or to find out about possible possibilities for self-data protection. This year we barely reached 4,500 submissions by the service center either through short-term advice or Provide the required information processed or put into formal administrative procedures were transferred.

As in all areas of our agency, further progress has been made towards achieved with the forthcoming changeover to a fully digitized process. From the almost 4,500 inquiries and complaints that the service point received this year recorded, more than 1,500 were transferred to administrative processes. thematic the data processing in health management should be emphasized, where further Progressive digitization processes and the corona pandemic played a role.308

Even with companies in the housing industry, with payment services and with mobile There is often a need for improvement in dealing with personal related data.309 There are also government agencies and here in particular the Police authorities repeatedly in our investigative focus.310 We were increasingly reached also inquiries due to fraud attempts on online platforms, warning Write or fake information on websites in different ways

also affected data protection rights of data subjects.311

conducting the census for a variety of submissions by individuals who

307

308

309

310

311

All GPA resolutions and reports are available on their website at

https://globalprivacyassembly.org/document-archive/adopted-resolutions/ and

https://globalprivacyassembly.org/document-archive/working-group-reports/ available.

See 5.2-5.4; 12.1-12.2.

See 6.2; 9.1-9.2; 11.1-11.2; 13.4.

See 2.1-2.3; 12.3.

See 10.11; 12.6; 13.1.

queries made there to be too extensive.312 These were carried out by us

on behalf of the state representative for data protection and the right to

File inspection (LDA) Brandenburg submitted.

We often had to refer to other authorities or institutions this year,

if fraud attempts in the digital space, although the processing of personal

contained data, but a data protection violation was not the main focus. So show

some people worried about being reported to an internet portal that

supposedly reported opponents of vaccination to health authorities. In the imprint of

Portals were called a dummy authority, which were the actual authors

can not be determined. People who feared have been reported through the portal

be, we recommended a self-disclosure request at the responsible health authority,

for further steps we could only refer to the law enforcement authorities. middle

while the website is blocked.

The situation was similar with fake invitations that were supposedly sent out by the police.

zei were sent by e-mail requesting personal data. Here could

we inform about the alleged phishing scam, but at the same time referred to

the police, who also made public statements about the fraud attempts

had turned. Also the often because of the embedding of Google Fonts on the

warnings sent out by a law firm on our own website

forwarded by those affected. Here we were able to explain the facts and

in many cases provide some peace of mind about the protection of your own data

concerns.313

A large number of different inquiries are received at the service point

on data protection and freedom of information. Also regarding others

Areas of life that relate to data protection and the digital world,

Berliners turn to us with confidence.

312

313

See 2.6.

See 13.1.

17.4 Privacy Literacy for Children and teenagers

After the restrictions caused by the corona pandemic, we were able to this year

offer regular workshops at primary schools again. Also, we have ours

Websites for children and young people revised and introduced new lessons

material ready for teachers.

Discover in our school workshops, each lasting five lessons

the children in grades 4 to 6, what data is, how it is collected and

why they are worth protecting. Using specially created case studies, the

Students already have their understanding of personalized advertising and its use

published data. From the beginning of May until the end of the year we have 15 workshops

carried out and thus reached over 300 students. A building block is also the

Cooperation with the Children's University Lichtenberg (KUL), for which we are part of “KUL

on the go” 90-minute workshops on the subject of “Your data, your rights”

ckelt.314 These took place in autumn at schools in Lichtenberg, Treptow-Köpenick,

Wuhletal and Buch.

On the occasion of this year's Safer Internet Day, we also published in the spring

new teaching materials on privacy and security on the Internet.315

These are divided into five units in which the students e.g. learn what

personal data are, what rights they have and what is involved in online

instruction must be observed. The materials are intended for 4th grade teachers

up to 6, but can also be adapted to the needs of higher classes if necessary

become. The units are each designed for one lesson and contain

Worksheets also provide detailed instructions and background information for

the teacher.

