privacy and

Freedom of Information

Annual Report 2020

annual report

the Berlin Commissioner for Data Protection and

Freedom of Information as of December 31, 2020

The Berlin Commissioner for Data Protection and Freedom of Information has

House of Orders and the Senate report annually on the results of their

activity (§§ 12 Berlin Data Protection Act, 18 Para. 4 Berlin Information

Freedom of Information Act). This report closes on April 3, 2020

Annual Report 2019 submitted and covers the period between 1 January

and December 31, 2020 onwards.

The annual report is also available on our website, see: https://

www.datenschutz-berlin.de

imprint

Editor:

Berlin representative for

Privacy and Freedom of Information

Friedrichstr. 219, 10969 Berlin

Telephone: (0 30) + 138 89-0

Fax: (0 30) 2 15 50 50

Email: mailbox@datenschutz-berlin.de

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

Layout:

april agency GbR

Sentence:

Print:

LayoutManufaktur.com

ARNOLD group

contents

contents

contents

8th

List of abbreviations

List of abbreviations

House of Representatives printed matter

General German Bicycle Club

Alternative for Germany

tax code

General safety and order law

building code

Federal Data Protection Act

Civil Code

Federal Court of Justice

Berlin Implementing Law for the Federal Registration Law

Berlin Commissioner for Data Protection and Freedom of Information

Abghs.-Drs.

ADFC

AfD

oh

ASOG

BauGB

BDSG

Civil Code

BGH

BlnAGBMG

BlnBDI

BlnDSanpG-EU Berlin Data Protection Adaptation Act EU

BlnDSG

BlnTG

BMG

BR-Drs.

BürgBG RP

Berlin Data Protection Act

Berlin transparency law

Federal Registration Act

Federal Council printed matter

State law on the ombudsman of the state of Rhein-

state-Palatinate and the commissioner for the state police

Federal Association of Data Protection Officers e. V

Federal Constitutional Court

Federal Administrative Court

Berlin transport company

Federal Elections Act

Federal Electoral Code

German Accreditation Body

German Hotel and Restaurant Association

Association of German Chambers of Commerce and Industry V

printed matter

Data Protection Impact Assessment

General Data Protection Regulation

Conference of Independent Data Protection Authorities

of the federal and state governments

European Data Protection Board

BvD

BVerfG

BVerwG

BVG

BWG

BWO

thanks

DEHOGA

DIHK

Drs.

DPIA

GDPR

DSK

EDSA

List of abbreviations

EFM

ground floor

ECtHR

EU

ECJ

EuWG

EEA

GBV

GDD

GewO

GG

GJPA

GKDZ

GRCh

GStU

GVBl.

GVG

HGB

IBAN

ID

IFG

IFK

IfSG

ICT

IMI

IT

ITDZ

IWGDPT

JB

KG

AI

KTDat

LKG

LMÜTranspG

MDK

public transport

Electronic fare management

recital

European Court of Human Rights

European Union

European Court of Justice

European Elections Act

European Economic Area

land registry disposal

Society for Data Protection and Data Security e. V

trade regulations

constitution

Joint Legal Examination Office Berlin-Brandenburg

Joint control and service center

Charter of Fundamental Rights of the European Union

City-wide control of accommodation

Law and Ordinance Gazette for Berlin

Jurisdiction Act

commercial code

International bank account number

identifier

Freedom of Information Act

Conference of Freedom of Information Officers in Germany

German Infection Protection Act

Information and communication technology

Internal Market Information System

information technology

IT service center Berlin

International working group on privacy in technology

gie (Berlin Group)

annual report

Court of Appeal

Artificial intelligence

Communications Technology and Privacy Committee

State Hospital Act

Food Control Transparency Act

Health insurance medical service

Transportation

List of abbreviations

OVG

OZG

PassG

PassVwV

PAuswG

PKS

POLICIES

rbb

RefE

RegMoG

RL

SaaS

SARS-CoV-2

SBC

SchoolG

SGB

StGB

StPO

TKÜ

TMG

TTDSG

VAG

VBB

VDV

VersFG-E

VersVermV

VG

Laminated safety glass Bln

VvB

VwVfG Bln

advertising agency

AWAY

ZBS

ZPO

ConditionCatOrd

Higher Administrative Court

Online Access Act

passport law

General administrative regulations for the implementation of the passport

legal

Identity Card Act

Police Crime Statistics

State police system for information and communication

and processing

Radio Berlin-Brandenburg

draft bill

Register Modernization Act

policy

Software as a Service

severe acute respiratory syndrome 2 (coronavirus)

Server based computers

school law

social code

criminal code

Code of Criminal Procedure

Telecom Surveillance

Telemedia Act

Telecommunications Telemedia Data Protection Act

Insurance Supervision Act

Transport association Berlin-Brandenburg

Association of German Transport Companies

Freedom of Assembly Act Draft

Insurance Intermediary Ordinance

administrative court

Constitution Protection Act Berlin

Constitution of Berlin

Administrative Procedures Act Berlin

Law on the Commissioner for the Armed Forces of the German Bundestag

condominium community

Central Contribution Service

Code of Civil Procedure

List of responsibilities for regulatory tasks

List of abbreviations

a notice

The glossary (at the end of the brochure) provides a list of explanations of

different technical terms.

foreword

The year 2020 was primarily characterized by the corona pandemic and its

Effects on social life, on education, training and work.

Our everyday life was sometimes completely turned upside down: the work was suddenly

Sometimes no longer possible or often only “remotely” – i.e. from a distance – possible.

The schools are closed, the day care centers are in emergency operation, most authorities and

other public facilities open at times. Shops – with

with a few exceptions –, restaurants and cultural sites: Closed. And everything

ahead: The sensitive restriction of social contacts. The lockdown triggered a

a real push towards digitization and also put data protection on top of it

tough test. Video conferencing, homeschooling and digital con-

clock tracking became a matter of course almost overnight.

However, the use of data

protection-compliant services and software.

In the first phase, this may seem unexpected and immediate.

it must have been understandable to the social and economic

to sustain life to some extent. The use does not comply with data protection

ter and thus legally inadmissible services must not become permanent.

Digitization, which is often hasty during the pandemic, opens up at the same time

also the chance to become aware of the problems and dangers involved

in order to take remedial action once the most critical phase of the pandemic has been overcome

and intensively on the data protection-compliant design of data processing

to work. Right now we should keep reminding ourselves that

data protection does not serve to prevent digitization, but to

Protecting people from the dangers involved. It is a fundamental right

of the citizens and at the same time a legal obligation for everyone

the data controllers, which must not be violated.

Foreword The fact that the data protection-compliant use of digital means is important to many

is also reflected in the large number of inquiries and complaints that my

authority reached on this topic during the peak phase of the pandemic.

We therefore developed fundamental recommendations and assistance at a very early stage

ments on the use of digital learning platforms and the use of video conferencing

border services issued. Additionally, we conducted a more detailed audit

of various video conferencing services, the result of which we use a traffic light

rated and published. Our clues didn't just call

among the users of such services, but also among the service providers themselves

a big echo. As a result of our publication, around a dozen of them

publication of his contracts after intensive exchange with us by the end of 2020

designed in accordance with data protection regulations. The choice of privacy-friendly services

has become so big that there is no longer any excuse for using it

offers that are questionable under data protection law.

This is a good example that data protection is not an obstacle to digital

talization, but on the contrary increases their quality. That's it too

from the outset can be compliant with data protection, shows the development of the Co-

rona warning app. In no time at all, the data protection

legal framework for mobile applications for contact tracing

puts. My authority has worked on the development of the corresponding guideline

actively involved and those responsible in Germany in the implementation

comprehensive advice on the specifications. And even if functional

If something is missing from the app, this does not change the basics

success of the project. The Corona warning app is proof that the development

Development of data protection-friendly solutions is possible if everyone pulls together

pull, and that it can also succeed in record time. As such poses

it is a prime example for other digital projects in public administration

And the large number of people using the app is proof that

People are more open to digital products if they trust them

ensure that their data is not misused. In countries opting for a

less data protection-compliant model, the usage figures are

len significantly lower.

On the other hand, the adaptation of the Berlin state

right to the requirements of the European General Data Protection Regulation (GDPR)

foreword ahead. The legislative project, with which about 80 Berlin laws to the European

cal data protection law were aligned, more than two years after

passed by the House of Representatives during the implementation period. we

have closely accompanied it - as far as it was possible for us - and our expertise

brought in. Nevertheless, no tick can be placed behind this major project,

because the Berlin state law still has numerous data protection regulations

shortcomings and does not always do justice to the European legal framework. Into the-

in particular the basic data protection regulations of Berlin, the Ber-

liner Data Protection Act, has significant deficits in the area of data protection

view and control. It is therefore only to be hoped that the House of Representatives

takes our criticism seriously and the Berlin Data Protection Act - as already

terminated – evaluated and adjusted accordingly in this legislative period.

Meanwhile, data protection at the European level again gained strength

Tail wind from the ECJ decision "Schrems II", which the world economy in

excitement. In principle, according to the GDPR, personal

Data is only transmitted to third countries that have a data protection policy

level that is equivalent to the level of protection of the GDPR. For the US

However, the court found that US authorities had access options that were too far-reaching

possibilities on data of European citizens and subsequently tipped over

the so-called "EU-US Privacy Shield" as the basis for over-

transfers of personal data to the USA. This means that personal

Genetic data are usually no longer transmitted to the USA. The verdict has

ultimately announced nothing surprising, but only referred to the rules

provisions of the GDPR. But through the unequivocal clarification

In view of the legal situation, many European companies are now taking precautions

enormous challenges, even after the DS-

GVO US services and software used and on the EU-US Privacy

Shield as the legal basis. With its decision, the ECJ

made it clear that the Privacy Shield cannot stand before the DS-

GMO. It still has the basic right to informational self-determination

once considerably strengthened and made clear that there are economic interests

must not be subordinated – an important signal for all European

data-processing bodies, which have hitherto neglected the subject of data protection

treated physically and have an “it will be fine” attitude in this regard

have gained weight.

Foreword The administration must also adopt a different attitude and be aware

what data it processes and how this is done. Simultaneously

it must continue to open up to citizens. It is therefore extremely gratifying

that with the draft bill for a Berlin transparency law, the

amendment of the Berlin Freedom of Information Act to finally take shape

seems. The aim is to provide a comprehensive

broadcast right of access to official information and environmental information

to ensure and public bodies to provide independent of the application

of information in a transparency portal. Unfortunately he stays

current draft of the law falls far short of what is expected of a modern

transparency law back. The numerous planned area exceptions and

Restrictions on the obligation to publish limit the freedom of information

namely de facto, rather than expanding them. This means that the law runs the risk of

contrary to its original purpose, the development of a modern and

discouraging rather than promoting transparent administration.

Trust in state structures and in politics is the fundamental basis

for a peaceful and orderly coexistence. How important are these parameters

shows us the corona pandemic day after day. Even if some of us

think that data protection issues would take a back seat in these times

orderly role in our lives, we must not commit the mistake and

hide that this civil right also, no, especially in times of crisis

Good represents what it is imperative to uphold. data that can be processed digitally

are exposed to the risk of misuse. And data that once

fallen into the wrong hands can no longer be retrieved. In order to

those affected may have serious consequences for a lifetime

threatened.

Therefore, lowering the level of data protection cannot be the solution

to be accepted for short-sighted reasons of practicality. Neither is

the banishment of digital means from our everyday life is the solution, since they are

valuable tools, especially for the challenges of the Corona crisis

to master. Rather, the aim must be the development and use of

be right products. Digital solutions must be fundamentally rethought and

Digital technology must be designed in accordance with data protection from the outset. digital

talization and data protection are not opposites, but must be

 be brought to future-proof both for the optimal benefit of the people

close. My agency and I will continue to work towards this.

Berlin, April 8, 2021

Maja Smoltczyk

Berlin Commissioner for Data Protection and Freedom of Information

17

Foreword 18

Foreword 1 .1 Corona

1 focus areas

1.1 Corona

1.1.1 The Corona-Warn-App - data protection by

technology design

The Berlin Commissioner for Data Protection and Freedom of Information took part

on the development of a catalog of requirements for mobile applications

Tracking the contacts of people who have contracted Covid-19.

To combat the corona pandemic, a number of technical solutions

proposed. These should serve to provide information about the dissemination

of the pandemic, identify people who have been in contact with the sick

had, or to support the diagnosis. Within our jurisdiction

we advised those responsible for these projects, which often cost a lot

time pressure were developed and put into use.

A

and

s

i.e

e

right

P

right

a

x

i

s

A central strategy in limiting the spread of the corona virus

is to find infected people based on their personal contacts and

to prevent the infection from being passed on. It stands to reason that the capabilities of

To use smartphones for this, more than 80% of the over fourteen year olds

Carry with you: They have a number of sensors that can be used for detection

can be used by contacts.

The first approach was to use data about the location of the devices that

record many of the devices and often pass them on to third parties. A stay of

two people with smartphones at the same time in the same place is one

Contact. Of course it would be possible to use a large database

This data includes the whereabouts of a large proportion of the population

to be compared to determine possible sources of infection. Technically

this could be done efficiently. And indeed was in some East Asian

countries to do so. But from the point of view of civil liberties

19

From a civic perspective, that's not a good idea. Whoever the data

collects, receives an extremely deep insight into the lives of the people

their habits and social contacts, their interests and vices. Ultimately

This results in an immense power over those affected with a huge

potential for abuse. In addition, with this method, the location information

are often not precise enough to really create an epidemiologically relevant

to be able to determine meetings.

Thankfully, it quickly became apparent that alternative approaches were available that

avoid problems. Smartphones not only receive data, they send it

also. And not just via mobile communications or Wi-Fi, but also with radio

short range. The most common of these procedures, which

supported by the number of smartphones is called Bluetooth. It serves e.g. B. to

Connecting wireless headphones to your smartphone can also be used to

Transfer messages between two smartphones that are used

are close together.

In this way, all people who have been in contact with sick people can be informed

want to send a contact address via Bluetooth. smartphones nearby

can collect this contact information. Become their owners

diagnosed as infected, they can identify their contact persons based on the contact

inform data. This data does not have phone numbers, email addresses

or even postal addresses. A contact set up for this purpose

service from which smartphones can pick up messages is also sufficient. The-

z. B. the French system.

This method also provides that the contact service the probability

of an infection from the contact or contacts. To do this, he uses the information

about the frequency and length of contacts as well as the distance between the smart

phones (and thus their owners) during the contact. The-

This distance can be derived from the strength of the signal with which the smartphone

nes have received the respective signals.

But even in this system, the central contact service makes a big difference

amount of data on people's contacts with each other. Although not

about the place where they met or stayed,

and thus much less than when dealing with location data. But it will open-

laid who met whom. In addition, the information may be

be assigned to identifiable persons. can be prevented

this assignment only if the retrieval take special precautions

fen. However, only a few, particularly technically knowledgeable people are in the position to do so

Location.

To counter this, another idea was developed. It consists in the

Documentation of contacts between people on their smartphones

relocate Each person participating in the system broadcasts to everyone else,

whom she meets, a pseudonym via Bluetooth. The contact persons register

rate this. If the first person finds out that they are infected, then publish them

her pseudonym without mentioning her own name. Who this pseudonym too

had previously registered was in the vicinity of the infected person.

The smartphone therefore regularly retrieves the published pseudonyms and

compares them with the pseudonyms registered with them. If there is a hit,

the respective contact person is warned. Also an estimate for the

The smartphone can calculate the probability of infection through contact

and show. The same algorithm can be used as

it is run centrally in the French system.

The pseudonym is changed frequently. In the event of the publication of a

infection, all pseudonyms from the period in which the affected

ing person was infectious. This can be organized in a data-saving manner.

And without affecting the functionality of the app, it prevents people from

During their movement in public space, people are tracked using pseudonyms

who send their smartphones all around.

This approach was supported by our authority. He settled in Germany

and several other European countries.

The European data protection framework for the implementation

Data Protection Committee (EDSA)1 in a publication of guidelines with requirements

to the “Use of location data and contact tracing tools”

1 See Art . 68 GDPR

tion related to the outbreak of COVID-19”2. Added

This publication was replaced by a "Declaration on the consequences of data protection

of interoperability of contact tracing apps”3. In the development of

We were actively involved in the documents mentioned. Given the urgency

the committee worked in record time.

The EDPB first notes that participation in an electronic con-

clock tracking should be voluntary. He assumes that a data

protection-friendly, trustworthy and transparent implementation for acceptance

dance of the procedure contributes. For a system with high participation rates

gains significantly in effectiveness, this is an important factor.

In particular, the committee highlights the following:

• The legal requirement to minimize data processing and

restriction to what is necessary must be observed.

• In view of existing alternatives, processing of

Location data for the purpose of contact tracing the data protection basic

set.

• The system should only work with verified information about infections in order to

met not to alarm unnecessarily.

• The decision to release information about the infection of a

person must remain in their hands.

• In references to contact with an infected person, this person must not

to be called.

• Data that is no longer required must be deleted immediately, both on central

l servers such as on the smartphones of the citizens.

2

3

See https://www .datenschutz-berlin .de/infothek-und-service/veroeffentlichungen/

guidelines

See https://edpb.europa.eu/our-work-tools/our-documents/muu/statement-data-

protection-impact-interoperability-contact-tracing_de

In an appendix, the committee then presents concrete test criteria for the implementation

of the procedure together. These concern the embedding in the general

Conducting contact tracing, strictly limiting the use of the

data collected in the process to contact tracing, providing

ment of suitable information about the procedure for the users, the

of procedures and information technology used, as well as an evaluation

the effectiveness of the procedure.

The risks that are already associated with the permanent activation of

Bluetooth in the smartphones of the users are connected. There isn't one

insignificant number of smartphones that are operated with outdated software

because the manufacturers do not keep them for a sufficient period of time

away with updates. Therein lies a vulnerability

makes smartphones with activated Bluetooth vulnerable. Equally unhappy

is that Google, as the manufacturer of the Android operating system, is activating the

Bluetooth is linked to the activation of the location service and from the to this

the collection of location data made possible in this way. This deficit

must be countered with other means: legal standardization

the manufacturer's obligation to provide security updates and a control of the

Data processing by Google by the competent Irish data protection authority

supervisory authority.

In weighing all the advantages and disadvantages, including the risks mentioned

However, we keep the system of electronic contact practiced in Germany

clock tracking with the Corona-Warn-App for data protection and exemplary

for other digital projects of public administration.

When politicians, those responsible, manufacturers and supervisory authorities in their

respective roles cooperate constructively, can also under pressure

a major health system crisis such as the Covid-19 pandemic

data protection-friendly solutions are found that integrate the

population in an effective containment of the crisis, deep

However, avoid encroachments on people's private lives and protect the

guarantee the personal data processed.

23

1.1.2 CovApp - recording of Covid symptoms

in the web

s

i

x

a

right

P

right

e

i.e

s

and

A

We consulted together with our Brandenburg colleagues

the Charité in the use of a web-based tool for recording

Data on people undergoing a test for corona infection

want.

As with any medical service, a corona test must also

important information about the state of health of the persons to be tested

be collected. The time spent in the test center should be as short as possible

to be kept. It is therefore advisable to fill out the questionnaire in advance

To make available. If this is done in electronic form, the data transfer

particularly easy. The Charité took this path, supported by

a Brandenburg company that develops digital health solutions.

We drew attention to the CovApp project from Brandenburg

the technical implementation was reviewed and identified deficits were pointed out.

As the project was expanded over the year to include new functionalities

to offer, it was necessary to repeat the verification after some time.

Basically, the structure of the electronic questionnaire could not be

queuing. The Charité provides it as a web application (web app) as part of its

res general website available. Once loaded, the communicates

Web application initially no longer with the servers of the Charité, but saves

is carried out in several steps by questioning the patient or the pa-

clients collected data in the web browser. At the end, the data ends with a

simple algorithm evaluated and a recommendation for further

Procedure - taking the test or not doing it - pronounced. Comes

it to a test, the data from the Charité can be read by reading the display

of the web browser.

There were only problems in the details. The manufacturer of the web app wanted the

Track usage (not user input)—but that, too, is

only allowed with consent. Consent was obtained later

wear. In addition, the deletion of the data worked after completion

Survey not reliable. This is tricky because there is a risk that

other web offers that the patients visit, who read out the data. the

Although the function has been repaired, the deletion must be due to the procedure

continue to be actively initiated by users.

Finally, the Charité wanted to ask the patients to provide their

be released for research. However, the information for a

effective consent are necessary were not sufficient and

probably the roles of those involved as well as the purposes of the research are unclear.

This possibility of a “data donation” was eliminated later in the year

removed from the program and by taking over the data in symptom

replaced by booked apps on a voluntary basis. At least one of them saw their turn

forwarding of the data for research purposes.4

All in all, we were able to determine that the Charité with the CovApp has a practical

tikable solution that meets data protection requirements.

The electronic survey of patients can be done safely and securely

be designed to be data-efficient. transparency and technical diligence

of fundamental importance.

1.1.3 Handling contact lists for containment

the corona pandemic

We received a large number of complaints about restaurants, cafés, bars and other

their localities, where the guests enter themselves in openly accessible lists

4

We have no indication that the disclosure of anamnesis data to

research institutions for purposes of medical research is unlawful

took place . Consent was obtained in each case, the wording of which is currently being drafted

can no longer be understood, however, since the studies have now been completed and

no more data collection takes place. Incidentally, this data processing took place outside

within our area of responsibility, since the operators of the symptom diaries have their

Headquarters in Lübeck or . have Fribourg.

25

A

and

s

i.e

e

right

P

right

a

x

i

s

should. Only in one case was there an additional improper use of the

data collected in this way in space.

A central part of the containment of the corona virus is the

tracking of infection chains. So that health authorities

Chains can be tracked effectively, saw the infection control regulations

of the federal states in the reporting period regulations for the collection of contact data

before. In Berlin, the obligation to document attendance applies, among other things, to hotels and

gastronomic facilities.5

In addition to the first and last name, the documentation had to include the telephone number

mer and the district or municipality of the place of residence or the place of the permanent

tive stay included.6 In addition, either the full

Address or e-mail address of the guest, the time of attendance and - so-

widely available – to document a seat or table number and for that

Duration of four weeks after the end of the event or use of the

service.7 Because the collection of the correct data from

of crucial importance for contact tracing by the health

offices, the provision of false data is now also subject to a fine.8

In data protection practice, problems quickly arose with the

Implementation of contact data collection. We received numerous complaints

those of citizens who have publicly available collection lists in

restaurants and collecting data from multiple people at once

single contact form reported. So existed z. B. in addition to the knowledge

taking of the data by guests present also carries the risk that these lists

be photographed.

With the entry into force of the SARS-CoV-2 Infection Protection Measures Ordinance (InfSchMV)

from 14 . December 2020, which the SARS-CoV-2 infection protection

ordinance, the collection of contact data was due to the obligation to close

Many facilities can only be used to a very limited extent; see in particular

§§ 15, 16 InfSchMV.

6 § 3 para. 2 Sentence 1 SARS-CoV2 Infection Protection Ordinance (of November 3, 2020)

7 § 3 para. 2 Clause 2 SARS-CoV2 Infection Protection Ordinance (of November 3, 2020)

8 § 3 para. 3 SARS-CoV2 Infection Protection Ordinance (of November 3, 2020)

A collection of the data by means of paper lists that are openly accessible

are not in accordance with data protection regulations. The after the

Infection protection regulations required documentation of contact

data must be kept or saved so that it is protected from third-party

chert.9 Appropriate technical and organizational measures must be taken

Restaurants, cafes, hotels or other localities ensure that a

Access to personal data by unauthorized persons

closed is. The data must therefore be used from the start of running an application

health documentation recorded for each person on a separate sheet and

be kept safe.

The restaurants, cafés and bars we checked were based on the data protection

compliant handling of the contact lists and due to the

Disclosure of personal data to unauthorized third parties partially

warns. Only in one case was there improper use of the contact data, e.g.

for a newsletter of the restaurant in the area. We have this case on ours

handed over to the sanctioning body.

As part of the processing of the individual complaints, we were particularly

informed that the contact lists used in some restaurants on

based on a sample template from the Hotel and Restaurant Association (DEHOGA).

A query to DEHOGA has shown that the sample form is not

collection list was designed, but based on the recording of six people

aimed, who were at a table. Due to the fact that the

location could be misunderstood and the infection protection regulations of the

countries were designed differently, DEHOGA has the template

removed from their website again in May and the individual national associations

informed about it.

We have a sample form for contact tracing on our website.

published by companies, which we have published in accordance with the current

Update protection regulations continuously.10

9

§ 3 para. 2 Clause 2 SARS-CoV2 Infection Protection Ordinance (of November 3, 2020); please refer

also kind . 5 para. 1 letter f GDPR

10 See https://www .datenschutz-berlin .de/infothek-und-service/themen-a-bis-z/

corona pandemic

s

i

x

a

right

P

right

e

i.e

s

and

A

Through regulations to protect against infections with the coronavirus SARS
CoV-2 mandatory attendance documentation must be protected from
kept or stored for inspection by third parties. contact
ten forms that provide for the recording of several people or even open
are not permitted.

1.1.4 Only fever-free in the supermarket?

In connection with the Covid-19 pandemic, we received several inquiries
from companies that use electronic fever measurements as admission controls
wanted to do in supermarkets. It was planned to raise people with
body temperature to deny entry to retail stores.

We don't think this makes sense. Elevated body temperature can not
must inevitably be regarded as an indication of a SARS-CoV-2 infection. Many
Infected people have no symptoms and therefore no elevated temperature
on. Conversely, an elevated temperature does not necessarily indicate a
SARS-CoV-2 infection. In addition, milder measures such as B. the
maintaining the ventilation routine and the hygiene and distance regulations
containment of the pandemic more effectively. This also applies in particular to the
measures that are already common in retail, such as limiting the number of
Customers, the attachment of information signs on rules of conduct and
access restrictions, ensuring compliance with minimum distances,
the request to wear a mouth and nose protector, the attachment of

partition walls in the checkout area and at sales counters as well as the implementation

hygiene requirements. Such a package of measures is promising

also with regard to potential contagion through symptom-free and not

people identified as infected provide more sustainable protection for customers and

employees as an electronic collection of health data, which

are specially protected by law.11

From a legal point of view, an electronic temperature measurement that

is aimed at identifying people infected with SARS-CoV-2, only with

11 See Art . 4 no. 15 i . v. m . kind . 9 GDPR

Consent or permitted on the basis of a legal regulation.12 The

Obtaining corresponding consent from all customers should not be allowed

be practicable or even counterproductive if the procedure of

declaration of consent and the temperature measurement would lead to longer queues.

Statutory regulations, to which a corresponding fever measurement in individual

trade could be supported do not yet exist. However, the

General Data Protection Regulation (GDPR) Scope for national legislation

Exercise to regulate the collection of health data in certain areas.13

Before the above However, we believe that there is a corresponding regulation at least

at least not useful at this point in time.

Together with the federal data protection supervisory authorities and the

We have instructed their countries on the use of thermal imaging cameras or electronic

temperature recording in the context of the corona pandemic, indications

works, which can be accessed on our website.14 Find there

There is also further important information on the use of thermal imaging cameras

in other areas, such as B. in airports, authorities and workplaces.

1.1.5 Dealing with the obligation to wear masks in schools

With the introduction of the obligation to wear a mouth and nose cover in the

Schools have new privacy issues related to

resulting from the corona pandemic. So after the introduction of the mass

compulsory in schools, a large number of inquiries from concerned parents. they wanted

have their child exempted from the mask requirement and asked to what extent

School may request the submission of a medical certificate and what information

should be included in it.

A

and

s

i.e

e

right

P

right

a

x

i

s

The obligation to wear a mouth and nose cover results from the

The SARS-CoV-2 Infection Protection Measures Ordinance in force in Berlin

12 See Art . 6 para. 1 sentence 1 i . v. m . kind . 9 para. 1, 2 GDPR

13 See only Art . 6 para. 1 sentence 1 lit. c, para. 2, 3i . v. m . kind . 9 para. 2 letters g-j GDPR

14 See https://www .datenschutz-berlin .de/infothek-und-service/veroeffentlichungen/

version as amended.15 An exception to the obligation applicable in schools
to wear a mouth and nose cover applies to people who, due to a
medically certified health impairment, a medically certified
chronic illness or disability, no mouth and nose
cover.16 In the case of a medical certificate and the documents contained therein
Information is sensitive health data belonging to the categories
categories of personal data with special protection. Her
Processing is only permitted if the data subject either (voluntarily, internally
formed and expressly) consents or if the processing is based on a
legal regulation is permissible.17 The DS-GVO as directly in the EU
The law applicable in the member states permits processing if this is for reasons
those of public interest in the field of public health, such as B.
protection against serious cross-border health risks,
on the basis of a legal requirement that satisfies certain requirements
regulation is required.18 For schools, the authority to present credibility
to have a certificate submitted for verification of a reason for exemption, in particular in the
SARS-CoV-2 Infection Protection Measures Ordinance i. V. m. the school law
(School Act) regulated.
The question of whether a medical certificate contains specific health information
must hold depends on whether this is necessary to achieve the purpose
is. The purpose of the mask requirement in schools is to prevent the infection of pupils
ners and teachers (and thus also the further spread of the infection in
of the population) under the special conditions of a community
prevent direction. The school management is responsible for

to decide on an exemption from the mask requirement. Your must be the reason for that

Exemption can be made credible with the help of a medical certificate. Since it is

15 Since 14 . December 2020 is not the name of the ordinance and its amendments

more SARS-CoV-2 Infection Protection Ordinance, but SARS-CoV-2 infection

protective measures ordinance .

16 § 4 para . 3 no. 2 SARS-CoV-2 Infection Protection Measures Ordinance (as amended

from 14 . December 2020) . While the requirement for a medical certificate itself beforehand

etc. from the spirit and purpose of the regulation, effective protection against infection

ensure revealed this is since the 10 . version of the SARS-CoV-2 infection control

ordinance expressly regulated .

17 art. 4 no. 15 GDPR; kind . 6 para. 1 GDPR; kind . 9 para. 1, 2 GDPR

18 art. 9 para. 2 letters i) GDPR

the exemption is an exception, the statement is sufficient

general impairments that can occur in all students,

not from. Rather, the certificate must contain an individual

impairment of the person concerned are presented. That's why it's in the

Usually required that specific information about previous illnesses or current

Special features are made and it is explained what the disadvantages are

individual impairment through wearing a mask in possible relevant

possible scenarios in school. That's the only way the school board can do that

as the responsible body, an appropriate decision on the exemption from

meet the mask requirement.

The situation is different than, for example, when you are on sick leave, in which

the diagnosis is not listed. Because when you are exempt from the mask requirement

are also the basic rights positions of the other students and the school

personals, such as the right to life and physical integrity.

The state's duty to protect applies in the school context in a special way, since pupils

due to the general compulsory education, pupils have no choice to enroll in school

classes (with or without a sufficient minimum distance) or not.

According to the decision of the school management, it is usually not necessary and

it is therefore also not permissible for the school to keep a copy of the certificate.

Rather, the school management should present the credibility in a separate

advise document confirm without this endorsement health claims

contains. Teachers may only use the

Receive information that a reason for exemption has been made credible.

Schools are entitled to ask themselves to substantiate a reason for exemption

to have a medical certificate submitted that refers to the specific health

situation of the person concerned. Keeping a copy of the

A medical certificate, on the other hand, is not required and therefore not permissible.

1.1.6 "Please cover your mouth and nose" - control

powers of transport companies

s

i

x

a

right

P

right

e

i.e

s

and

A

In order to contain the corona pandemic, in recent months

various measures by the regulators of each

states decided. Since April there has been an obligation to wear a

ner mouth and nose cover in Berlin subways, trams and buses

sen and in the S-Bahn. Not infrequently you could find people without such

Face a mouth and nose cover in local public transport (ÖPNV).

Since for certain groups in the case of health impairments

If there are any exceptions to the mask requirement, this must be

to prove evidence. A particular challenge is

the mask requirement i. s.d. To enforce protection against infection and at the same time

Proof of an exception to protect the personal data

Zen.

The SARS-CoV-2 Infection Protection Measures Ordinance stipulates wearing a

ner mouth and nose cover, especially in public transport

Train stations, airports and ferry terminals and in other vehicles where

different passengers are staying, before.19 An exception applies, among other things, to persons

those due to health impairments, chronic diseases

or a disability are unable to wear a mask.20 For people who rely on

the respective responsible persons have invoked this exception in their rooms

the right or obligation to have a medical certificate presented.21

In public transport, the domiciliary rights of each

respective transport operation to bear. That's how it is in the case of the Terms of Use

of the Berliner Verkehrsbetriebe are not permitted to go out without a mouth and nose cover

to stay in the means of transport, unless this obligation is no longer applicable due to

19 § 4 para . 1 no. 1 SARS-CoV-2 Infection Protection Measures Ordinance (as amended

from 22 . December 2020)

20 § 4 para. 3 SARS-CoV-2 Infection Protection Measures Ordinance (as amended by

22 . December 2020)

21 See Art . 6 para. 1 sentence 1 lit. e, type . 9 para. 2 letters i GDPR i . v. m . § 4 SARS-CoV-2 infection

Protection Measures Ordinance (as amended on December 22, 2020)

of the exceptions provided for by the applicable SARS-CoV-2 ordinance.22

In the event of violations of the obligation to wear masks on public transport, the usage

a contractual penalty of EUR 50.00. In addition, the

regulations refer to domiciliary rights, according to which, in the event of violations, house expulsions, house

or entry bans and carriage exclusions are issued

be able.

The SARS-CoV-2 Infection Protection Measures Ordinance does not

strongly prescribed that the facts leading to an exception of

the obligation to wear a mouth and nose cover made credible

Need to become. However, the requirement for proof arises from both

the meaning and purpose of the SARS-CoV-2 Infection Protection Measures Ordinance,

to ensure effective protection against infection, as well as from the legal

Principle that those who rely on an exception, the existence

of such an exception. The respective person responsible

it must be made possible for this to verify the authenticity of a corresponding certificate

to check and to be able to assign it to the person presenting it. On the other hand, for

the fulfillment of the test obligation the knowledge of the medical diagnosis, which the exemption

ung from the mask requirement is not required.

Citizens who, due to a health impairment

are exempt from wearing a mouth and nose cover can therefore

the diagnosis on which the exemption is based in the medical certificate

Blacken if this serves as a template for local public transport.

22 § 3 of the usage regulations of the Berlin transport company

33

1.2

International data traffic after the

"Schrems II" decision of the Euro

European Court of Justice

s

i

x

a

right

P

right

e

i.e

s

and

A

With its judgment of July 16, 202023, the European Court of Justice (ECJ)

the "Privacy Shield" for the second time special regulations for the transmission

personal data to the USA has been declared invalid. The EU Com-

mission issued standard contractual clauses for data exports to third countries

remain valid, but can export data on their own

no longer justify. This means, for example, that US American

Cloud services by companies and authorities only in special

cases permitted.

Austrian Maximilian Schrems' complaint against the transfer

his data through Facebook to the USA was the subject of this for the second time

a fundamental decision of the ECJ. That has now been declared invalid

"Privacy Shield" agreement was developed as a follow-up to the 2015

if, following a complaint from Mr Schrems, invalidated24 “Safe

Harbor Agreement.

The “EU-U.S. Privacy Shield" provided - similar to the "Safe Harbor" regulations -

that US companies register in the so-called "Privacy Shield" list and thus

to comply with certain data protection regulations.

The US government also made a number of promises on data protection at official

common access to personal data. through an adequacy

conclusion of the EU Commission, the "Privacy Shield" was therefore the basis for

Justification for transfers of personal data to US companies

been recognized.25

23 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II"

24 ECJ, judgment of 6 . October 2015 - C-362/14, "Schrems I"; see JB 2015, 14.1

25 Commission Implementing Decision (EU) 2016/1250 of 12 . July 2016 according to the

Directive 95/46/EC of the European Parliament and of the Council on the appropriate

security of the protections provided by the EU-US Privacy Shield (announced

under case number C(2016) 4176); see JB 2016, 1.1

Chapter 1 Key points 1 .2 International data traffic after the “Schrems II” decision of the ECJ

In its judgment "Schrems II", the ECJ now analyzed in detail the legal

location in the USA and presented with various, each individually already

sufficient justifications that the level of data protection in the USA is not

meets the requirements for a permissible data export.26 Because the

tem law gives the US authorities unrestricted surveillance powers

data subjects, on the other hand, have no guarantees of their rights.27

The supervisory powers of the US authorities therefore violate the

principle of moderation.28 In addition, affected persons have no judicial rights whatsoever

Legal protection against US authorities.29

The standard contractual clauses drawn up by the EU Commission can

towards justifying data exports.

be pulled. However, this means that only at the level of civil law the

NEN data export necessary guarantees created, because a contract between

Data exporter and data importer can be the authorities of the respective third country

not bind. If you want to continue using the standard contractual clauses, you have to

therefore in future the legal system and practice of the third country with regard to a

possible access by the authorities of this country to the transmitted personal

Check related data.30 Only if for the exported data also regarding

possible access by the authorities, the required level of protection is given

Standard contractual clauses for the necessary data protection. If this - as in

case of the USA - is not the case, the guarantees in the standard contractual

clauses can be supplemented by additional measures.31

If no additional measures can be found that would

Eliminate gel in the third country, data exports must be avoided and ex-

ported data is retrieved.32 An obligation to suspend or

The data export is terminated in particular if the right of

respective third country the data importer obligations z. B. regarding the

26 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 185, 191, 197ff.

27 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 180, 183

28 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 184

29 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 181, 182, 192

30 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 104

31 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 132f.

32 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 135, 140

right of access imposed on the authorities of that third country to the data held by the

contradict standard contractual clauses and which are therefore suitable for

to undermine the contractually agreed guarantee of an appropriate level of protection

ben.33

We immediately analyzed the consequences of the ECJ judgment "Schrems II".

and the data-processing offices in Berlin on the day after the verdict was

requested to transfer personal data stored in the USA according to EU

to relocate ropa, unless the data processing in the USA is exceptional

is permissible, in particular in the special cases provided for by law.34

The European data protection supervisory authorities have - under our

participation - recommendations drawn up as to how those responsible and

contract processors who transfer personal data to third countries

want to proceed.35 In addition to a step-by-step

step-by-step instructions also conceivable supplementary measures to eliminate deficits in the

To equalize data protection levels in the target country of the data export.

The procedure required for the examination based on the case law of the ECJ

of data exports to third countries for which no decision by the EU Commission

on the adequacy of the level of data protection exists,36 is very complex.

Data exporters must - if necessary in cooperation with the data importers -

assess whether there is anything in the third country's legislation or practice,

which could affect the effectiveness of the agreed guarantees. Is this

the case, for example because authorities in the third country have disproportionate access rights

have access to the processed data, additional measures must be taken

33 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 135, 140

34 press release of 17 . July 2020, see https://www .datenschutz-berlin .de/fileadmin/

user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_

Autonomy .pdf

35 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to

ensure compliance with the EU level of protection of personal data; retrievable and

ter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-

recommendations-best-practices_en

36 The EU Commission publishes a list of adequacy decisions at

https://ec .europa .eu/info/law/law-topic/data-protection/international-dimension- data-

protection/adequacy-decisions_de

will. To answer the question of which access rights are disproportionate

are appropriate, the focus should be on European fundamental rights.37

if e.g. B. as in the case of the USA with providers of electronic cloud and communication

communication services disproportionate access rights of the authorities of the third

countries insist on the data to be exported, the additional measures

assumed to be of a technical nature only. 38 These measures must prevent

the authorities of the third country can access the data at all,

or at least that they can do something with this data.39

is that other recipients who are not themselves providers of electronic

ronic communication services within the meaning of US law, indirectly such

may be subject to disproportionate access rights, namely when they

data transmitted to you by a provider of electronic communication

process services.

In the case of the USA – and other third countries with disproportionate regulatory requirements

Access rights - this means that, for example, the use of local IT service providers

as cloud providers is only permissible in very few cases. But also on

their recipients can be problematic - not only if they themselves

Subject to government access, but because many companies use cloud services

and are thus indirectly subject to surveillance.

The use of US cloud services to store personal data

can e.g. B. come into consideration if this data is encrypted in such a way that

that over the entire length of time they must remain confidential

37

In particular Art. 47 and 52 of the EU Charter of Fundamental Rights; see also EDSA,

Recommendations 02/2020 on the European Essential Guarantees for surveillance

measures; available at https://edpb.europa.eu/our-work-tools/general-guidance/

gdpr-guidelines-recommendations-best-practices_de

38 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to

ensure compliance with the EU level of protection of personal data, Chapter 2 .3, Rn . 44;

Chapter 2 .4, Rn . 48; available at https://edpb.europa.eu/our-work-tools/general-

guidance/gdpr-guidelines-recommendations-best-practices_de

39 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Chapter 2 .3, Rn . 44; available at https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guide-lines-recommendations-best-practices_en

37

Decryption by US authorities can be safely ruled out.40

In addition to various complex technical requirements, this requires, among other things, that the key required for decryption never crosses the area allowed, in which there is an appropriate level of data protection. Because he is US cloud providers in possession of the key, the authorities there cannot only request the release of the encrypted data, but also the return of the key. Exceptionally, under strict conditions unencrypted pseudonymised data can also be exported, for example for research purposes.41 Pseudonymisation must be designed in such a way that that it cannot be overridden in the United States, even by linkage with other information.