We also have a program for teachers as part of the campaign day “Data competence makes

School” offered a data protection workshop. The day of action took place on May 17th this-

th year and was funded by DigiBitS (digital education meets school), a project

314

315

See https://kul-unterwegs.de/angebote/workshop/deine-daten-deine-rechte.

Retrievable at https://data-kids.de/fuer-lehrkraefte/.....

from Germany safe online e. V., organized.316 Our workshop was attended by

Around 40 teachers took part, to whom we conveyed the data protection regulations

which are to be particularly observed when dealing with personal data of students

are. The participants learned how children and young people can

handling of their personal data can be sensitized and received practical

Xis-related and methodical suggestions for the media competence of the students

to strengthen.

We also have the website in a transnational working group

youngdata.de redesigned and preparing for its relaunch in the coming year.

Youngdata is an Internet portal for young people that is run by the independent data

protection supervisory authorities of the federal and state governments as well as the Swiss canton

Zurich is offered. On this platform young people and young adults can find

Information on data protection and your right to freedom of information. Also

our website data-kids.de, which is aimed primarily at children aged 6 to 12 years

as well as parents and educators, we have asked for additional materials and new ones

formats added.

17.5 Public Relations

The focus of our public relations work this year was the expansion of digital

tal communication and the expansion of our media information offer.

So we opened our profile on Mastodon, launched our start-up school and

revised our website.

In mid-February we launched our account on the social network Mastodon.317 Bei

Mastodon is a decentralized microblogging service that provides data

represents a protective alternative to Twitter. About a profile will be short posts

published, in which we draw attention to current topics of data protection and information

tion freedom and questions from now almost 2,400 followers:in-

answer.

316

317

See https://www.sicher-im-netz.de/datenkompetenz-mit-digibits-–-aktiontag-für-mehr

-digital-enlightenment.

See https://social.bund.de/@blnbdi.

Chapter 17 From the office

With the introduction of the virtual series of events "Start-up School" at the end of March

we were able to expand our range of information events. The start-up

School is aimed at Berlin start-ups and associations, which we support with the events in

support data protection issues in a targeted manner.318 The topics presented

ranged from compliance with data protection in data processing and

the integration of external service providers via data protection-compliant design

from websites to the fulfillment of corporate transparency obligations. The

Start-up school results from the previous offer of start-up consultation hours and

bundles the persistently strong need for information of newly founded companies

and associations on data protection issues and the application of data protection law

regulations.

After the restrictions caused by the pandemic, we have again this year

more face-to-face appointments and our work with lectures and information

information stands at various congresses and conferences. lecture topics

were i.a. data protection in the school context, video surveillance in museums, the

Sanction practice of the data protection supervisory authorities as well as the most frequently asked questions

Use of cookies. By participating in the events, we

inform the citizens about current data protection issues and

establish numerous contacts for future projects and cooperations.

318

See https://www.datenschutz-berlin.de/themen/unternehmen/start-up-schule.

165

Chapter 18 Statistics

18 Statistics

The following comments on the number of complaints and data breaches per year

2022 not only fulfill our reporting obligations under the General Data Protection

Regulation (DSGVO) and the Federal Data Protection Act (BDSG), they also orientate themselves

to the uniform statistical criteria that the conference of independent data

protection supervisory authorities of the federal and state governments (DSK).

18.1 Complaints

In total, our authority received 4,445 submissions from those affected this year,

of which 840 as formal complaints i. S.v. Art. 77 GDPR were to be dealt with.

For the majority of the complaints, we opened procedures under our own responsibility.

There were 1,525 procedures this year. Of these, almost 85% were opposed

private bodies (1,327), the rest against government agencies and other public bodies (198).

In 315 cases, the complaints were not within our area of responsibility, which is why

they have been handed over to the responsible supervisory authorities.