However, it should be noted that in the typical use cases of Services that US companies offer, regular access to clear data is required. In such cases are not sufficient supplementary Measures conceivable.42 In particular, other measures such as a contractual obligation of the data importer, against production orders to complain, not. Data exports are not permitted in such cases, already exported ted data must be retrieved immediately.43

40

41

42

In detail about the requirements: EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Appendix 2, Use Case 1, Rn . 79; available at https://edpb .europa .eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

In detail about the requirements: EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Appendix 2, Use Case 2, Rn . 80; available at https://edpb .europa .eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

In detail to the requirements EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Annex 2, Use Case 6, Rn . 88; available at https://edpb .europa .eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

43 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Chapter 2 .4, Rn . 52; available at https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

In the case of the USA, this applies e.g. B.

• Communication services such as email, video conferencing, messenger, web and Shop hosting, integration of third-party content on your own website, in the usually also the defense against (dDoS) attacks,

• Services for managing relationships with customers (Customer Relations management), for personnel administration, for project management or for Management of requests (ticket systems),

• Services for distributed collaboration, such as joint editing

of text documents, presentations, spreadsheets,

• Services for synchronizing data between different devices, data

file storage, calendar and task management services,

• Directory and other services used to authenticate people

are used and contain data about them,

• Service providers who carry out the verification of ID cards, driver's licenses and other

other documents.

The new standard procedures provided by the EU Commission as a draft

tragsklauseln44 – we work together to comment on and improve them

involved with other European supervisory authorities - change this one

Problem nothing and can not, because of contractual regulations

which the foreign authorities are not involved cannot bind them.

How the “Schrems II” judgment affects other legal bases for data exports

such as binding internal data protection regulations (Binding Corporate Rules, BCR),

codes of conduct, certifications and individual approvals

currently unclear. The same applies to the question of whether US companies or their

44 See https://ec .europa .eu/info/law/better-regulation/have-your-say/ initiatives/12741-

Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-

transfer-of-personal-data-to-third-countries

European subsidiaries or other US related companies

be subject to US surveillance laws when sharing data

not processed in the USA, but in the EU. Also in these discussions

and exams, we participate intensively.

However, the judgment "Schrems II" is very clear with regard to the consequences

siger data exports: comes a supervisory authority at the end of their investigation

to the conclusion that the data subject whose data is transferred to a third country

were communicated does not enjoy an adequate level of protection there, it shall be

Union law obliges to respond in an appropriate manner to the established

to remedy the inadequacy - regardless of which origin and which

of what nature the inadequacy is.45 From this, the ECJ concludes an obligation

the respective supervisory authority, a transfer of personal data

to a third country without granting a transition or adjustment period

to impose or prohibit,46 if in the light of all the circumstances of the concrete

Data transfer believes that the standard data protection clauses in

are not or cannot be complied with in this third country

and that the protection of the data transmitted is required by Union law

cannot be guaranteed by other means.47 The only exception to the

Obligation to issue such a ban is the situation that the data

exporter has already suspended or terminated the transfer itself. such

Incidentally, illegal data exports are also threatened with fines. 48

The examination of transfers of personal data to third countries for which

there is no adequacy decision by the EU Commission is initially one

Challenge for data exporters. But it is also a challenge

for the supervisory authorities, who in turn check these tests themselves and

may have to prohibit data exports. This challenge that the ECJ

derived from the fundamental rights of people in the European Union

we us.

45 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 111

46 See Art . 58 para. 2 letters f and j GDPR

47 ECJ, judgment of 16 . July 2020 - C-311/18, "Schrems II", para. 113, 121, 135, 146

48 See Art . 83 para. 5 lit. c GDPR

Chapter 1 Focus 1 .3 Use of video conferencing systems

The transfer of personal data to third countries without
The appropriate level of data protection recognized by the EU Commission
performed and precisely documented checks by the data exporters
out. EDPB recommendations are available for this. Depending on the result
Additional measures may have to be taken before the test is completed. Lies
the data protection problem of the third country (also) in disproportionate
Appropriate official access rights, only technical measures come into play
Consider, which exclude the access of the authorities or the data for the
render authorities useless. Such measures are currently only available for very few
some use cases. Therefore, the use of the vast majority of US services
ter is inadmissible and cannot be made lawful at the moment. ver
responsible persons who use such service providers directly or indirectly must
retrieve processed data immediately.

1.3 Use of video conferencing systems

As a result of the pandemic, the number of people working in home jobs has increased
are, multiplied. Schools also closed and relocated part of their business
lessons in the digital space. Under these conditions, video conferences are
an important tool for maintaining communication. We he-
held a large number of inquiries and complaints on the subject. Around
to be able to help as far as possible, we have in addition to the direct
Advice for those responsible and providers, including general recommendations
published for users.

A

and

s

i.e

e

right

P

right

a

x

i

s

Video conferencing offers significant added value for communication

the telephone. The need for them under the conditions was correspondingly great

of working from home and school closures. offers in particular

US providers flooded the market. Your claim is available

However, this often contradicts data protection law. But also with the

offered by European providers, we had to find some extensive shortcomings.

In a constructive exchange with a large number of providers, we were able to

achieve improvements on both a legal and technical level.

41

In principle, those responsible can set up video conferences in two ways-

place:

Firstly, they can operate the necessary information technology themselves –

either by providing the service in-house or by

drove in an external data center. The necessary software is available on the market

and can be adapted by those responsible to their needs.

It should be pointed out that data protection is possible through technology design

is. But only large institutions can afford the necessary expertise

ready.

The second variant consists in hiring a service provider who

does all the work. He inevitably comes up with a variety of personal

related data in touch: data on the conduct of the conference and

the participants, audio and video recordings of the conference itself, possibly

happily also text messages between the parties involved and documents that

to get presented. The content of the communication can also vary

relate to third parties. In any case, all this data says a lot about the partici-

coming persons themselves.

Therefore, those responsible must ensure that the data is lawful

are processed. This becomes difficult if the data is stored outside the EU in a

be processed in a country such as the USA, which does not have adequate data

protection for EU citizens guaranteed. In its ruling, the ECJ

part "Schrems II" set high requirements. 49 In fact, many providers

of video conferencing services based in the United States. It is also problematic that

quite a few providers reserve the right to collect data about the use of their services for their own use

processing purposes. Those responsible are not allowed to allow this on a regular basis.

49 See 1.2

We have systematized these requirements and included them in a handout

Checklist presented in more detail.50

As a challenge, especially for small and medium-sized managers

the necessary examination of the order processing contracts of the providers of video

deoconferencing services exposed. To support those responsible

we have the results of our supervisory and advisory activities

ness, tests were carried out on offers that offer video conferencing as software-as-a-

service (SaaS) 51 published.52 We focus on

the assessment of the legal conformity of the services offered by the providers

Contract processing contracts laid because without legally compliant order processing

ment contract, use by those responsible within the scope of the DS-

GMO is excluded. If there are no legal defects in a short test

could be determined or the providers eliminated the identified deficiencies and

provided us with information or test access, also took place

a cursory examination of some technical aspects of the Services.

As a result, we were able to use five services in the first version of our hints

provided with a "green light" on the legal level, which under consideration

certain technical and organizational conditions are used in accordance with the law

can become. With a “red traffic light”, on the other hand, we primarily had to

Evaluate offers from US companies or their EU subsidiaries. the

However, problems were not only encountered with illegal data exports to the USA

50 Berlin data protection officers to conduct video conferences during the

Contact restrictions: https://www .datenschutz-berlin .de/fileadmin/user_upload/

pdf/orientation aids/2020-BlnBDI-Recommendations_Videoconferencingsystems .pdf;

Checklist for conducting video conferences during contact restrictions

conditions: https://www .datenschutz-berlin .de/fileadmin/user_upload/pdf/orientation-

hilfe/2020-BlnBDI-Checkliste_Videokonferenzen .pdf

51 With Software-as-a-Service (SaaS), the provider operates the servers and the software for

the respective service. Users only get access to the services of this

service, usually just the interface that is often displayed in the web browser. It deals

is a typical cloud service. In contrast, users acquire

or . their institutions in the classic software and server model and operate them

software itself.

52 Notes for those responsible in Berlin on providers of video conference services: ht-

tps://www .datenschutz-berlin .de/fileadmin/user_upload/pdf/ orienteering aids/2020-

BlnBDI-Notes_Berliner_Responsible_to_Providers_Videoconferencing-Services .pdf

to do, but also with very fundamental violations of the European

Privacy. These included z. B. partially extreme restrictions of

Providers' obligation to provide information regarding the fulfillment of their contractual obligations

obligations or the control rights of those responsible. those responsible

Use current services not only violate the legal regulations

Order processing53, but can also be subject to their statutory accountability

not comply with duty54. In addition, they deny themselves the possibility

to relieve oneself of claims for damages by data subjects. 55

Our information was met with enormous interest by those responsible. we

also received a large number of inquiries from suppliers who sell their products

also wanted to be included in the list. During the year led

we have many constructive discussions with both vendors whose products we

identified deficiencies, as well as with new providers and were thus able to

Significant improvements in the legal regulations and on the technical

reach page of products. At the end of the year, a total of eleven providers in the

intensive exchange with us, their contracts have been adjusted in such a way that we can

could evaluate gel-free. The order processing contract of another

bidder was now free of defects in itself, but saw inadmissible data exports

the USA before, which, however, when using the service under certain

conditions avoided. A (US) provider had improved its contracts

sert that in addition to the problem of data exports only the - by the

Provider irremediable – defect remained that he could

unlawful access by US authorities to the data processed by it

data could not be ruled out.

When checking the order processing contracts, we had to repeatedly

find similar deficiencies. In order to ensure that those responsible also

We therefore have to support bidders that we have not checked ourselves

53 See Art . 28 GDPR

54 See Art . 5 para. 2, art. 24 para. 1 sentence 1 GDPR

55 See Art . 82 para. 3 GDPR

typical defects are summarized and published.56 Of course, these can be

also be used by providers and their legal advisors to

sluggish to examine themselves for easily avoidable defects.

Care is also required in the technical design. The data transfer

must be sufficiently secure. Normally, only those invited should attend the

conferences can attend. The software necessary for the conferences

should not have any gaps that can be attacked and exploited by third parties

be able.

If a larger number of participants take part in the conferences, which

have different tasks – teachers and learners, for example – then

the software must be able to map these roles. Who moderates a conference,

needs the rights to allow a participant to speak or that

to withdraw the right to speak, to allow the presentation of documents or to

prohibit and remove uninvited guests from the conference. Also recordings

to produce sound and images - provided there is a legal basis for this

in the hands of the conference organization.

On the other hand, neither the moderator nor third parties should peek

into the private world of the participants. It should be the decision

of the participants remain, when they switch on the camera and microphone and when

Not. However, many providers do not comply with this legal requirement.

set, instead joining a video conference is often compulsory

wise with activated camera and/or activated microphone.

After all, only the data should remain from a video conference after it has ended.

remain that are still needed. This can information about the conference

and their participants, log data, recordings of the chat or also

be recordings. Are they no longer needed or is the legal basis for

their processing ceases at the end of the conference, they are to be deleted.

56 Recommendations for reviewing data processing agreements from providers of

Video conference services: https://www .datenschutz-berlin .de/fileadmin/user_upload/

pdf/orientation aids/2020-BlnBDI-Recommendations_Test_Order Processing-

contracts_video conference services .pdf

45

Against the background of our own examinations, we also have on

the preparation of a guide for the Conference of Data Protection Supervisors

federal and state authorities (DSK) on the topic57.

Video conferences are important tools of our everyday work and ours

become educational institutions. The choice and design of the used

Video conferencing service must meet the data protection requirements

consider. This requires careful consideration and planning. We have

Various assistance is provided on our website for this purpose. the

The selection of offers that can be used in accordance with the law is now so high that it

there is no longer any justification for continuing to use services that are against

violate data protection law.

1.4 Digitization of schools – BER 2.0?

s

i

x

a

right

P

right

e

i.e

s

and

A

With the start of the corona pandemic and the widespread

The significant deficits in the

Digitization of schools apparently. The past few months have clearly

shown that the state of Berlin has failed for many years to provide the necessary

to take measures to educate students and their teachers

to put digital learning into practice. Next to everyone

practical problems, a halfway functioning learning by means of digital

ler to enable tools inside and outside of school at all,

we had to realize that there was also a failure to comply with data protection regulations

to consider the design of the environments used. It's him-

sobering to have to state that in view of a now many months

nate ongoing pandemic and again necessary school closures also for

At the end of 2020, no positive balance can be drawn. On the contrary:

Some of the deficits identified in the spring remain unchanged. On

Many schools still use digital learning tools that

57 Orientation guide for video conferencing systems and checklist for data protection in video

conference systems; both available at https://www .datenschutz-berlin .de/info-

library-and-service/publications/orientation aids

are not compatible with the applicable data protection law and otherwise

the digitization of schools is progressing very slowly.

With the precautionary measures to contain the corona pandemic,

in all areas of life necessary restrictions the students, but

also the teachers and parents in a special way. The schools were ahead

Challenge with the students and teachers from one day to the

to organize lessons at a distance for others, mostly without

to be equipped with suitable instruments. Convinced that the pandemic

only accelerated the change that was already pending in this area

we follow the developments very intensively throughout the year. We have this

done in the conviction that the digitization of schools can only be successful

can be rich if data protection is taken into account from the outset –

even if this was initially only under the enormous pressure to act due to the pandemic

could be implemented to a limited extent. From our point of view, however, it was fundamental

meaning that the requirements of data protection are not lost sight of

advised in order to at least be able to improve them as quickly as possible. Then

in the digitization of school lessons, data from children and young
processed, which are under the special protection of the DS-GVO. A
Misuse of this data can have serious consequences for those affected
lead.
So in the first wave of the pandemic we have no sanctions whatsoever
taken if non-data protection-compliant digital teaching materials were used,
but have dedicated ourselves exclusively to the intensive consultation of those affected
and our advice to the responsible Senate Department for Education
education, youth and family offered again and again. At the same time we have very
pointed out early on that the use of appropriate tools with
considerable dangers for the personal rights of the students on the one
one side, but also the teachers on the other side.
In contrast to analogue school lessons, the use of digital learning
platforms offer a variety of data. There is a risk that just private
Providers evaluate the usage behavior of the students very precisely and for
own economic purposes. There are also missing delete functions
the danger that information no longer required for pedagogical tasks

information remain stored permanently and are later disadvantageous for the students
be used. At least since the decision "Schrems II" of the ECJ58
is the admissibility of the use of offers from US providers
to be examined particularly critically. If providers for data transmissions
through their products B. still refer to the "US Privacy Shield", the
was declared invalid by the ECJ, these cannot be used in the school context
come into action.
We have repeatedly pointed out that digital learning environments

must be designed in accordance with data protection regulations. This is because of that
of fundamental importance because it gives the necessary trust to all those involved
can be built up in the use of digital offers. The multitude of
The inquiries we receive in connection with this shows us that on the part of
school administrations and teachers there is great legal uncertainty, which
che offers can be used without hesitation in terms of data protection. loading
Complaints from parents show that there is a great deal of concern about being too lax
with the personal rights of the students in the schools.
In order to offer initial assistance, we already have information at the beginning of April
on the data protection-compliant use of digital learning platforms
licht.59 It was important for us to give school management and teachers criteria for the
hand, which should make it easier for them to recognize which offers
can be used in the design of the lessons in compliance with data protection regulations.
With the corona pandemic, there was also a high demand for in all areas
conducting video conferences. We have detailed instructions for
Responsible for the use of video conferencing services developed and published
fentlicht.60 Of course, these tips also apply in the school context.

58 See 1.2

59 Information on the data protection-compliant use of digital learning platforms
in class: https://www .datenschutz-berlin .de/fileadmin/user_upload/pdf/
orientation aids/2020-BlnBDI learning platforms_notes .pdf

60 Notes for those responsible in Berlin on providers of video conferencing services:
https://www .datenschutz-berlin .de/fileadmin/user_upload/pdf/orientation aids/
2020-BlnBDI-Notes_Berliner_Responsible_to_providers_ Videoconferencing-
Services .pdf; see also 1.3

Chapter 1 Priorities 1 .4 Digitization of schools – BER 2 .0?

The school management and teachers are tasked with ensuring data protection

with the quality of individual products is regularly overwhelmed. This is understandable

because it is technically and legally extremely complex

A task that goes far beyond examining pedagogical aptitude. we

see the education administration as having a duty to provide appropriate offers both

in educational terms as well - according to the regulations of the also for the

School area applicable DS-GVO - with regard to compliance with the requirements

to check data protection and data security and to give the schools a

to provide suitable pre-selection. It is necessary that the

education administration defines clear guidelines as to which digital teaching and learning

tel can be used by the schools and the teachers are legally secure

Offers submitted. The repeatedly cited by the education administration

ten concerns that a list of data protection-compliant products could result from legal

Reasons will not be created and would otherwise be included in the Education Act

guaranteed freedom of teaching and learning materials61 is incomprehensible. It

it goes without saying that teachers can decide for themselves which school

books are, from their point of view, pedagogically suitable for their lessons and

are to be used. However, the situation is different for digital offers

that the teacher not only has to decide on the pedagogical suitability,

but is at the same time obliged to ensure the data protection conformity of the

each product from a legal and technical point of view. the us

extensive feedback shows that the teachers are not in their

see educational freedom restricted, but rather support

tion in the selection of suitable and legally compliant digital products as well as

want clear guidelines.

Unfortunately, we had to find out throughout the year that the Senate Administration
for education, youth and family their task to give the schools the necessary
giving support is not fair. Our authority was in the necessary
gene process of designing the school offers in accordance with data protection regulations
also insufficiently included. As the following examples
clear, was the professional support we repeatedly offered
only partially and then only very hesitantly accepted.

61

In particular § 7 para. 2 SchoolG

1.4.1 "Berlin learning space"

The “Lernraum Berlin” project has existed since 2005. An integration
This authority was not involved in the project at any time. With the school
ments in March, the “learning space Berlin” suddenly got a very significant
importance for the maintenance of teaching at a distance. Since we
Shortly before the start of the corona pandemic, information about the project and
associated data protection deficiencies, such as B. a missing client
capability62 and missing deletion routines, we had un-
documents are requested from the responsible Senate administration in order to have an examination of the
to make an offer. Unfortunately, the education administration reacted to this in several ways
Months not, so that we send a reminder to send the documents in the summer
had to, but at the same time offered our advice again. Us
it was about getting rid of it as early as possible during the summer holidays
of any deficiencies and in the implementation of data protection compliant
Offer necessary requirements could have been worked. The first
The documents submitted to us confirmed the existence of significant defects

in relation to compliance with data protection and data security. We have-

be given comprehensive instructions for remedying the defects and are with us

unfortunately only since the end of the summer holidays with the for the project "Lernraum

Berlin" those responsible in a very constructive exchange.

We welcome the fact that the educational administration has entered the "Berlin learning space".

own, state-operated learning management system for the digital

teh provides. Due to the intensive exchange in the past

In the last few months, significant improvements have been achieved, so that we

"Lernraum Berlin" is now on the right track. It could be between

in terms of time, the lack of an existing legal basis for the processing of personal

ment-related data when using digital teaching and learning materials

necessary declaration of consent for the use of the "Lernraum Berlin"

be worked. It now complies with data protection requirements.

Since the "Lernraum Berlin" also offers the possibility of carrying out video

62 When designing systems, care must be taken to ensure that these, insofar as they are

other responsible parties (e.g. schools) run on one and the same server, so

are designed so that only authorized persons may access their own data

and mutual access is excluded.

conferences, we particularly welcome the fact that the education administration

the previously integrated video con-

reference solution through a data protection-compliant solution using the Open

Source software replaces BigBlueButton.

We will continue to support the development of the project in 2021.

1.4.2 Digital devices for the disadvantaged

Pupils and so-called summer schools

Many students have experienced significant disadvantages as a result of the school closures.
suffered, e.g. B. because they have the necessary equipment with appropriate
Terminals were lacking. The procurement of devices for the students concerned
lers is of course welcome, so that they do not fall behind
to lose. The implementation of so-called summer schools in the summer and
Autumn break was very useful to give the students the opportunity to
catch up on missed lessons.

However, in the whole process we had to show a lack of sensitivity
quality of the education administration with regard to the data protection concerns of the
students find out: The schools were run by the education administration
requested to send the personal data of the
affected students to the education administration or the private provider, the
to carry out the so-called summer schools. It was about
this data for entitlement to claims under the Social Security Code
and thus sensitive social data. Regardless of whether this data
permitted at all to the education administration or the independent provider
it would have been sufficient to increase the number of entitled persons
To transmit students and the personal data in the schools
to leave. The request of the education administration to the schools, the data
in an Excel table via unencrypted e-mail is possible with the
Regulations of the DS-GVO not compatible. The education administration is in the posi-
tion to ensure secure communication channels between her and the schools.
Education administration schedules, secure email addresses for all teachers
set up are expressly welcomed by us.

In the course of the year, the education administration purchased a further approx. 40,000 tablets for disadvantaged students. From a privacy perspective, it would be preferable decided to buy laptops for the students. Laptops offer German Significant advantages over tablets, as they are much more versatile, offer more freedom in software selection and even without a cloud with providers outside the European Union and thus data protection are quite usable. After all, cheaper prices would certainly also be one more comprehensive distribution to the students would have been possible, so that a uniform learning environment could have been created for everyone. We regret ern it that our towards the Senate Department for Education, Youth and Family and the recommendations made to Parliament have been taken into account. 63

1.4.3 Communication via messenger services

Communication between teachers, students and parents is a still an important topic. In March we were informed that the quality ity officer of the Senator for Education in response to an inquiry about the use of WhatsApp in schools in the context of the corona pandemic, with consent of all those involved, WhatsApp and Skype may be used temporarily. we have taken this as an opportunity to ask the senator to to make it clear that only data protection-compliant offers for are allowed to come. At the same time, we have our support and advice offered. However, we have not received an answer.

In view of existing alternatives, the use is not more data protection-friendly products unacceptable. In our last annual report, we detailed clearly explained that the messenger service WhatsApp in schools is not only set.64 Rather, there is a need for the state of Berlin

in the future will make its own messenger service available. Current

Examples from other federal states show that data-secure messenger services

63 See https://www .parlament-berlin .de/adosservice/18/Haupt/vorgang/h18-2735 .G-v .

pdf

64 JB 2019, 1.1

can also be set up at short notice.65 It is about time that that too

State of Berlin follows these examples.

1.4.4 Legal basis for school digitization

are urgently needed

Whenever personal data is processed, this requires an appropriate

net legal basis or consent. In areas where data

are processed by minors, this should be a matter of course. children

and young people are under the special protection of the DS-GVO.66 The school

law and the School Data Ordinance67 that has existed since 1994

no regulations on the use of digital tools. The General Rules

of the Schools Act on the processing of personal data can be found here

not be used.

In its materiality case law, the Federal Constitutional Court

mer again that essential decisions by a parliamentary

are to be regulated by law. The decision to use digital teaching aids is

due to the associated dangers of misuse of student data

without a doubt to be described as essential. the change

moving from purely analogue teaching aids to digital products entails

that no longer only about the pedagogical suitability of the respective product

is decisive, but now also about compliance with the most complex technical

technical and data protection regulations. In view of the special quality

Action of encroachments on fundamental rights when using digital tools must therefore be

school law to be adapted to this situation. The specific design should

be carried out by a special legal regulation that regulates data protection

requirements.

65 Since August 2020, the state of North Rhine-Westphalia has provided schools with

school platform LOGINEO NRW the LOGINEO NRW Messenger available free of charge

tion to enable communication with the students, and the cultural

Ministry of Baden-Württemberg provides teachers with a free license for the

Messengers Threema Work Education available.

66 See EG 38 GDPR

67 On the amendment of the School Data Ordinance, which has still not been completed in 2020,

was closed, we reported in detail in JB 2019, 5.4.

Currently, due to a lack of a sufficient legal basis, consent must be obtained

of parents for the use of digital learning aids can be used. The A-

However, consent encounters fundamental concerns in the school context. One

Consent can only be effective if it is given voluntarily. In between

the students and teachers, however, is due to the

Compulsory schooling is a relationship of superiority and subordination. In such cases, the GDPR

generally assume that the consent is inadmissible. In order to

It is therefore important to be able to fulfill the terium of voluntariness in practice

necessary that schools provide those who have given their consent for the use of

do not want to give digital offers, equivalent alternative learning offers

provide. In practice, this can certainly lead to implementation

troubles. In order to ensure the necessary legal certainty and

also to achieve a higher level of commitment for the digital lesson design

chen, we think it is necessary for the legislator to act quickly.

The experiences of this year show that the goal of a successful and

data protection-compliant digitization of schools is still a long way off.

Steps in the right direction - as in the case of "Lernraum Berlin" - definitely are

recognizable, but these are still much too small to reach the goal soon

be able. We expect that the education administration will finally recognize that the

Data protection is not an end in itself or even an obstacle to digitization

is, but a necessary prerequisite for a safe and trustworthy

full working in the digital space. We will continue to work to

that children and young people in digital lessons are carefree and unobserved

learn without companies looking over their shoulders. Of

We expect the education administration to act quickly and decisively in order to

a protected digital learning environment for all students in schools

to accomplish.

1.5 Starting signal for the certification

s

i

x

a

right

P

right

e

i.e

s

and

A

High quality and trustworthiness are the most important expectations

Certification bodies that certify data processing operations. The DS

GVO therefore provides that a corresponding qualification and organization

of the certification bodies must be guaranteed. This will be particular

ensured by prior accreditation. The German supervisory

authorities have presented concrete requirements, which within the framework of the

credit must be proven.

Long before the GDPR came into force, there was a desire for reliable

according to data protection certificates and seals that consumers use as a guide

who value data protection and privacy, and which ones

at the same time strengthen the competition for data protection-friendly applications. With

of the GDPR, the legal prerequisites were created for this, but

still have to be filled with life. Certifications do not have to

due to the data protection supervisory authorities themselves. After the in

The model chosen in Germany is rather the responsibility of the supervisory authorities

certification, in cooperation with the German Accreditation Body (DAkkS)

accrediting bodies, which in turn may issue certificates.

All companies or other bodies can therefore apply as a certification body.

apply to those who think they meet the accreditation requirements. There

These requirements are not detailed in the GDPR or other standards

result, the DS-GVO provides that the supervisory authorities must meet the requirements for

Specify accreditations in the data protection area. Our authority has

the last two years together with the other German supervisory authorities

who worked intensively on it in a working group and “Requirements for

Accreditation according to Art. 43 Para. 3 GDPR i. in conjunction with DIN EN ISO/IEC 17065"

68 The document has the necessary opinion procedure of the EDPB

already successfully completed.69

The most important requirements are:

subject of certification

A certification program must be created in preparation for accreditation

will. This program relates to a certification subject. A

The object of certification must relate to data processing operations, namely

68 See https://www .datenschutz-berlin .de/fileadmin/user_upload/pdf/themen-a-z/

a/2020-DSK-DIN17065-supplements-de .pdf

69 See https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202015_en_

requirementscertificationbodies_en.pdf

only those that are rendered in products, processes and services.

This means that they are products without a specific area of application or application

not suitable as certification objects. Because without a specific application

It is not possible to determine whether data processing is GDPR-compliant

present. Management systems for controlling data processing

taken separately are also an object of certification

closed. However, as part of a "certification mechanism" they are

consideration.

impartiality

Impartiality is a central requirement for reliable work

a certification authority. It is only given if independence and

objectivity are guaranteed. Conflicts of interest must not exist. It

In particular, the following requirements must be met:

• The independent

ability to prove. This applies in particular to the financing of the certification

authority as far as ensuring impartiality is concerned.

• The certification body must comply with the relevant data protection supervisory authority

de also prove that their tasks and duties do not lead to an internal

lead to a conflict of interest. Such conflicts could B. by a high

Dependence on sales of certain customers or through other economic

scientific pressure on the certification body.

• A certification body must be in relation to its customers

be an independent third party who is associated with the facility that he owns

evaluates, is not connected. The certification authority, your top one

Management level and those responsible for fulfilling the certification tasks

In particular, employees may not work as designers, manufacturers,

Supplier, installer, buyer, owner, user or

maintenance company of the products to be evaluated.

• The status of a certification body as an independent third body is sometimes

particular cases. Does a certification

e.g. B. join an association whose members are manufacturers,

Chapter 1 Focus 1 .5 Starting signal for the certification

Providers, processors or persons responsible are those who are

Certification authority must be examined more closely.

The independence or impartialities and the absence of anyone

Conflicts of interest must be precisely proven, especially in these cases

will. In the example chosen here, it has a positive effect if the certification

certification body is legally separated from the association. Also the staff

both positions must be separated. The staff of the association may not

Way for the certification body, especially in certification, testing and

inspection procedures. The top management of the certification

must be stated in the partnership agreement or in the statutes of the certification

have committed to impartiality. It has a positive effect

from this if the articles of association or the articles of association contain a passage on

Independence of the management or the management of the certification

ornamentation site contains. In addition, no economic dependency

relationship to the members of the association or to the association itself.

Liability and Funding

Another important criterion for impartiality and objectivity is a

financial stability and independence. On the one hand, the certification body must

be able to demonstrate that they are aware of the risks arising from their certification activities

arise, has assessed and can cover. For this z. B. Insurance

or reserves suitable funds. On the other hand, the certification authority has its

to demonstrate financial stability and independence themselves. The decision

with regard to the selection and naming of suitable evidence is at the discretion

sen of the DAkkS and the competent data protection supervisory authority. The certification

In any case, the agency must have an appropriate

have their pecuniary damage liability insurance.

Publicly Available Information

Transparency is an important prerequisite both for the quality of certification

ments as well as for trust in them. To ensure transparency,

such as information on how to deal with complaints from the certification body

to publish. This publication obligation applies in particular to

the structure and procedure for handling complaints by the

Certification Authority. In addition, information about the certification

used certification programs and all versions of the approved

approved certification criteria, stating the respective period of use

space to publish.

The form of publication should be suitable for the general public if possible

comprehensive to achieve. This is usually through publishing on the

Website guaranteed.

Directory of certified products, processes and services

A special transparency obligation is the obligation to publish

a directory of certified products, processes and services.

The certification body can generally access this directory via the Internet

keep callable. The directory must contain a short report on the respective

include certification results. From this must in particular

Exact object of certification (including version or functional status), the

test method and result as well as the expiry date of the certification.

resources and human resources

A certification body must have the appropriate expertise regarding both

of data protection as well as their independence and specific expertise

with regard to the subject of certification. This serves

especially ensuring the required quality of certifications.

If certification activities are outsourced to external bodies, then apply to

these bodies have the same requirements as for the certification body.

In order to be able to assess the competence of the certification body, accre-

editing procedure in addition to the documents submitted in writing, e.g. B.

Proof of training carried out an accompanying assessment.

The knowledge of the staff required for the certification activity must

must be kept up to date. Evidence can in particular

through further training certificates and relevant work experience, e.g. B.

certification procedures carried out.

Process requirements – evaluation

The certification body must use suitable evaluation methods, i. H. procedure

for verification, to ensure the consistency of processing operations

to be evaluated with the certification criteria. These methods and the results

or the findings of the review must be documented in detail.

The evaluation methods must cover the following areas in particular:

• a methodology for assessing the necessity and proportionality of

processing operations in relation to their purpose and, where appropriate, in relation to the

affected person,

• a method for evaluating the compilation and rating of all

relevant data protection risks and the definition of technical and

organizational measures,

• a method for evaluating the corrective actions, including guarantee

ties, safety precautions and procedures through which the verification

it is made sure that the legal requirements are met.

The certification body can add more during the course of the certification process

request information that they consider necessary for certification. she

can cancel the certification process if the applicant

Applicant fails to submit the information despite being requested to do so.

The certification body must determine the importance of other certification

customer requests, e.g. B. the IT-Grundschutz, for their evaluation

men. It must be clear which other certifications, how and in which ones

scope can be taken into account for an evaluation and what effects

effects this has specifically on the remaining scope of the test.

Complaints and Appeals

So that certification bodies know when there are problems in practice, e.g. B. with

of a certified service there is provision for complaints and

Objections can be lodged directly with her. She must determine who

complaints or objections, whoever can file them on the side of the Zer-

The certification body processes which checks in this context

take place and what opportunities there are for the parties involved to be heard.

In addition, deadlines for those involved must be defined.

59

In the case of justified complaints, the competent data protection supervisory authority

heard to inform.

There is a detailed paper from the data protection supervisory authorities that

describes the requirements for the accreditation of bodies that process data

want to certify work activities. Prospective Certification Bodies

can use this document to check if they and their organization are eligible for a

accreditation procedures are adequately prepared. The task of

data protection authorities does not end there. against

part, it only really starts then. We will

carry out the accreditation procedure together with the DAkkS

and prospective certification bodies on the basis of the criteria mentioned

and check kidneys. We have already received a number of expressions of interest in Berlin

before.

60

Chapter 1 Priorities 2 .1 Status of digitization projects

2 Digital Management

The corona pandemic has created deficits in the di-

gitalization.70 This also applies to the area of administration. in

limited service hours of citizen registration offices, but also the shutdown of the

Management with the lockdown in the spring have shown how important it is with

to make even faster progress with digitization. Here the data protection of

It is important to us to think along from the start - not only so that in the event of

observance of this principle, comprehensive and

expensive technical revisions can be avoided, but also to

the necessary trust of citizens when using digital

not to squander achievements. We therefore bring ourselves both in the state of Berlin and

also at the level of the Conference of Independent Data Protection Supervisors

federal and state authorities (DSK) are very active in the process of data

Intellectual property support for the implementation of digitization projects.

A

and

s

i.e

e

right

P

right

a

x

i

s

2.1 Status of digitization projects

The basic ICT service “digital application” has been put into regular operation.

With the "digital application" application processes from the application to the

Transfer to the respective specialist procedure carried out. administrative services

in this way - as required by the Federal Online Access Act (OZG)

specified - are provided electronically as far as possible. The Senate Administration

for internal affairs and sport involved us in the conception of the digital application

the. As reported last year, we welcome the fact that with the online access

gesetz Berlin (OZG Bln)71 the necessary legal bases have been created

are that allow the administration to use basic ICT services

required personal data to be processed without being here on

consent of the citizens must be resorted to.72 In the course of

70 For the digitization of schools, see 1 .4

71 Law to improve online access to administrative services in Berlin

Administration - Online Access Act Berlin (OZG Bln) from 4. March 2020

72 JB 2019, 2.1

year, the Senate Department for the Interior and Sport has various application processes

included in the "digital application" procedure.

In the implementation of the OZG, the State of Berlin, together with the Federal Ministry

Ministry of the Interior, for building and home and the states of Brandenburg, Ham-

burg and Thuringia responsible for cross-sectional services.

The provision of digital evidence plays a special role here. Also

we reported on this last year.73 While it originally

was about the digital proof of a birth certificate when providing a

ner electronic administrative service, the implementation

project "Basic component verification retrieval" was created in which the country

Berlin Procedures are developed that require the provision of evidence such as

the extract from the population register, the birth certificate or the certificate of good conduct

should be mapped tronically. Since this is a matter of close interlocking with federal law

Lich regulated procedures such. B. when applying for housing or electricity

terngeld, it requires coordination with the responsible federal departments. here

play in particular questions on the classification of data protection

wording between the federal and state governments plays an important role.

2.2 Implementation of the Online Access Act in federal and state governments

The OZG obliges the federal, state and local governments to

to also offer maintenance services online via administration portals. This

Time frame is ambitious. In addition, the corona pandemic is increasing the pressure

digitize individual services even faster.

The federal and state governments work according to a so-called “one-for-all principle”.

in the implementation of the digitization of the various administrative services

ments. Those under the responsibility of a federal state together with the

respective federal department digitized administrative services should then also

be adopted and implemented by the other federal states and municipalities

can. Because of the numerous associated with the implementation of the OZG

73 JB 2019, 2.1

DSK has set up a sub-working group to deal with issues

occupation with regard to compliance with the data protection framework

should accompany things. We are actively participating in this sub-working group.

2.3 Register modernization and data cockpit

This year, the Federal Government launched plans for register modernization

and a draft for a register modernization law74

submitted. The aim is to fundamentally modernize the registers kept in the administration

dernize in order to relieve citizens of having to submit proof of

having to provide digital administrative services. Much more

should it be possible to send these to the other authorities without media discontinuity

procure. For this purpose, the tax ID should be used as a uniform personal identifier and

cross-register classification feature can be used for identification.

The linking of the databases via the tax ID, however, encounters considerable

common constitutional concerns. In this way, a comparison

the most diverse databases is possible and carries the risk of being linked

a personality profile.75 It is also possible and, from a data protection point of view, a great deal

area-specific indicators would be more appropriate. These could

significantly reduce the informational self-determination of citizens

adorn. An adjustment of the provisions of the draft law is therefore urgent

necessary.

Last year we informed about our participation in the digitization

laboratory for a so-called data cockpit.76 This data cockpit is intended to

experience when using digital administrative services

know which of their data is stored by the various authorities

74 Law on the introduction and use of an identification number in public administration and to change other laws (register modernization law - RegMoG), BR-Drs . 563/20

75 See resolution of the DSK “Register modernization in conformity with the set!” from 26 . Aug 2020; available at https://www .datenschutz-berlin .de/infothek-and-service/publications/decisions-dsk

76 JB 2019, 2.1

and can be exchanged between them. This is intended to create the greatest possible transparency. Since Berlin is the field of cross-sectional services, which also includes the data cockpit, the Senate Department responsible for the development and implementation administration for internal affairs and sport with regard to data protection aspects included.

With the plans of the federal government, the register modernization and thus the Linking of the databases from different registers via a uniform The data cockpit also gets to implement personal identification in this context is important. The merging of different Databases on the use of a uniform personal identifier encountered because of the associated risk of creating personal here, too, constitutional concerns. As compensation measure According to the plans, the data cockpit should now also be used for this purpose ensure in this connection that for the citizens at least currently transparency about what is stored about them and between registers exchanged data exists. The data cockpit should be compatible with the currently still im Register Modernization Act77, which is in the draft stage, to a statutory

be made on a solid basis. We welcome this. It is important that the

tencockpit was then quickly implemented technically as an effective tool

and the desired transparency is guaranteed.

A data protection-compliant digitization of the administration is associated with considerable

challenges connected. In order to set the right course here,

we are both in Berlin and at the level of the DSK in the process area

design. Only if the data protection rights of citizens are respected from the outset

be taken into account, the necessary trust in the claims

acceptance of digital administrative services.

77 See Article 2 of the Draft Register Modernization Act, § 10 OZG –

BR - Drs. 563/20

3

3.1 Poor police cooperation

with our authority

When reviewing requests for personal information in police records-

banks involved in right-wing extremist death threats

hen, we had a violation of the police against their legal

Obligation to cooperate with us.

The reason for the review was a complaint from a person at their home

the threat "9 mm for [...] head shot" was sprayed. This person was after

according to his own statements, had previously been a victim of alleged right-wing extremist violence

senior To clarify the facts, we asked the police in May 2019

Examination of all access to entries relating to the complainant and

to their residential address in the police database POLIKS as well as to transmission

the corresponding protocol tape data together with evaluation for a specific one

Period.

A

and

s

i.e

e

right

P

right

a

x

i

s

The evaluation provided by the police showed that several

employees of the police on personal data of the data subject

had accessed. Some accesses were justified in more detail in the evaluation,

others not. Finally, in the evaluation without further explanation

found that there were no indications of official inquiries that could not be justified

exist. The subsequent request, also the hitherto incomprehensible data

to justify the retrieval, the police came despite several reminders and a

NEM direct letter to the chief of police, in which also given the

political consequences of the suspicion once again urgently about the necessary

Information was requested, not after.

The police justified this refusal with the fact that previously the procedural rights

of the employees involved would have to be clarified, since this is always the case

there is a suspicion that in such cases employees are committing a criminal offence

or may have committed an offence. In addition, the complaint

65

no concrete indications of illegal data processing

called by the police, but merely made vague assumptions as to why

half questionable whether the complaint was sufficiently substantiated.

Our tasks include, among other things, the application of the regulations on the

monitor and enforce data protection, deal with complaints

further persons and investigations into the application of the

to carry out writings on data protection.78

This task fulfillment is a legal obligation, which is not

agreed prerequisites such as the existence of concrete indications of a

violation of data protection regulations. Therefore the sub

stampedness of citizen complaints without relevance for the information

and duties of the police to cooperate with us.

In the present case, it was a matter of our legal mandate

Investigation as to whether the police, when retrieving data from POLIKS, comply with the regulations on

has properly applied data protection. In the event of unlawful

tenabrufe it is up to us to apply the regulations on data protection

enforced by the police for the future. This can e.g. e.g.

obligation of the police done certain technical and organizational

Measures such as better logging of queries in POLIKS or

Suitable internal sampling procedures to control access to POLIKS or similar.

Ä. to take to ensure the security of the processing of personal data

guarantee.

In order to fulfill these tasks, we first need information about the

Reasons for the queries made. Otherwise we cannot check whether

the queries were legitimate.