The graph below lists the number of complaints to public and

non-public bodies and our payments to other German supervisory

authorities compared to the last six years.

complaints

public bodies

Non-Public Bodies

duties

281

1222

195

2018

17

88

312

2017

523

521

1684

1656

248

2019

253

2020

166

580

1589

267

2021

315

1327

198

2022

Chapter 18 Statistics

18.2 Consultations

Consultations include all written information to affected persons,

Responsible persons and representatives of the public administration summarized.

With 2,605 cases, the focus was on advising affected persons.

In addition, we advised those responsible in 133 cases and issued a large number of

phonic information, which is not statistically recorded.

consultations with affected persons

2079

2402

2438

3235

2605

195

655

2017

2018

2019

2020

2021

2022

18.3 Data Breaches

Data breach reports

public bodies

Non-Public Bodies

1163

1026

137

2021

1068

920

148

2022

1015

873

43

142

2019

925

821

104

2020

167

357

314

2018

45

7

52

2017

Chapter 18 Statistics

This year there were a total of 1,068 reports, of which 920 reports

to the non-public area, i. H. mainly private companies.

Public authorities reported 148 data breaches to us.

18.4 Remedial Actions

If we discover a breach of the GDPR by those responsible, we can

take various remedial actions.319 Accordingly, in this

Year 7 warnings and 269 warnings issued. In one case, a

issue an order. We have 35 fine notices with 326 fines

totaling 716,575 euros. The relevant procedures were up to

By the end of the year, however, not all of them had been legally concluded. In addition,

44 penalty payment notices issued. In 5 cases we filed a criminal complaint.

23 fine proceedings were discontinued over the course of the year. In addition, one

a large number of further proceedings were opened in which no decision had yet been issued.

Remedial Actions 2022

warnings

warnings

Instructions and Orders

fines

7

269

4

326

319

See Art. 58 Para. 2 GDPR.

18.5 Formal support for legislative projects

According to the Berlin Data Protection Act (BlnDSG), our authority has the task,

the House of Representatives, the Senate and other bodies and institutions on legislative

lative and administrative measures to protect the rights and freedoms of natural

to advise other persons.320 This includes both written statements and

also meetings with political groups and MEPs as well as formal hearings

in the House of Representatives and in its committees.

This year we accompanied several legislative projects, such as B. the

Amendment of the State Hospitals Act (LKG).321 Together with the State

commissioned for data protection and for the right to inspect files (LDA) Brandenburg

we gave an opinion on the draft of the RBB state contract.322

Advice on legislative projects that involve the creation and amendment of legal

ordinances and administrative regulations. As an example

here the adaptation of the implementation regulations for youth welfare in criminal proceedings

(JuHiS) to the provisions of the GDPR.323 For projects of the federal law

together with the other supervisory authorities of the Federal

of and the countries position.

18.6 European Procedures

The GDPR stipulates that the European data protection supervisory authorities

cross-border cases.324 Within the framework of the cooperation procedure

a lead supervisory authority is determined for this purpose, which in each case

Investigations are in progress.325 Other supervisory authorities may identify themselves as affected authorities

report if those responsible have a branch in their country

or the data processing has a significant impact on the citizens of their country

320

321

322

323

324

325

Section 11 (1) sentence 1 no. 3 BlnDSG.

See 5.1.

See 13.5.

See 4.1.

Art. 60 et seq. GDPR; see also 15.4.

Art. 56 Para. 1 GDPR.

des has. After completing their investigations, the lead supervisory authority

submit a draft decision to the supervisory authorities concerned for their comments.326

In total, our authority published 15 draft resolutions and

15 final resolutions. For coordination and cooperation we use like the others

European supervisory authorities the electronic internal market information system

(IMI). The table below provides an overview of our participation in the

most important of these European procedures.

European procedures with our participation 2022

Procedure according to Art. 56 GDPR (affected)

Procedure according to Art. 56 GDPR (responsible)

Procedure according to Art. 60 et seq. GDPR (responsible)

335

21

30

326

Art. 60 para. 3 sentence 2 GDPR.

170