Would the data protection authorities responsible in cases like this

present the information with reference to the procedural rights of their employees

in most cases it would be impossible for us to refuse

to check the legality of data processing by these bodies. Because the

78 § 11 para . 1 sentence 1 no. 1, 6, 8 Berlin Data Protection Act (BlnDSG)

Chapter 3 Internal affairs and justice 3 .1 Poor cooperation between the police and our authority

respective data processing is generally not considered by the respective body

institution, but carried out by its employees. You come to the

Examination of the legality of data processing by a responsible person

So do not avoid regularly providing information about the employees

to obtain. Our powers are correspondingly broad. you will be

not legally affected by criminal or regulatory procedural rights of the

made dependent on the responsible body. Both

must be strictly separated from each other.

Insofar as there are sufficient factual indications of a criminal or

unlawful behavior of individual police officers

this from this point in time, of course, corresponding statements or

rights of refusal. On the one hand, however, such indications are currently available

not visible. On the other hand, only the employees concerned have

these rights, not the police as the responsible body. This remains comprehensive

obligation to provide information.

In order to avoid a previous self-incrimination of the employees involved

We had also pointed out to the police that for answering

our questions also investigations to clarify the facts independently of

the questioning of these persons could take place. In particular, it is possible

to question their superiors and gain insight into the

ongoing operations. This could be used to check, among other things, whether the

meeting employees were responsible for processing the

events that they have seen. Furthermore, it could be checked

for what reasons they had access to the files at this point in time

have taken.

We have the persistent refusal of the police to assist us in our work

support, objected.79 The police are legally obliged to provide us with all information

to provide functions that are necessary for the fulfillment of our tasks.80

79 See § 13 para. 2 BlnDSG

80 § 13 para. 4 no. 2 BlnDSG

She is also obliged to cooperate with us in fulfilling our tasks.

work.81

It is still unclear to this day whether the data queries in question were lawful

However, after talking to our house management, the police contacted us

the chief of police in the meantime - more than a year after the start of the

ment – has now agreed to provide us with comprehensive information on our review

support. We now hope for improved cooperation.

3.2 Amendment of the Police Act

s

i

x

a

right

P

right

e

i.e

s

and

A

The police are to be given new legal powers for their work in the area of

driver protection.82 These include the introduction of bodycams and

preventive telecommunications surveillance. We have to the corresponding

commented on the draft law to Parliament.83

It is gratifying that the planned regulations with regard to data protection

are very differentiated. They do not correspond in all formulations

the data protection regulations, but the claim becomes visible,

to meet these.

At the same time, however, it is very regrettable that the present

draft law does not make the long-needed legal adjustments to the

General Safety and Order Act (ASOG) to the Directive (EU)

2016/680 (JI Directive).84 Neither is the adjustment

of the ASOG to the amended Berlin Data Protection Act (BlnDSG).

81 § 54 BlnDSG

82 See Draft Twenty-Third Amendment General Act

Safety and Order Act and other laws, Abghs-Drs . 18/2787 from

12 . June 2020

83 According to § 11 para. 2 BlnDSG

84 Pursuant to Art. 63 para. 1 sentence 1 of the JI Directive, the member states had to May 2018 to enact and publish the legal and administrative regulations that require required to comply with this policy.

This leads to practical application problems, e.g. rights.85

In our statement on the draft law, we pointed out, among other things, that it is unlawful to record images and sound once started with a bodycam took by the police indiscriminately until the conclusion of the police to continue measures. In the explanatory memorandum to the law, it is explained that This is the only way that operations can be comprehensively assessed, with the "geschehen" is not to be understood narrowly in this respect. The general continuation of and audio recordings to record the entire operation, which is under Circumstances can persist for a very long time without the original danger remaining exists and without this being for a subsequent review by a police Measure is necessary, in particular with regard to the depth of intervention Image and sound recordings for all those involved in the event and also any unrelated shared third parties disproportionate and therefore inadmissible.

With regard to switching on a bodycam, we have required that to sufficient guarantee of the transparency of data processing on this should always be pointed out in advance. Because this is the only way those affected can respond and exercise their rights. At the same time, when activating An optical signal should be recognizable with a body cam, e.g. B. a red light that shows the recording.

The planned continuous operation of bodycams in use by means of a

We have criticized the so-called pre-recording function86 as being contrary to European law. He WI-

corresponds to the data protection principle of necessity, according to which

data processing is only permitted if this is specifically necessary for the task

ment of the responsible body is required.87

The pre-recording independent of a concrete task fulfillment is included

based on a technical necessity, which, however, does not exist. To

85 There are currently two different regulations for this – Section 50 ASOG and Section 43 BlnDSG .

86 The bodycams should record everything in the field of view in an endless loop and

after 30 seconds at the latest, regardless of whether it is for the data

collection and storage gives an actual reason.

87 See Art . 8 para. 1 JI guideline, which is already in § 33 para. 1 BlnDSG was implemented

of the justification for the law, delays after the triggering of the recording

be prevented by booting the camera. Modern cameras

can, however, be available in standby mode88 and be switched on immediately

without causing a time delay. The camera is in this case only

temporarily disabled, similar to a pause button, and can be left without at any time

switched to activation mode with a time delay. Such

Technology is used, for example, by Deutsche Bahn. That a boot up a camera

no longer corresponds to the state of the art before it can be used,

also check everyone who turns on the camera on their smartphone.

The planned changes in the law will give the police new data

administrative powers, precisely with regard to their actual necessity

are to be observed. It is therefore to be welcomed that the benefits of this

powers in practice according to the draft law independently scientifically evaluated

should be discussed and Parliament will then discuss this again

will replace.

3.3 Introduction of a citizen and

police officers

s

i

x

a

right

P

right

e

i.e

s

and

A

In the state of Berlin, the position is that of a citizen and police officer

been introduced.89 The aim was to create an external ombudsman, i. H.

an impartial arbitration board that handles official processes independently

should control the interest of the citizens.

According to the explanatory memorandum to the law, the model for the new office

in Rhineland-Palatinate.90 However, the regulations there were passed to

initially not taken into account in the Berlin legislative project.

88 Also called ready or waiting function

89 Citizens and Police Officers Act (BürgBG)

90 state law on the ombudsman of the state of Rhineland-Palatinate and the

Commissioner for the State Police (BürgBG RP)

70

Chapter 3 Home Affairs and Justice 3 .3 Introduction of a or . a ombudsman and police officer

takes. We have a position on this at a hearing in the House of Representatives

taken.91

According to the original draft law92, the citizen and political

commissioned the work of the Petitions Committee of the House of Representatives

support and her or his task as an auxiliary organ of the Chamber of Deputies

ses in the exercise of parliamentary control. simultaneous

However, the Ombudsman and Police Commissioner, as the supreme state

authority to be set up. It was not clear whether the institution was part of the

Should be executive or the legislature. We had required this in law

to clarify. It is now regulated that the citizen and police officer

contributed as an auxiliary organ of the House of Representatives in the exercise of parliamentary

of public control, but is not the supreme state authority.93

clarified that the institution is part of the legislature.

In this context, it should also be noted that the initially planned

Organization of the Ombudsman and Police Commissioner as the supreme state

authority would run counter to the administrative structure of the State of Berlin. In Ber

lin are only the Senate, the Court of Auditors and the Berlin Commissioner for

Data protection and freedom of information supreme state authorities. These authorities

have constitutional status.94 The establishment of the Office of the Citizens and

Police Commissioner as the supreme state authority would not have this constitutionally

conform to the legal structure.

As the example of Rhineland-Palatinate showed, however, there were other ways to

to achieve the greatest possible independence of the institution. The Land Rhine

state-Palatinate has its ombudsman as the permanent representative of the petition

committee.95 The Commissioner for the State Police takes up her position

gabe as an auxiliary organ of the Landtag in the exercise of parliamentary control

91 Pursuant to Section 11 Para. 2 BlnDSG

92 See draft law establishing the Ombudsman(s) of the

State of Berlin and the Commissioner for the Berlin Police, Abghs-Drs. 18/2426

from 21 . January 2020

93 § 1 para . 2 and § 3 BürgBG

94 See Art . 47, 67 and 95 of the Berlin Constitution (VvB)

95 See § 4 sentence 1 BürgBG RP

true and is independent in the exercise of its office, free from instructions and only to the

Subject to law.96 The commissioners are part of a public law

Official relationship with the state of Rhineland-Palatinate, but are not the supreme state

set up by the authority.97 These regulations otherwise correspond to those for

Parliamentary Commissioner for the Armed Forces98, which is considered part of the legislature.99

In the version of the law that was ultimately passed, the legislature has

attached to these examples.

The draft law presented to us during the hearing to set up

the Ombudsman and Police Commissioner in Berlin also contained

also very far-reaching powers with regard to data processing, which

had to be determined and limited. For example, there were no provisions

genes for handling sensitive data that are regularly associated with

Complaints about the police, but also about health and social authorities

attack. In addition, there were no regulations on the rights of those affected, such as the obligation to delete

ten. There was also no authorization standard for public bodies that would allow them to

personal data to the ombudsman and police officer

to transfer. In this respect, too, our objections were taken into account: Sensitive

Data may now only be processed if there is a significant public

ches interest requires it.100 A data transfer authorization was granted for

created public bodies.101 Incidentally, reference is now made to the regulations of

General Tenant Protection Ordinance (DS-GVO) and the BlnDSG, so that the

application of the rights of the data subjects there is guaranteed.102

Furthermore, all state authorities should be obliged to

ger and police officers in carrying out the necessary surveys

to provide official assistance. According to the wording, this would also include the Berlin

mandated for data protection and freedom of information. This would have

96 § 16 para . 2 BürgBG RP

97 § 10 para . 1, § 17 BürgBG RP

98 See § 1 para. 1, § 14 para. 3, § 15 para. 1 of the Law on the Military Commissioner

German Bundestag (WbeauftrG)

99 See Maunz/Dürig/Klein, Basic Law, Art. 45b, para. 13, 14 mwNw

100 § 5 para . 1 sentence 2 BürgBG

101 § 5 para . 2 BürgBG

102 § 5 para . 3 BürgBG

but in contradiction to the data protection regulations, according to which

the representative neither direct nor indirect external influence

subject, neither seeks nor accepts instructions and

is obligated, about the affairs of which she or he has officially become aware

to maintain secrecy.103 In this respect, too, it has now been clarified that

that the legal status of our authority remains unaffected.104

The introduction of a citizen and police officer is to be welcomed

ßen, because they strengthen parliamentary control and the rights of the

Citizens in relation to the police and other authorities

can lead. It is very gratifying that our concerns about the original

original bill were included and the constitutional and

data protection aspects are now sufficiently taken into

the.

3.4 Separate assembly law for Berlin

With the federalism reform in 2006, legislative competence was increased

shifted to the federal states for the right of assembly. So far Ber-

lin only with regard to the production of image and sound recordings for public

public gatherings in the open air and elevators

done.105 Now the entire right of assembly in Berlin is to be newly regulated

become.106

A

and

s

i.e

e

right

P

right

a

x

i

s

We have made the following statements to Parliament on the draft law, among other things:

taken lung:107

103 § 10 para . 2, para. 5 BlnDSG, Art. 52 para. 1, 2 GDPR

104 Section 6 sentence 2 of the Civil Code

105 Act on recordings and recordings of images and sound at meetings

in the open air and elevators (VersAufn/AufzG)

106 Draft law on freedom of assembly in the state of Berlin (VersFG-E),

Abghs-Drs . 18/2764 from 2. June 2020

107 Pursuant to Section 11 Para. 2 BlnDSG

The European Court of Human Rights (ECtHR) measures the peaceful,

political and trade union protest for the democratic process

great importance and issued a decision in 2019 accordingly

high demands on the processing of data by the British police.108

Personal data processed in connection with meetings

are processed regularly fall under specially protected categories. she

can in particular provide information about the ethnic origin, about political

ments, religious or philosophical beliefs that

belonging, but also about health or sexual orientation

and have an increased need for protection due to their sensitivity.

The ECtHR emphasizes in its above decision that the storage of such data

by authorities can have a deterrent effect ("chilling effect")

to participate politically.109 Membership or affiliation with a group

or movement should therefore only be recorded if this is for a specific

review is necessary.110 The ECtHR concedes to the national authorities

when assessing the need for a wide margin of appreciation.111

Taking this European jurisprudence into account, it should be criticized that

that in the Berlin draft law a purpose-changing use of the under narrow

Conditions raised for security purposes at a meeting

Data should also be allowed to carry out fine procedures. Because here-

there is a risk that, for example, through the additional use of image and

Sound recordings for the clarification of less serious offenses through the

tertür exactly the deterrent effect could arise, the people of it

discourages political participation.

The currently planned further processing of lawfully collected data

collecting data solely for documentation purposes is to be criticized. The re-

The reason for the data processing for this purpose is not apparent. When a

108 See ECtHR, judgment of 24 . January 2019, CATT v . THE UNITED KINGDOM (Application

no . 43514/15)

109 para. 123 of the decision

110 para. 124 of the decision

111 para. 118 of the decision

If danger has arisen, i.e. there is a fault, it only resolves it regularly

repressive action by the police. For this specific purpose, the

However, further data processing is already permitted.112

It is also planned that the assembly authority

together with information on the progress of the

collection indiscriminately two years after the conclusion of the assembly for the

Assessing a risk situation at future meetings

113 In the present form, this violates the rule of law

principle of necessity. The regulation also does not take into account that personal

Personal data related to meetings, usually sensitive

and are therefore particularly vulnerable.

The assembly authority collects the aforementioned contact details in order to

preparations during the assembly and, in emergencies, quickly and

to act efficiently. In principle, this need for provision ends with the

end of each meeting. Longer storage for purposes of

Prepare for danger at future gatherings may be required

be nice For this, however, there must also be concrete evidence that

that the persons responsible for the meeting that has taken place

hold a similar meeting in the foreseeable future. Is about due

the topic of a meeting (e.g. "75 years after the end of the war") it is clear that this

only takes place once, further storage of the data is not required

lich. On the other hand, certain congregations such as B. Vigils possible

happily also occurs so frequently that it is already sufficient to determine the behavior of other

reporting and/or leading persons of the meetings as well as the course

of the respective meeting within one year.

The law should also regulate that our authority and the

official data protection officer of the police compliance with the police

Documentation requirements in connection with the processing of meetings

ment data.114 According to the BlnDSG, however, we are authorized to

112 § 18 para . 3 sentence 1 no. 1 VersFG-E

113 § 30 para . 2 VersFG-E

114 § 18 para . 6 VersFG-E

to check data processing procedures of public authorities in Berlin.115

The regulation in the present draft law is in this respect ambiguous and

also superfluous due to the regulations in the BlnDSG. The same applies to the

powers of the official data protection officer of the police.116 We

have therefore called for the regulation to be deleted.

The processing of personal data in connection with meetings

due to the sensitivity of this data i. V. m. the constitution

very strict prerequisites guaranteed by the right to freedom of assembly

stipulations that are taken into account in the corresponding legal regulations

Need to become.

3.5 Unlawful data processing

Sinti and Roma

s

i

x

a

right

P

right

e

i.e

s

and

A

In the publication of the police crime statistics (PKS) 2017 it was stated

Page 48: “Out of the 86 suspects involved in the trick theft, 53 were Sinti

and Roma."117 Based on a submission, we have stopped the processing of personal

collected data on the Sinti and Roma ethnic groups checked by the police.

The police initially stated that the information in the PKS 2017 was based on the technical information

well-founded assessment of the specialist department. A systematic assignment of facts

suspicious to the population group of Sinti and Roma basically takes place

Not. At best, it comes occasionally in the context of police processing

for the processing of data about ethnicity, for example when people

self-identified as Sinti, Roma, Jenische or “Gypsies”.

However, such information would not be documented systematically and searchable,

as saved, but only recorded in the word log and would thus become part of the

process.

115 § 11 para . 1 sentence 1 no. 1, 8 BlnDSG

116 See § 6 para. 1 no. 2 BlnDSG

117 This passage was meanwhile published on 15 . January 2020 due to an instruction

by the Senator for the Interior and Sport, Andreas Geisel, in the online version of the PKS

canceled in 2017.

We then conducted an audit with the police to verify the use of the

Terms "Jeniche", "Roma", "Sinti" and "Gypsies" in processes from the year

randomly checked in 2017. It turned out that from the im

Cases completed in 2017 with the event title Trick Thief

stole from apartment” 31 one or more of the terms “Roma”, “Sinti” and “Gypsy”

ner” included. The naming was mostly on quoted or reproduced

testimonies of witnesses or suspects. But also documents

without direct reference to witness or accused statements, such as the

Facts summarized by the investigating police officers

stop at the criminal charges, search, interim or final reports

the public prosecutor's office, contained the above Terms without recognizable necessity.

According to § 33 Para. 1 BlnDSG, danger prevention and criminal prosecution authorities may

only process the special categories of personal data if this

to fulfill their tasks or to protect vital interests

natural person is required or the processing relates to data,

which have obviously been made public by the data subject. the eth

Niche affiliation belongs to the special categories of personal

Data.118

For the fulfillment of the "law enforcement" task, law enforcement agencies may

save, change and use personal data in files, insofar as this

is required for the purposes of criminal proceedings.119 For the task "Danger

defence" the police and regulatory authorities can lawfully collect personal data

save, change and use related data in files or files, as far as

this for the fulfillment of their tasks, for a temporary documentation or

is required for process management.120

When assessing the necessity of data processing for the aforementioned

Task fulfillment is to be differentiated according to which term is used,

to whom the use of the term can be attributed (police or third parties, esp.

118 See § 31 No . 14 lit. a BlnDSG

119 § 483 para. 1 StPO

120 § 42 para. 1 ASOG

special witnesses and suspects) and to whom the respective text (po-

lizei, public prosecutor's office) directs:

The words "Gypsy" and "Landfahrer" are generally not permitted and

removed from all processes. Quotations clearly marked only

as an exception, they can be in processes if they are relevant to the investigation

are.

The following applies to the terms Sinti and Roma:

• Their use in final reports to the public prosecutor is inadmissible

sig, since the public prosecutor's office investigates the acts, but not the suspected

son rated.

• Their use in facts in criminal charges, notes, interim

is permitted in exceptional cases,

= if the feature specifically promotes investigation or search

provides breakpoints, e.g. B. Whereabouts or gang structure. The assignment

tion should always be based on binding criteria or instructions

and only presented by appropriately trained officials

be taken. So-called "racial profiling" must be avoided at all costs

will;

= if knowledge of the ethnicity of the victims and/or crimes

suspect suspected of being xenophobic or racist

motives committed (§ 130 StGB) for their exact assessment

is relevant.

• Their use as self-ascriptions by those affected or as literal

Reproduction of statements by third parties, for example in interrogation records or reports

pay attention, is permissible.

Knowledge of the ethnicity of suspected or aggrieved persons

NEN is therefore regularly not required for police work and at best

permitted in exceptional cases. With regard to all of these exceptions

the police bear the burden of proof.

78

Chapter 3 Home Affairs and Justice 3 .6 Unauthorized photographing of identity cards or passports

As far as the police the necessity of data processing on Sinti and Roma

cannot prove that they have fulfilled their tasks in the cases examined by us

could, we have raised a complaint.121 In addition, we have the

Police to independently check the other police databases

to illegal data processing in connection with the ethnicity of the

Sinti and Roma and, if necessary, to clean up this data

stood asked.

3.6 Unauthorized photographing of personnel

ID card or passport by the police

A citizen complained to us that when a witness testified in

connection with the report of a disturbance of the peace to the police

national ID card was photographed with a smartphone without his consent.

The police informed us that the ID data for the court-proof documentation

tion of the operation would be required. Photographing the ID card

made the job easier. When copying ID card data, it comes

mer again to errors. By photographing the identity card should

avoid that erroneous data is stored in the police database

will. In addition, the police needed less time for data collection

takes. The police could not name a legal basis for their actions. That

Photo was from the police after transferring the data to the police database

been deleted.

A

and

s

i.e

e

right

P

right

a

x

i

s

The police have the right to identify themselves in order to carry out the tasks assigned to them

of persons and the personal data collected in the process

to be saved.122 Citizens must, upon request, submit an identity

present their identity card to authorized authorities such as the police.123

121 See § 13 para. 2 BlnDSG

122 §§ 21 para . 1, 42 para. 1 ASOG

123 § 1 para . 1 p. 1, 2 Personal Identity Card Act (PAAuswG)

However, photographing the ID card is only possible within narrow limits

authorized. Police officers must have an identity card before they can

photograph to verify identity, the consent of the ID card holder

or the ID card holder.124 The person concerned can also request

that certain data are made unrecognizable after being photographed

the.125

We have complained to the police about the photographing of the staff

identification without the consent of the person concerned, a finding of deficiency126

pronounced. Employees of the police are only allowed to carry their identity card with them

Photograph the ID card holder’s consent.

Copying the identity data from the ID card is also still possible

possible without consent, insofar as this is necessary for police tasks

is.

3.7 Storage of data in the registration, passport and

identity card register

s

i

x

a

right

P

right

e

i.e

s

and

A

We received numerous complaints and inquiries about the memory

Storage of personal data in official registers, in particular in

Registration, passport and identity card register.127

In principle, the competent authorities may only process personal data

ten if a legal regulation provides for this. Depending on the type of

registrar, there are specific laws that govern data processing

arrange The Federal Registration Act (BMG) determines which

information about a person may be stored in the population register. The scope

the data to be stored in the passport or ID card register, on the other hand

in the Passport Act (PassG) or Personal Identity Card Act (PAuswG). This

124 § 20 para . 2 sentence 1 PAuswG

125 § 20 para . 2 sentence 3 PAuswG

126 See § 13 para. 2 sentence 2 BlnDSG

127 For data processing in the population register, see JB 2019, May 3

three official file systems are not public registers, but for

official purposes.128

The population registers are kept by the registration authorities, whose task it is to

to register the persons residing in their area of responsibility in order to

to be able to determine and prove their identity and apartments.129 Which ones

personal data the registration authorities to fulfill their tasks in

Section 3 of the BMG finally stipulates that the population register may be kept.130

The population register data to be saved can be divided into three groups: The

Basic data131, the special data132 and the reference data required to prove the

Correctness of the basic and special data are processed.

Basic data in the area of responsibility of the registration authority include family name,

Doctoral degree, date and place of birth, gender, information on the legal

chen representative, current nationality(s) and current and former

address(es). This data may be used to carry out the registration authorities

assigned tasks133 and according to specific reporting

legislation are used. In contrast, the processing of

Special data to the specific support tasks specified in the law

bound by the registration authority (e.g. in connection with the preparation and

conduct of elections and voting). Any processing other than that

data in the population register provided for in the Federal Ministry of Health and the implementation regulations

is generally not permitted. You are therefore immediately by the registration authority

to delete.134

128 Despite this internal character, if certain conditions are met

information is given to private or public bodies; see e.g. B. §§ 34, 44 BMG.

129 § 2 para . 1 BMG

130 Further data or . Information may only be given on the basis of § 55 para. 1 BMG i . v. m .

§ 2 Berlin Implementation Act for the Federal Registration Act (BlnAGBMG).

will .

131 See § 3 para. 1 number 1 to 19 BMG

132 See § 3 para. 2 BMG

133 Pursuant to Section 2 Para. 1 and 3 BMG these are: identity verification and accommodation

information, issuance of information from the population register, data transmission to other public

positions and participation activities (additional tasks) .

134 § 14 para . 1 set 2 BMG

Keeping the passport register is the task of the passport authorities.135 They serve to

from issuing passports and verifying their authenticity and other

on the one hand to establish the identity of the person who holds the passport or for whom

it is issued.136 The content is conclusively determined in the law.137 Accordingly

In addition to the photo and the signature of the passport holder, they may

Passport holder and procedural processing notes, including the following

Data included: names, doctoral degree, date and place of birth, gender, height

and color of eyes, current address, nationality, serial number

mer of the passport, expiry date and information on legal representatives.

Similar to the population register, the processed data is between the

named basic data on the one hand and notes or "procedure-related processing

processing notes" on the other hand. The latter have the function

of auxiliary data to prove the accuracy of the information contained in the passport

to allow gifts. This includes, in particular, file numbers, documents and

other evidence that arises as part of the passport application and issuance

len.138

Passport authorities are obliged to keep the data in the passport register by at least

Issuance of a new passport, however, in the case of lost documents

to be kept in case the lost document is lost again

which appears and must be assigned. No later than five years after the

During the validity of the passport, at least certain information such as the photo

to delete the image, the signature and the procedural information.139

Finally, the ID card registers are managed by those responsible for ID card

responsible identity card authorities and serve to carry out

tion of the PAuswG, in particular the issuance of ID cards and the determination

ment of their authenticity and the identity of the person holding the ID card

possesses or for which it is issued.140 The identity card register may

135 § 21 para. 1 passG

136 § 21 para . 3 PassG

137 § 21 para . 2 no. 1 to 16 PassG

138 See also no. 21 .2 .1 General administrative regulation for the implementation of the

Passport Act (PassVwV)

139 § 21 para. 4 sentence 1 PassG

140 § 23 para . 2 PAuswG

the photo, the signature of the ID card holder

as well as process-related processing notes exclusively those in the law

listed data.141 These are e.g. B. Surname and birth

name, first names, doctoral degree, date and place of birth, height, color of the eyes,

Address, nationality, last day of validity and issuing

Authority. As with the passport register, the stored in-

information about basic data and process-related processing notes. the

Use of the data processed in the ID card register is under the

Subject to a permit standard.142 Personal data in the ID card

register are at least until a new ID card is issued, at most

however, up to five years after the expiry of the validity of the card on which they are based

relate, store and then delete.143

What data is stored in the registration, passport and identity card registers

are governed primarily by federal regulations and

is partly supplemented by state implementation regulations. As far as

relevant specialist laws do not make any special regulations, apply to the management

tion of the registers, the restrictions and requirements of the General Data Protection

ordinance (DS-GVO), the Federal Data Protection Act (BDSG) or the

Berlin Data Protection Act (BlnDSG) on technical and organizational

Measures.144 The IT process responsibility for the central electronic

Registration, passport and identity card registers are located in Berlin at the state office

for civil and regulatory affairs.145 In addition, the

registration, passport and identity card systems from the Berlin

district offices perceived.146

141 § 23 para . 3 no. 1 to 19 PAuswG

142 § 24 para . 1 PAuswG

143 § 23 para . 4 sentence 1 PAuswG

144 See e.g. B. kind . 24, 25 and 32 GDPR

145 Annex ASOG – No . 33 para. 1 letter a, para. 2 letters a and para . 3 lit. a List of responsibilities

Order tasks (ZustKat Ord)

146 Attachment ASOG – No . 22a para. 1 condition cat

3.8 Common Center for Telecom

nification monitoring – Broad service on

narrow base

s

i

x

a

right

P

right

e

i.e

s

and

A

The states of Berlin, Brandenburg, Saxony, Saxony-Anhalt and Thuringia are building

a joint center for telecommunications surveillance. we

have commented on the planning documents. We had to

Overstretching of the scope of duties and the lack of preparation of radio

Criticize the protection of the rights of those affected.

The joint control and service center (GKDZ) for the telecom

communications surveillance is carried out on the basis of a state treaty by the

States of Berlin, Brandenburg, Saxony, Saxony-Anhalt and Thuringia

builds.147 It is intended to replace the systems that have been operated up to now in the countries

Pool competencies and ensure efficient support of preventive policies

temporary work and law enforcement.

After we had already accompanied the drafting of the state treaty, which

legal basis for the use of the center by the police

authorities of the federal states, we now also commented on the ones presented to us

planning documents. We coordinated with the supervisory authorities of the

other countries involved.

One deficiency immediately stood out: The plans of the center exceed

sen powers set by the state treaty. The state treaty limits

the competences of the center to support the police authorities

in the field of telecommunications surveillance. However, the plans see

in addition, support for other monitoring measures

before, e.g. in the acoustic monitoring of living spaces. The countries can

assign tasks in this area to the center. For this must

However, the state treaty with the participation of the parliaments can be changed. There-

we have expressly pointed this out.

147 See GVBl. 2017, p. 651 ff.

Since the surveillance of the telecommunications of suspicious persons

is a significant encroachment on fundamental rights and often also includes persons who do not

are the subject of the respective police investigation are in the criminal

ordinance (StPO) contain a number of provisions that protect the rights

serve these people.

This is how communication with persons subject to professional secrecy (e.g. with doctors

or lawyers) specially protected and should not be recorded, es

unless the investigations are directed against those who are subject to professional secrecy

itself. Also the core area of private life – and thus the most intimate

Part of our lives - must not be caught by telecom surveillance

be caught.

However, the center will initially unfilter the telecommunications data

taken over by the telecommunications companies, which they

give instructions. Employees only decide at a later point in time

the respective police, which parts of the recordings due to the protection regulations

are to be deleted. This alone puts those affected in a worse position than in

a recording under the direct control of police officers who

can intervene immediately if the protection area is affected. The plans

of the GKDZ also stipulated that only the

data processed by the police authorities. The original data should

remain. We emphasized that a full solution

of all data copies should be provided for.

Also for the granting of the other rights of the persons concerned by the state

police authorities, the GKDZ must provide functionalities. This includes

the blocking of data whose deletion has been postponed and the information

about the processed data, but also the identification of the data - depending on

who they refer to: suspects, offenders, victims,

witnesses or others.

Furthermore, the plans for the logging of the data processing in

GKDZ in deficit. It is fundamental that the legality of the

processing of highly sensitive data operated in the center subsequently

can be checked. For this purpose, planning must specify which information is to be

cher technology are to be logged and how the logs against unintentional

loss and unauthorized modification. In addition, must

Methods and workstations for evaluating the logs are available and it

must be possible to transfer the logs to the data protection supervisory authorities

to enable them to carry out a thorough examination.

Finally, we pointed out to the GKDZ that the police authorities

are obliged in a systematic process, the so-called data protection consequences

assessment (DPIA), the risks of future data processing for the

to analyze the people affected and to take appropriate and effective measures

to adequately mitigate the risks. It makes sense that that

GKDZ carries out this impact assessment jointly for all police authorities.

We will carefully review it as soon as it is available.

It is in the public interest that the police

form can efficiently fulfill the tasks assigned by law. The ones there

The funds used must be within the framework defined by law

keep. This also applies to joint institutions that operate transnationally

like the GKDZ. With the involvement of the data protection supervisory authorities in the

planning process opens up the possibility of ensuring this at an early stage

place.

3.9 Information rights of examinees in the

legal education

s

i

x

a

right

P

right

e

i.e

s

and

A

The Joint Legal Examination Office Berlin-Brandenburg (GJPA) asked us

to assess a draft bill for a law amending

writings for legal education.

This draft saw, among other things, the new regulation of information rights of examinees

before, which, however, the basic right of information of data subjects according to the DS-

GVO on the processing of the data148 concerning them unlawfully shortened.

148 Art. 15 para. 1 GDPR

The right to information under the GDPR relates to all data processing

processing of the GJPA, not only to the automated storage of personal

related data, as provided for in the draft law. Incidentally, due to

the clear wording of the DS-GVO in this respect also no legal clarification

lung requirement. A repetition of the regulatory content of the GDPR in a
A state law would be legally questionable. We have therefore deleted the
planned regulation recommended.
According to the draft law, the rights to information should also apply with regard to copies
the examination files, including the examination papers from the capacity and internship
be restricted for reasons of quality.
The right to information should be guaranteed by the examinees
after completion of the test procedure in the premises of the GJPA inspection of
the examination files kept on them and they are granted during the
should also be allowed to make copies.
The GJPA, on the other hand, is obliged under the GDPR to provide a free copy itself
of the processed personal data.149 A
Restriction of this obligation in the planned form would be against higher-ranking EU
violating copyright law. It is not clear why the creation and transfer
Sending or handing over such copies to those affected “poses a considerable risk
the damage, modification, interchange or destruction of the examination materials
beiten” should exist, which, according to the explanatory memorandum of the law, constitutes a restriction of
should allow access rights.150 To avoid confusion or
Damage to the documents to be copied by GJPA employees
organizational measures can be taken. So we have that too
It is recommended that this planned provision be deleted.
149 See 15 para . 3 i . v. m . kind . 12 para. 5 sentence 1 GDPR
150 See Art . 23 GDPR

The extent of the information rights for examinees in legal training results
from the GDPR. According to this, there is in particular a right to an un-

Paid copy of the examination papers together with assessment documents. This

Rights must not be prohibited by national legal training regulations

education to be shortened.151

151 See also the very detailed judgment of the VG Gelsenkirchen of 27 April

2020 – 20K 6392/18

4 Youth and Education

4.1

On the use of Microsoft 365 in schools –

continuation

In our last annual report, we used Microsoft 365

(previously Office 365) existing data protection problems.

At the same time, we have the voting process between representatives

the conference of independent federal data protection supervisory authorities

and the countries (DSK) with the company Microsoft Corp. about the requirements

of permitted use of Microsoft 365 products.152 On

Years later we have to admit that the concerns persist.

A

and

s

i.e

e

right

P

right

a

x

i

s

This year we received numerous inquiries about the admissibility of the use of

Get Microsoft 365 in the school context. Due to the corona pandemic, many

Schools Take a look at products from the Microsoft 365 package and

possible replacements checked. Especially the software that can be used for video conferences

Microsoft Teams153 as part of this package came into use in various schools

sentence. The use of Microsoft teams is also the subject of several

heavy from parents who have reached us.

A major problem with using Microsoft 365 is that micro

soft reserves the right, who is actually responsible for the respective school on behalf of

to use any processed data for their own purposes. This construction

is the order processing according to the General Data Protection Regulation (GDPR)

foreign.154

It is the essential feature of order processing that in its framework

If the contractor processes the data exclusively for the client

tet. Any further processing by the contractor

152 JB 2019, 5.3

153 On the use of video conferencing technology in detail 1 .3

154 See Art . 28 GDPR

to act in the role of a responsible person. For the

bound disclosure of personal data by the client

there is a legal basis that schools do not have.

The consent of the parents, which is often obtained by schools, can also

Using Microsoft 365 does not offer a solution here. First must be established

become that it is not possible to intervene in unlawful processing

consent. Even in the event that the respective processing is not unlawful

and consent is therefore possible in principle, however, the DS-GVO provides

strict requirements for their effectiveness. In particular, they must be informed

and done voluntarily. Because of the relationship between students and teachers

existing relationship of superiority/subordination, however, the GDPR assumes that

that consent in the school context cannot, in principle, be voluntary.155

The school, as the client, is also responsible for the unclear and contradictory

contradictory regulations in the contract to be concluded with Microsoft

employment contract is not possible, which is associated with the use of the software

Data processing in detail for their data protection conformity according to the DS-

review GMOs. This applies in particular to the presentation of the technical

and organizational requirements that are not sufficient to enter the schools

able to decide whether these are appropriate. the shoes

are therefore not in a position to comply with the rules incumbent on them under the GDPR

accountability.156 Against this background, the

Declarations of consent to be obtained from parents also do not meet the requirements

Being informed is enough, since the school does not have this sufficiently about the im

could inform individual data processing taking place. As a result

the use of Microsoft 365 by schools can under no circumstances be

approval be justified.

To our regret, the data protection supervisory authorities of the

The federal and state governments did not reach agreement this year on how

the use of Microsoft 365 is to be finally evaluated. Although the

supervisory authorities, the majority of the requirements for a data protection compliant

155 See EG 43 GDPR

156 See Art . 5 para. 2 i . v. m . kind . 5 para. 1 letter a GDPR

The use of Microsoft 365 is not considered given, however, the DSK

advocated further talks with the company here,

to achieve improvements. However, this has no effect on

the evaluation of the product currently on the market.

We maintain a privacy-friendly use of Microsoft 365 in schools

currently still not possible. We see Microsoft as having a duty to

make significant improvements. Until then, we advise all schools

urgently to refrain from using Microsoft 365.

4.2 Data protection for image, sound and video

admissions to child care facilities

Data protection is an important issue in day-care centers

roll to. The inquiries we have received from parents over the years

and of institutions show that considerable legal uncertainty in handling

with data protection issues in practice. reach us

are always asked when and under what conditions film

and photographs taken and to whom these may be passed on.

A

and

s

i.e

e

right

P

right

a

x

i

s

As announced in our last annual report157, we have shared our

sam published with the Senate Department for Education, Youth and Family

Brochure “Data protection for image, sound and video recordings. What's in the

in the day-care center?" In the 2nd edition, it has been fundamentally revised

and adapted to the current legal requirements of the GDPR.158 Precisely because

in everyday pedagogical work there is often uncertainty as to how

increasing digitization of the protection of the personal rights of children

can be guaranteed, we would like to provide the pedagogical professionals with the

brochure provide assistance on how to deal with the particularly sensitive

157 JB 2019, 5.1

158 See the joint press release by the Berlin Commissioner for Data

protection and freedom of information and the Senate Department for Education, Youth and

family from 14 . Aug 2020; available at https://www .datenschutz-berlin .de/

infothek-and-service/press releases

active data of the children, but also of the employees in the facilities

can handle in a protective manner. The brochure was published at the beginning of the kindergarten year

sent by the Senate Administration to all 2,700 Berlin day-care

sent and can be obtained as a printed brochure from the Senate Department for Education

Education, Youth and Family and the Berlin Commissioner for Data Protection

and freedom of information can be requested free of charge. It is also available as a PDF

available for download on our website.159 In addition, the Senate

administration to hold a training course on the new data protection brochure.

The 44-page brochure deals with the following topics, among others:

related to image, sound and video recordings in day-care centers: data protection

regulation (legal bases and principles), data protection when recording

children (declaration of consent, recordings at events and in

agogic everyday life, scientific projects, publication by external parties),

Data protection of employees (requirement for the employment relationship,

dependent relationship from the employer) and media

competence in everyday teaching.

Children are under the special protection of the GDPR. We see it as

our task, in times of increasing digitization, from the outset

Protecting the privacy of our youngest. The feedback

to our brochure show us that it is a valuable

offers full support for their everyday practice.

4.3 Photos of children and young people

sporting events without consent

The parents

s

i

x

a

right

P

right

e

i.e

s

and

A

The Croatian supervisory authority has submitted submissions to a Berlin photographer

fenteam submitted. Several parents in Croatia had complained that

that the photographers specializing in sports and event photography

159 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/

information materials/2020-BlnBDI-Datenschutz_Bild_Ton_Video .pdf

92

Chapter 4 Youth and Education 4 .3 Photos of children and young people at sporting events

international children's and youth tournament in diving Pictures of the participating

minors had made and these via a website for

offered to buy. From this competition alone, around 18,000 pictures were taken by the

Participants published on the website. The children and young people

are shown on the photos mostly individually during their jumps. a

explicit parental consent for the preparation, publication and

Those responsible had not caught up with the sale of the pictures. As responsible

supervisory authority, we have been responsible for processing the complaint.

Photographs of people generally constitute personal data,

because the persons depicted can be identified directly or indirectly.160

For the processing of this personal data, in particular for the

production of the photographs and the further use of the recordings must be

the conditions set out in Art. 6 Para. 1 Sentence 1 GDPR must be met. the pro

Scripts of the DS-GVO only apply in exceptional cases if the photographs

are intended solely for personal or family use and

do not leave this private area.161 In view of the by the Berliners

Photographers professionally operated sports and event photography with the aim of

In the present case, however, the photos were then sold

a commercial activity.

The photographers responsible did not have the legally effective consent of the

affected persons or their legal guardians in relation to the

preparation and publication of the photos.162 An implied consent

approval of the persons concerned or their legal guardians

the mere participation in the competitive tournament is ruled out, as according to Art. 4 No. 11

DS-GVO for this a declaration of intent in the form of a declaration or other

term unequivocal confirmatory action is necessary.

The production and publication of the photos cannot be based on a legal

be supported on the basis. Article 6(1)(b) GDPR serves as the legal basis

not considered as taking the photos of those at the sporting event

160 See Art . 4 no. 1 GDPR

161 so called . "Household privilege" according to Art . 2 para. 2 letters c GDPR

162 See Art. 4 no. 11 and Art. 7 i . v. m . kind . 8 GDPR

participating children and young people is not the subject of a contract with

the persons concerned or their parents. A contractual relationship in form

the commissioning only existed between the photographers and the event

ter of the tournament.

The taking of photographs during the event is also not permitted

Art. 6 Para. 1 lit. f GDPR are supported. Although subject to the operation of

Photographers in the field of sports and event photography in general, professional and

Art freedom163 and represents a legitimate interest. Due to the official

Invitation or accreditation at the sporting event is also from a

Interest of the organizer of the children's and youth tournament in the documentary

tion of competition and thus of a legitimate interest of a third party

to go out However, these interests are subordinate to the

interests of the minors photographed. Especially with children and

After 16 years, the GDPR assumes a special need for protection

makes it necessary to involve the parental representatives.164 It follows from this

also for the weighing of interests according to Art. 6 Para. 1 lit. f GDPR, that regularly

the legitimate interests of the child concerned prevail.165

When weighing up the interests, it also had to be taken into account that not only

Parents of the affected children and young people found the images on a website

can be purchased, but in principle anyone. The pictures were

and are not stored in an internal or closed portal, but

freely available worldwide. The photos should therefore primarily be used for commercial purposes

interest and not only the interests of the children and young people in a

position of their performance or the sport.

We have now informed the Croatian supervisory authority that we are

due to the large number of persons affected, initiate sanctions

and request that the photos be removed from the website.

163 See Art . 15 and 13 Charter of Fundamental Rights of the European Union (GRCh)

164 See Art . 8 para. 1 GDPR

165 See Kühling/Buchner/Buchner/Petri, DS-GVO, Art. 6, recital . 155

Without the consent of the persons concerned or their educational

Authorized persons may not publish or sell the photos.

Even if the pictures are taken at a public event with an international

importance in the competitive sports sector is marketing

of photos of the children and young people in the present case not as a result

to be reconciled with the personal rights of those affected.

4.4 Evidence of mandatory measles vaccination in schools

and child care facilities

Since March 1, 2020, there has been one in Germany in certain contexts

Compulsory vaccination against measles: According to the Infection Protection Act (IfSG) it is compulsory for all children

and employees in schools, day care centers and other community facilities

proof of adequate vaccination protection. We have requests from

Parents, however, also receive institutions themselves, which show that the procedure

questions about the need to vaccinate in day-to-day practice. Again and again ha-

asked us parents whether their children's school or day-care center had copies of the measles

collect proof of vaccination.

A

and

s

i.e

e

right

P

right

a

x

i

s

The personal data contained in the vaccination cards is

It is health data that belongs to the specially protected categories of personal

personal data.166 Their processing is exceptionally permitted unless

far this for reasons of public interest in the field of public

health is required. The IfSG stipulates that community facilities

are authorized to request proof of measles vaccination protection167,

and are obliged to inform the health department if there is no sufficient

the proof was submitted.168 Even if the wording of the IfSG the submission

to the "management of the respective institution"169 does not provide it from

constitutes a violation from the outset if the measles vaccination certificate, e.g. the class

166 See Art . 9 para. 1 GDPR i . v. m . kind . 4 no. 15 GDPR

167 alternative proofs are listed in § 20 para. 9 sentence 1 no. 1–3 IfSG listed.

168 § 20 para . 9 sentence 1, sentence 4 or . Section . 10 sentence 1 and sentence 2 IfSG

169 § 20 para . 9 sentence 1 or . Section . 10 sentence 1 and sentence 2 IfSG

is presented to teachers. The purpose of the regulation is not that the service

tion personally carries out the data collection in detail, but that they

responsible for the process. The practice of some institutions that submitted vaccination

However, it is normal to make copies of ID cards and to keep the copies

not permitted. Because the copied page of a vaccination certificate regularly contains

Information about other vaccinations required for the purpose of proving a

adequate measles vaccination protection are not required. Instead, the

Set up confirmation of whether full proof has been provided or

not, note independently in a separate document.

Community facilities such as schools and day-care centers are authorized to

to have proof of measles vaccination protection presented. However must

the processing of this sensitive data takes place in accordance with data protection regulations. the

Practice of some schools and day-care centers to collect copies of the vaccination card

and keep it is not necessary and therefore not permitted.

4.5 Childhood House at the Charité – After-

improvement required

s

i

x

a

right

P

right

e

i.e

s

and

A

Shortly before the planned opening of the so-called Childhood House at the Charité

Universitätsmedizin Berlin, the Charité asked us to develop the concept

from a data protection point of view. In view of the considerable

In terms of data protection relevance, this was unfortunately far too short-term to

to implement protection requirements in good time before the planned opening

be able. It would have made sense to involve us in the project right from the start

pull, as it would have been possible in this way to comply with data protection law

Requirements to be taken into account right from the conception stage.

With the so-called Childhood-Haus (literally: children's house) the Scandinavian

navigable model of an interdisciplinary and cross-agency center

implemented for children who have experienced violence and a central contact point

be created. The aim should be to create a competence center for violence and/or

or abused children and adolescents who have already been investigated

development procedure is pending. The care of children and youth

agreed, the preservation of evidence and further support should be shared in this house

be bundled. This is a professionally certainly worth supporting

Issue. However, the cooperation of different people involved in a case throws up

Institutions such as child protection clinics, trauma clinics, police, state

Attorneys and investigating judges as well as youth welfare offices and family

set up data protection issues, if - as in the Childhood House - one

interdisciplinary exchange of information is planned.

We have the Charité on the problem of case conferences between different

n institutions that perform different statutory tasks,

made aware. Data transfers between all parties can only

be considered when powers for data exchange between

available to all institutions involved. However, given the very different

different tasks of those involved (criminal prosecution, child and youth welfare,

medical diagnostics) and different legal bases

not the case for data processing. Each institution is allowed only those data

become aware of what is necessary for their specific task. these are

e.g. B. for the youth welfare other data than for the police. So required the police

for their investigative work not that of the youth welfare office for the socio-educational
care of a family available sensitive data on certain family
conditions or possibly known in the context of medical diagnostics
knowledge gained. The exchange between different participants
must therefore be limited to what is absolutely necessary. This will be
difficult to succeed.
In this context, case conferences can usually not be held on the
perform on the basis of consents. Consent must be voluntary and
informed. It must be given to the legal guardian or the young
be made transparent which specific data for which if possible
precisely described purposes to all other participants in the case conference
passed on and what consequences may result from this.
This will usually not be possible in practice, since it is not
know what information is brought together during a case conference
be and what consequences may result from it. Also, the consent
ment with regard to data processing by law enforcement agencies is very tight
set limits.
97
The conception of the Childhood House envisaged a
rité to provide the person employed with a coordinating role in which the
Information on a specific case should be brought together. Also
here significant data protection issues arose because the bundling
all information on a specific case in one place is also available
contrary to the legal provisions applicable to the institutions involved
Data Processing Powers. These do not provide – for good reason –
that z. B. medical information from the child protection ambulance or the

Trauma outpatient clinic, the data available from the youth welfare offices and the

information known to the law enforcement authorities without further ado.

which may be linked.

We have informed the Charité that fundamental changes to

the conception of the so-called Childhood House are necessary for the project

to be able to implement data protection. It is primarily about that

the goal associated with the Childhood House, the children and young people with

To provide the best possible care for experiences of violence and abuse, to

moves within a permissible data protection framework. Especially in such a sensitive

active area, it is essential that those affected and their families

trust that there will not be a comprehensive

rich exchange of data over which they no longer have any influence

and the potentially unexpected and unwanted ones

could lead to consequences. In the meantime, the Charité has given us a

updated concept. On this basis we will provide further advice

carry out with the parties involved.

98

Chapter 4 Youth and Education 5 .1 Amendment of the State Hospital Act

5 health and care

5.1 Amendment of the State Hospital

legal

With the Berlin Data Protection Amendment Act-EU170, the state law

numerous state laws to the European legal ones in one fell swoop

Adapted to the requirements of the General Data Protection Regulation (GDPR). to these

also included the State Hospitals Act (LKG). In his novella

much has been achieved. Unfortunately, the final vote on this is just around the corner

law, a fatal change from a data protection point of view without the necessary advice

tion has been inserted.

A

and

s

i.e

e

right

P

right

a

x

i

s

The LKG contains special data protection regulations for Berliners

Hospitals.171 They determine, among other things, who the hospitals

are allowed to disclose data and under what conditions hospitals

ser when processing their patient data on external service providers, so-called.

processors.172

We were involved in the development of a draft of the amendment to the law by the

national administration for health, care and equality

been. The aim was to offer hospitals new options for processing

to open up the processing of patient data that is necessary in everyday clinical practice

have proven without lowering the level of data protection. Therefore also found

an exchange with representatives of the hospital sector took place several times.

The version of the law valid until the end of 2020 stipulated that patient data

Basically only in the hospital or on behalf of another patient

kenhaus were allowed to be processed. Processing by other bodies

on behalf of the hospital was permitted only if by technical

170 BlnDSanpG-EU; see GVBl. 2020, p. 807-828

171 §§ 24, 25 LKG

172 § 24 para. 7 LKG

Protective measures ensured that the contractor had no way

had to establish the personal reference when accessing the patient data.173

A disclosure of patient data associated with the assignment

private companies that are not a hospital themselves were therefore ruled out.

From a data protection point of view, this regulation was not objectionable

to a special degree the high sensitivity of the pa-

client data invoice. Also with a view to European developments,

therefore the entry into force of the GDPR, there would have been no change in this point

tion required. Rather, the DS-GVO even expressly provides for the member states

subject to the possibility of additional conditions, including limitations

gene, to introduce or maintain, as far as - as here - the processing

is affected by genetic data or health data.174

From the point of view of many hospitals, however, there was an urgent one

Request for an "opening" of order processing in order to - of course also from

economic considerations - more flexible in the future when integrating external

to be a service provider.

One of the desired innovations was the permit, including subsidiaries

(or other companies in the same group of companies).

allowed to. Another was the involvement of service providers for the operation and

the maintenance of the complex information and medical technology of the hospitals

ser.

With regard to the second point in particular, it is understandable that hospitals

not have the necessary in-house expertise for the entire technology

can hold. Therefore, the use of external expertise should be made possible

will.

In principle, however, patient data must be

activity in the hospital and under his control. A concentration

of patient data in the hands of fewer cloud service providers would

173 According to the old version of § 24 para. 7 LKG

174 art. 9 para. 4 GDPR

pose dangers. The dangers are not only that the data

collections from these service providers would represent an attractive target

the. They are also in the nature of service providers who have a vested interest in the

evaluation of the processed data. In addition, many cloud services

directly or indirectly through service providers from corporate groups

brought, which have their headquarters in the USA and thus access US American

exposed to Canadian authorities.175 An outsourcing of patient data

to service providers without a direct connection to the hospital sector and without input

We therefore reject the patient's understanding and possibility of intervention.

After several years of coordination and discussion between

between the responsible Senate Administration, the Senate Chancellery and our house

Finally, a draft regulation was created that serves the interests of all

shared account. In particular, the new regulation stipulates that the

Contractor does not necessarily have to be a hospital itself. A lot of-

more it is sufficient if the commissioned service provider of the group of companies

belongs to a hospital. In this way, the hospitals

possible to outsource processing activities to own or subsidiary companies

to outsource their hospitals.176 These new regulations are clear

beyond the previous possibilities, without sacrificing the protection of sensitive

Losing sight of patient data.

So all is well that ends well? – Yes, there isn't a catch.

Because the new regulation of order processing occurs in contrast to all

their changes to the LKG only two years after the promulgation of the BlnDSanpG-EU,

i.e. H. came into force in October 2022.177 This is due to a still

amendment tabled at the last minute by the coalition factions.178

This hasty action is not understandable. As a consequence, she has to

resulted in the LKG not having any area-specific

175 See 1.2

176 See § 24 para. 7 LKG

177 art. 57 para. 2 BlnDSanpG-Eu

178 Abghs .-Drs . 18/2598-1 from 1 . October 2020

specific regulation for order processing. At least they apply

temporarily only the general regulations of the DS-GVO.

A specific reason for this change was not given to us, nor

is she known to us. If there were any fears that

the new regulation stands in the way of increased cooperation between hospitals,

In any case, this assumption is completely unfounded and incomprehensible.

In our consultations with the hospitals, we will work towards that

the new regulation on order processing before it comes into force

respect. We can only appeal to the insight of the hospitals

to be clear about the dangers of all these, among the most sensitive

ten data counting patient data are exposed. Is the data first

once they fall into unauthorized hands, they can – e.g. B. after expiry of the

transition period - can no longer be retrieved. The impact on the

Patients could be serious.

5.2 New developments in the Charité saga

s

i

x

a

right

P

right

e

i.e

s

and

A

For several years, the Charité has been trying to process our

posed profound deficits. You will be closely accompanied by us. In this

There were initially long delays. But at the end of the year,

Cleaning up the deficits is finally gaining momentum.

As already reported in detail in previous years179, exams

in the years 2015 and 2019 at the Charité profound deficiencies in compliance

compliance with data protection regulations. The Charité presented in

After consultation with us, we drew up plans to rectify defects and have been working on them since then

systematically. This year, too, there were considerable delays

some of them are undoubtedly due to the demands placed on the Charité by the co-

vid-19 pandemic. But even in times of low infection rates

progress is low. This only changed in the fourth quarter.

179 JB 2019, 6.2; JB 2018, 6.5; JB 2017, 7.5; JB 2016, 6.1; JB 2015, 8.4.1

Like all controllers who process sensitive data on a large scale,

the Charité must determine the risks in a systematic process,

on the one hand their patients in the data processing

support, documentation and billing of the treatment and on the other hand

their subjects in medical research projects

are exposed. Such risks exist e.g. B. in the disclosure of patient

nominal data to unauthorized persons or the unlawful disclosure of the identity of

Test persons in research projects. For each of these risks

Appropriate and effective measures are to be determined and implemented, with

which reduce the likelihood that the processing

realize the risks associated with this data and mitigate the impact

be changed if a data breach occurs.

The process to be completed is stipulated by the (European) legislator

given and referred to as a data protection impact assessment (DPIA). Last year

In 2019, the Charité carried out the first DPIA. The results stayed

but sometimes far behind the legal requirements. We have the

Charité therefore supports the creation of a model DPIA and a

Sample outline provided. From September, the Charité started up

the basis of the pattern and further hints given by us finally there-

with creating meaningful DPIA reports.

She left two big gaps open:

Initially, it followed the pattern for clinical procedures only. Only at the beginning of October

However, we received the first halfway adequate DPIA reports, also for research

research project – five years after the lack of risk analyzes and

Concepts for the technical and organizational measures to be taken

men was first detected by us. By mid-2021, too

Thirty DPIAs are created in the research area for various research projects

the. In doing so, they should provide a cross-section of the different types of research

project and serve as blueprints for other projects. The procedure

makes sense, but the plan completely ignored the fact that new

research projects are to be started. For these new research

upstream DPIA were by no means planned from the outset. we

the Charité therefore had to point out that new projects could not be

103

fulfillment of the legal requirements may be tackled. It

will not be able to come to terms with past omissions if

not for current and future data processing from the outset

legal requirements are observed.

The second major gap extends to the risks arising from the use of the

technical infrastructure of the Charité arise, and on the functionalities that

must provide this infrastructure in order to be able to

safeguard the rights of the persons concerned and the data protection principles

to be able to comply with the rates.180 Neither did the Charité succeed in analyzing the

relevant to individual processing activities, stemming from the infrastructure

the risks nor the determination of the functionalities to be provided centrally

ten, as z. B. are necessary for finding all copies of data that are

relate to an individual exercising their data protection rights. We have

a separate test procedure was included for this purpose.

On the other hand, the Charité made some significant progress in relation to the

legal protection of data about patients and their treatment

has been completed for a long time. Now employees will at least

warned against accessing such data. A complete exclusion of

Accessibility will only take effect if appropriate technical and

organizational rules ensure that in the case of a re-stationary

Admission, outpatient treatment or demand for post-treatment

directions then delay the required patient data

are freely available. After all, the Charité has at least partially

created the conditions for using the data from the outpatient

Delete an action whose retention period has expired. First deletions

were made.

The Charité still has the task of collecting data that has been built up over

to eliminate deficiencies in protection. Further delays, insofar as they do not result from one

medical emergencies are unacceptable.

180 See 17.3

5.3

(Un)safe ways for patient files

We were made aware of a procedure by a hospital in which a

Service provider for the medical services of the health insurance companies (MDK) in one

Mass procedure accepts patient data from hospitals. we

then checked the security of the procedure.

In the course of treating their patients, hospitals process

a large amount of health data. This is necessary in order to

to be able to carry out the development in the best possible way. to treat them as strictly confidential

the patient data may contain information whose disclosure is permitted

can have serious consequences for those affected.

A

and

s

i.e

e

right

P

right

a

x

i

s

As part of their statutory mandate, the MDK review invoices from

medical services for a large proportion of treatment cases. In addition

ask for medical documentation about the treatment. This

previously in paper form. With the passing of the MDK reform law

was regulated that hospitals from January 1, 2021 this data transmission

ment in electronic form.

The MDK have a common to receive the transmitted data
technical platform set up and its operation to a joint subsidiary
company based in Berlin.181 This company is responsible for the
responsible for the security of the processing carried out by him.
In the electronic transmission of countless personal data sets
with health data via the open Internet, there are high risks for the
confidentiality of this data. It is therefore necessary to provide the data sufficiently
encrypt to the acknowledgment and a possible misuse by
exclude third parties.
The method used only saw the encryption of the communi-
communication channel between the hospital and the platform using standardized pro-

181 See § 80 SGV X

demonstrate how they are also used to establish the connection between a web
browser and a website to encrypt. Given the high risks
this is not sufficient. Even if the encryption of the communication
as error-free - and in the past several weak points have been
uncovered, the exploitation of which gives third parties access to the communication
content would have made possible – the data are at the end points of the connection
nevertheless always unencrypted. With that, they continue to represent exceptionally
productive and thus attractive targets for cyber attacks.
In addition, end-to-end encryption must therefore be used. This
has the effect that the data is encrypted before it is sent in such a way that only
the recipient, i.e. in this case the responsible MDK, decrypt the data
can. He can do this on a section of his computer network that is not
directly connected to the Internet and specially protected. corresponding

Accordingly, the hospitals can already use the encryption in an internal

internal network. The handover to the platform can then be done by a

less secure, directly connected device.

This procedure corresponds to the prior art and is in view of the

proportionate to the existing risks. We have therefore contacted the operator of the platform

form prompted, in addition to the already existing transport encryption

use end-to-end encryption.

Special care is required when transmitting sensitive health data

required to protect confidentiality. This is all the more true when

a large number of patients are affected. There is one for this

use end-to-end encryption.

A

and

s

i.e

e

right

P

right

a

x

i

s

5 .4 Disclosure of health data to the immigration authorities

5.4 Disclosure of Health Information to the foreigners Authority

In one petition it was stated that a treating clinic doctor contacted the state authority and informed them that the complainant rer after consuming various drugs in the rescue center there had been included. The complainant asked us to examine it.

At our request, the clinic informed us that the complainant was taken to the hospital unconscious in an ambulance. an accompaniment Tender acquaintance stated that he had various alcoholic drinks that evening consumed drinks and ecstasy. However, the existence of a ner language barrier when communicating with the accompanying person whether the complainant had previous illnesses, allergies or chronic suffering from physical illnesses. He was then in the clinic for further treatment ment was transferred to the intensive care unit. Because of the unconsciousness he was been unable to provide any information about himself. Also be his Accompanying person was no longer available for questions. The clinic laid understandable to us that the necessary information about any suicide quality, external aggression and previous psychiatric illnesses were necessary and could only be obtained through information provided by third parties. A deportation Scheid was the only document that could be found on the complainant's so that contact was made with the issuing foreigners authority for clarification had been. However, the immigration authorities were not given any medical details informed about drug or alcohol consumption. To dangers for the Complainant himself and any endangerment of the clinic staff To avert tendencies, it was necessary to contact the immigration authorities record.

This reasoning made sense to us. The admissibility of the processing

processing of personal data was based on the provisions of the DS-GVO i. V. m. the

Support LKG.182

182 Art. 9 para. 2 letters c GDPR i . v. m . § 24 para. 5 no. 3 LKG in the up to 24. October

2020 applicable version

Sensitive patient data must be handled with care. This applies in particular

their for passing them on to third parties. In the course of our examination it turned out

out that in the specific case the transfer to the immigration authorities

was to be regarded as legally permissible after a weighing of interests.

6

integration, social and

work

6.1 Complaints office for refugees

needs privacy

In our last annual report183 we informed that the

National Administration for Integration, Labor and Social Affairs is planning an independent

to create a difficult place for refugees who have "low-threshold"

complain about facilities or about processes in connection with the

should accept accommodation. In the first place, in terms of data protection

From a legal point of view, the problem that the complaints office after the planning

should process extensive personal data, a legal

However, there is no specific assignment of tasks to this position. The processing

of the data can only be based on the lack of a legal basis

consent of the complainant.

A

and

s

i.e

e

right

P

right

a

x

i

s

Basing the processing of personal data on consent raises

difficult questions in practice. A consent can only be effective

be informed if done. This is the case if the complainant

who can classify what effects the granting of consent will have for them

are connected. This includes the circumstances of the data processing

must be completely and specifically recognizable from the declaration of consent.

A declaration of consent can only serve as the basis for data processing

used if these requirements are met. For the data transfer

processing by the complaints office, this means that the declaration contains all

All data processing processes must be named in detail.

We have discussed this problem in detail with the Senate Department for Integration,

Discuss work and social affairs. Our recommendation from the start was to

to place the authority of the complaints office on a legal basis and

Consent should only be regarded as a temporary solution. Since it was planned
to put the complaints office into operation as soon as possible, the pre-printed
cke for the declarations of consent and the accompanying information
ben in an intensive consultation process between the Senate Administration and
matched us. The strict requirements for consent are now
Fulfills. Due to the corona pandemic, the originally planned for 2020
delay the planned start-up of the complaints office, but stand still
the data protection requirements no longer prevent the start.
We expressly welcome the fact that the Senate Department for Integration, Ar-
work and social affairs the consent solution is only offered for a transitional period
would like and intends to contact the complaints office, our recommendation
to be anchored in state law in a timely manner. It is very gratifying that we
the Senate administration a first draft for a corresponding regulation
very early on, so that the data protection regulations
can be taken into account for a long time from the outset. We will draft
review and constructively advise the Senate administration in the further process.

6.2 Accommodation for the homeless - not without
privacy

s

i

x

a

right

P

right

e

i.e

s

and

A

The project "City-wide control of accommodation" (GStU) is a

important project of the Senate in the field of social affairs. With the project by the

Senate Department for Integration, Labor and Social Affairs is realized, the

housing situation for homeless people to be improved. Future

are to be allocated places in accom

that are specifically tailored to their needs. Here should

city-wide capacity planning and occupancy control using a

central IT technical procedure. In addition, a central data

basis can be created in order to carry out statistical evaluations. The goal,

the needs-based accommodation of homeless people throughout the city

Controlling and organizing "at the push of a button" is understandable. Since this

However, extensive processing of particularly sensitive data also takes place

should, such as B. Information about diseases or disabilities or the

sexual orientation, is a special consideration when implementing the project

pay particular attention to compliance with data protection requirements.

Unfortunately, our authority only got involved in this important project in the summer

been bound. This is surprising against the background that the Senate

National Administration for Integration, Labor and Social Affairs in 2016 with the development

development of a suitable set of instruments and the project assignment in July
decided in 2018. It was not until September 2020 that the Senate Administration gave us the
provided the documents necessary for our examination. It turned out
then there is still a fundamental need for clarification on many points, in particular
more about the roles of those involved. Taking care of the homeless people
and their assignment to suitable accommodation takes place - depending on the
legal relationships - either through the social housing assistance of
Districts or through the State Office for Refugee Affairs. Next to it should
later a "Central Service Unit GStU" will be set up, which will be responsible for both the
contract and accommodation management as well as for billing and quality
quality assurance should be responsible. The decision on the organizational
However, a precise location of this service unit has not yet been made. First should
the Senate Department for Integration, Labor and Social Affairs take on this role.
The Senate administration is planning a pilot project with two district offices at the beginning of 2021
and the State Office for Refugee Affairs. It should
be allowed to use the accommodations already in the state of Berlin for
IT specialist procedure184 used for another purpose. The responsible
The Senate Department for Integration and Labor is responsible for this procedure
and take on social issues.
Complex questions arise from the point of view of data protection law: On the one hand,
take into account that the parties involved have different legal duties
according to asylum law, social law and security and regulatory
perceive correctly. This also means that different legal bases
for the admissibility of the processing of personal data

184 This is a report from the Senate Department for Education, Youth and Fa-
milie used for the accommodation of unaccompanied minor foreigners

IT procedures .

111

have to be taken. In particular, it should be borne in mind that it is for

needs-based accommodation may also be relevant, sensitive data, e.g. B.

about illnesses or disabilities, etc., to process. To the admissibility

the processing of such data must be subject to strict requirements. To the

others, with regard to the IT process used, is due to several participants

to define exactly who may access which data, how the responsible

between those involved is regulated and for which processing

gene agreements on order processing between the parties involved

are close.

All in all, extensive data protection assessments are required here.

gen. We are in contact with the responsible Senate administration

to clarify data protection issues before the start of the pilot project. Also

we will discuss the next project steps in particular with regard to the

associated with the planned establishment of a "Central Service Unit GStU".

accompany data protection issues and the senate administration

advise accordingly.

6.3 Household surveys and the thing with

of anonymity

s

i

x

a

right

P

right

e

i.e

s

and

A

We were informed of a planned household survey by a tip

district office carefully. The questionnaire, according to certain characteristics

randomly selected citizens were asked to answer voluntarily received one

Variety of personal questions, the level of detail of which requires an identifiable

ability of the participating citizens for the district office, at least theoretically

made possible. In the cover letter to the citizens, the district office awakened

however, the incorrect impression that no one could establish a connection between

the participants and their answers.

The survey was aimed at senior citizens and should be given to the district

serve as a basis for further planning (e.g. for housing

care, leisure activities or the expansion of medical and nursing

services) in the realities of life of this population group

judge. However, the attached questionnaire had it all: queried

were e.g. B. Highly detailed personal information (e.g. age, specific

amount of net income, year of moving to the district), on the housing situation

(e.g. number of rooms and square meters in the apartment, total, heating and

operating costs), the state of health (e.g. chronic diseases, degree of

disability, degree of care) and much more. An identifiability of

Due to this wealth of information, individual participants could
cannot be excluded here. That was from the accompanying cover letter
to the participants, with whom they can discuss the background of the survey
should be clarified, but not highlighted. Rather, originally even ex-
implicitly stated that no one allegedly established a connection between the
participants and their answers.
When we intervened, the district office informed us that an evaluation
of the individual questionnaires by the district office itself is not planned. These
who sends it back to the district office, but from this in a closed
The envelope is passed on to a service provider who reads it by machine
and destroy immediately afterwards. The district office only receives a number
meric evaluation. The same applies to those with the district office at this one
University cooperating with the project, which based on this evaluation
should create a study.
The district office then sent the information letter to the citizens
changes and transposes this procedure in a new version of the cover letter
parent made. The processing of the data collected with the questionnaires
based on the consent of the participating citizens.
However, the procedure was not ideal. Although the district office in which
revised cover letter waived the inaccurate note that never
to establish a connection between the participants and their answers
could ask. The indication that participation in the study is "anonymous"
however, was retained. On closer inspection, however, this was still the case
incorrect. Even without collecting the names, it is possible to identify
tion of individuals given the scope and level of detail
of the questionnaire is by no means excluded. In this context

The question therefore arises as to whether the consent of the data subjects is still valid

113

can serve as a basis for data processing if the state of affairs in this

point is not reproduced correctly.185

We have alerted the district office to the problem. Since the district office

due to the chosen procedure, however, actually no knowledge of the

individual data sets, but rather the envelopes in the sealed

envelope, we have in this specific individual case under two

conditions apart from further measures: On the one hand, the district office has

to ensure that there is no insight into the individual

questionnaires is possible. On the other hand, it had to be ensured that the

together with the provided "numerical evaluation" in a way

It is generally understood that it is no longer possible to draw conclusions about individual persons

is. Only in this case is it really anonymous data. In addition

we advised the district office to use this environment for future projects

to be included in the planning at an early stage.

Basically, we recommend increasing the level of detail for similar surveys

be drastically reduced in order to be able to relate to persons from the start

shut down. If no or insufficient use is made of this, the

affected persons are again not suggested to take part in the study

successes anonymously. Furthermore, when designing the process from the outset

consider whether the district office is actually the "recipient" of the questionnaires in

should come. There is usually no need for this if the

Questioning not by the district office itself, but by a third party (e.g.

a university) is scientifically evaluated.

In principle, household surveys are a legitimate means of

an overview of the living realities of individual population groups

pen and in this way to enable them to carry out their planning

align with this. Despite all the thirst for knowledge, the data protection laws

However, aspects of such studies need to be considered from the start.

185 Consent must include: be given in an “informed manner” in order to

to be able to legitimize data processing; kind . 4 no. 11 GDPR.

6.4 Submission of official files to the Neighbors

A law firm drew our attention to the fact that the

The package deliverer, who is also responsible for health and social affairs, takes the package with you

the official files containing sensitive health data, in the case of

barn, as nobody was to be found in the office.

It turned out to be a common practice. we

have both towards the State Office for Health and Social Affairs as well

to the person responsible for organizing the Berlin-wide parcel delivery

literal State Administration Office made it clear that packages, the documents

with sensitive data such as health data, only to the respective

authorized recipients personally or to named authorized recipients

may be delivered. We were told that the contractual

conditions did not allow personal delivery of parcels

ensure. Personal delivery is only possible for letters.

After an intensive exchange with the authorities involved, we were able to

achieve that now through the conclusion of an additional agreement

is guaranteed that the state office for health and social affairs in packages

Always hand over the files sent personally to the receiving offices

will.

6.5 Nursing service publishes names of

dependent

One complainant was surprised to see her name on the internet

to find the page of the care service taking care of you. She asked us for support

tongue.

It turned out that the nursing service divided its nurses into groups for

training courses had been assigned. The nursing

service to those in need of care they care for. Because the nursing service

Made training plans for all teams available on his website, that's what happened

115

A

and

s

i.e

e

right

P

right

a

x

i

s

A

and

s

i.e

e

right

P

right

a

x

i

s

to the publication of the complainant's name. The Nursing Service

explained to us that for easier assignment, the teams would be named after the

named persons to be cared for. We informed the nursing staff that it

this is an inadmissible publication of sensitive data and the

data to be deleted.

The nursing service was very insightful and has used other terms since then.

drawings for the training teams. This will address privacy concerns

of those involved are now taken into account.

Chapter 6 Integration, social affairs and work 7 .1 The police, your friend and researcher

7 science and

research

7.1 The police, your friend and investigator

The Berlin police have been involved for several years as part of a research

research project to find out which test procedure you can use to test people in

one's own ranks can identify the exceptional and for the

Police use particularly relevant skills in the recognition of

faces (so-called "Super Recognizer"). The police receive support

shown by a scientific body specializing in this subject area.

from the University of Friborg (Switzerland). We have the police all over the place

period of the project and worked towards ensuring that the research

also intend to comply with the data protection framework

will.

A

and

s

i.e

e

right

P

right

a

x

i

s

Accurately recognizing people in photographs or video recordings,

that you only met fleetingly once – maybe even years earlier – is for

impossible for the vast majority of the population. Not so for "Super Re

cognizer", who should be able to do exactly that on a regular basis. How many people actually

It is not possible to say with any certainty whether they have such abilities. estimate

According to genes, it should be at most one to two percent of the population.

The fact that the police in particular have a special interest in carrying out a test for

Developing verification of “super recognizers” is not surprising. After her

prognosis, these exceptional talents could advance police work quite a bit.

gene. For example, they could also put a wanted person on the recordings

identify a surveillance camera if they are in a larger one

crowd stops. This should not least include the reconstruction of escape

because of facilitate and would be according to the police z. B. also after

Attack on Breitscheidplatz in 2016 was a great help in the manhunt

been.

117

As the research project raises significant data protection issues

are, the police approached us early on and gave us theirs

Considerations for the design of the test procedure are presented. This stipulated that

the participants go through several modules that develop their skills

put visual recognition to the test in different variants. To the

For example, one module stipulated that the test subjects should have 20 good-quality images of

similar-looking people and underneath a target

have to find someone again. Only people who pass a module should go to the

to be “let ahead” of the next.

The data protection problem? For the creation of the tests wanted the

On the one hand, the police resort to “real data”, i.e. authentic image material

(e.g. from the police photo file or from investigative

files of the public prosecutor's office). On the other hand, she wanted to take advantage of that

with around 24,000 employees, they have a large pool of potential pro-

bands.

Both the use of photographs from police databases and

from files of the Berlin Public Prosecutor's Office for research purposes is

under protection law, even without the consent of the persons concerned,

barred in. However, it is linked to specific conditions. In addition

heard in particular that the purpose of the research project is not also on

can be achieved in other ways. In addition, the public interest in the

implementation of the research project, the interests of the affected

fenen people significantly outweigh.186

Against this background, we had to comply with the data protection law for the first planning

certify inadmissibility. The police were able to plausibly demonstrate that

the purpose of the research project cannot be achieved in any other way

the can. The fact that it is difficult to

such a large number of volunteers to take photographs or vi-

to win deodorant shots in order to draw enough test subjects from this pool

to be able to filter out those that show the required similarity to each other.

The fact that the test reflects actual everyday police work also played a role

186 See Section 35 BlnDSG and Section 476 StPO

should, i.e. the images had to look as authentic as possible (e.g. through

different qualities).

However, the also necessary weighing decision was made here first

at the expense of the police. That there is an important public interest in the

We do not dispute the carrying out of the research project

placed. However, it had to be taken into account that the images also represent the potential

purposefully stigmatizing information that the people depicted

who had been processed by the identification service in the past. In addition

was the legitimate interest of the data subjects in the original

chen planning particularly affected by the fact that the

Photographs of up to 24,000 employees - this corresponds to the population of one

small town – should be presented.

However, we have also signaled that the consideration in favor of

interest in research could fail if far fewer test subjects were involved

“real data” would be confronted. We suggested e.g. B. a pre-test

to be integrated into the study structure that does not contain any authentic material and

with which at least those participants are filtered out from the outset

can be, which definitely does not have the special skills you are looking for

feature.

The following procedure was finally developed by the police: Decide

If the law enforcement officers decide to take part, they must now take part

complete a pre-test consisting of three individual tests, which does not contain any material from the

databases of the police or files of the public prosecutor's office. personal

Those who achieve a certain level in all three tests can then take part in the

Also complete the first test module with authentic image material. To-

the intensity of the data protection encroachment of the first test module is re-

been dubbed. Now it is provided that in the authentic footage

also pictures of volunteers are interspersed. That's how it is for the subjects

It is not clear whether the people shown to them are actually recognizable

have been officially treated. The legitimate interests of those affected

People are far less affected.

119

As a result, we agreed to this course of action.

However, this assessment relates exclusively to the processing of the in

Data in question for the research project carried out. Is the goal of

project, i.e. the development of a scientifically valid test

rens to identify "Super Recognizers" for police operations

new assessment required. The personal data used in the test

related data cannot subsequently be used for

tere "Super Recognizer" in the ranks of the Berlin police, at police authorities

other countries or, for example, at the Federal Criminal Police Office. Because the

pure identification of "super recognizers" for the purpose of use in the police

time service is no longer used for scientific research.

Also personal data contained in police files and databases

and public prosecutor's office are not available for research in every case

taboo. From the outset, however, special attention should be paid to

that the interests of the persons concerned, which are worthy of protection, are special

get attention.

s

i

x

a

right

P

right

e

i.e

s

and

A

7.2 Research in youth welfare offices – “What to do

Are you there right now?”

The Senate Department for Education, Youth and Family informed us about

that a university in Lower Saxony is interested in offering a study

to be carried out in Berlin youth welfare offices. Since this also applies to data protection

Any questions that arose, she asked us for advice.

The target of the study are not children or young people, but the employees

youth welfare offices themselves. This is intended to analyze how the

used IT applications busy case processing and decision-making

influence finding.

Various methods should be used for the investigation. Next to

Interviews with employees should include them in every sense of the word

be looked over the shoulder. But that's not all - also a phase

Wise filming of the monitors was part of the study design.

The data processed in the youth welfare offices is

particularly sensitive social data. A transmission of this data – and

this also includes enabling the acknowledgment and filming

Third - is only under the narrow conditions of the Social Code (SGB)187

allowed. Above all, these requirements include that the transmission

ment of the data for a specific project of scientific research188

must actually be necessary. It failed here because of that.

We were able to infer from the researchers' concept that the image

screens are to be filmed. However, when asked, it turned out that

For the researchers, it is only about the interaction of the employees with the

software went; the personal data themselves were irrelevant to them

tion. These should be after the planning before the actual evaluation anyway

be made unrecognizable.

As a result of our indication that we would not film the film against this background for our

admissible, the university has changed its concept. Now on to that

No filming of the monitors. Instead, the employees should

Commenting on actions verbally, i.e. communicating what, similar to a soliloquy

they are doing.189

Provided that the employees are very precisely instructed in advance

are rued not to reveal any social data when commenting, and the

Scientists also do not use this data in their on-site observations

became aware of it, we have agreed to the procedure.

The processing of the personal data of the youth welfare office

(e.g. in the context of the interviews) is only possible on the basis of their consent

possible. In this context, we have made it clear that the

187 See in particular § 75 SGB X

188 Specifically, it must be a project of scientific research in the social

general performance area or scientific labor market and career research

act .

189 “Thinking out loud” method . Example: “I have a case here that has been used as a

was critically assessed. I'll click on the XY box now to see what

at that time the reason for reporting was .”

Consent can only serve as a basis for data processing if

this is also based on a free decision of the employees. Just in

employee context, it must be ensured that the skilled workers do not

some of their employers have to fear if they refuse to take part

decide.

We welcome the fact that the Senate Department for Education, Youth and Family

in good time in the project on the work of the employees of youth welfare offices

integrated with IT applications. In this way, an appropriate

right solution can be found.

122

Chapter 7 Science and research 8 .1 360 degree feedback in the workplace

8 employee data

protection, unions,

recruitment agencies

360 degree feedback in the workplace

8.1

With a so-called 360-degree feedback, the work performance of employees

evaluated by several people, some of whom are in higher and some in

are in lower positions. A possibly more accurate assessment

the work performance is countered by the risk that the processing will

related data is inadmissibly expanded.

A

and

s

i.e

e

right

P

right

a

x

i

s

Normally, employees receive performance reviews at regular intervals

judgments by superiors. Regarding executives, there has been some

Decades, the tendency to get different perspectives on their work:

In addition to the assessment by superiors, a self-assessment is carried out

demanded of the manager; In addition, employees give

how colleagues from other parts of the company make an assessment

division to the respective person. Depending on the methods used

a more comprehensive picture of the activity of the manager can be created. at

Executives are recognized that because of their position, this type of performance

assessment is generally permissible.

Recently, this concept is sometimes also applied to employees without or with only

assigned to subordinate managerial tasks. Here, too, a triad is made

Reviews obtained: First a self-assessment, then assessments

by colleagues from different areas and finally

an evaluation by supervisors. The companies that use this

are pursuing similar goals as in relation to executives. That

Overall, feedback should be more comprehensive and accurate, Employees with

special abilities or support needs can then be specifically

speak and be used better according to their abilities.

123

As advantageous as such processes are on the one hand in the constant development

development of organizations can be just as problematic on the other

Page the assessment by several people for each employee

be. In other words: In case of doubt, an employed person must not only
always expect that your relationship with your boss will
keep the next testimony influenced, but also with every encounter
another person in the company, since these encounters also have an
effects on the next appraisal and thus also on further professional life
could have. The result can be permanent monitoring pressure and stress
be that arises from concerns about professional advancement.
In the procedure we examined, employees, in consultation with their
direct superiors who are to evaluate them. the
Individuals could refuse if they found them unsuitable
held. At the same time, they should make sure that the selection is as different as possible
different people and functions. All workers were in it
trained to include only professional contexts in the assessment and to
assessment to proceed as considerately and objectively as possible. Above all
the work of the person to be evaluated should be described. When introducing the
Methods were also able to score points for strengths and weaknesses on a scale
be given.
The evaluations given in this way were given by the superiors
reviewed and supplemented by their own summarizing assessment, which also
could deviate. The final decision on the assessment was made
special panel, which also informed the evaluated person of the result. at
In the event of discrepancies, an arbitration board could be called in. One
non-participation in the procedure, whether as an assessor or assessed person
no negative effects so far.
A 360-degree feedback is not fundamentally impermissible, but
data protection regulations are complied with. This means, above all, that

Workplace no permanent monitoring pressure may arise that on the

principle of data minimization is respected and that the classic

rights, such as B. the right to information, must be ensured.

Based on these specifications, we checked the specific system and

take asked to make various changes. This prompt

it came up.

In order to counteract permanent monitoring pressure on employees

on our recommendation

the number of people rating another person is reduced to three.

In addition, the person to be evaluated must now communicate with the persons who

rate them, too, agree. The data subject can use the

tend not only to propose themselves, but also to veto when in doubt

lodge a complaint against people she does not like.

In terms of the content and scope of the assessments, it was clear that the assessors

have adhered to the specifications and have not made any unnecessary or irrelevant

have incorporated considerations into the assessments. The point scale was

recognized by the company itself as not very effective and abolished. the

The storage time of the ratings has been significantly reduced by removing the data

storage has been refrained from for several cycles. Well can

basically only to the evaluations of the previous cycle

be resorted to in order to understand developments and discrepancies if necessary

to be able to. Excluded from this is the end result: This may be like a

regular reference to the personnel file and for the duration of the

employment relationship are saved.

The question of how to deal with requests for information from employees was somewhat more complicated.

to deal with. The company found it problematic that reviewed

Insight into all created ratings and possibly also into the comments of the am

End advisory bodies received. One concern was that the evaluators

with a comprehensive right to information might no longer trust

to formulate the evaluation honestly. Unwelcome ones were also feared

Effects on the personal rights of the assessors. Since the

tending persons, however, perform a task of the employer by

They cannot do preparatory work for a job reference

predominate. However, we have considered two limitations to be permissible:

On the one hand, it is possible to obtain complete information only after the end of the

to issue an evaluation cycle so that the evaluation process is not influenced

125

becomes. On the other hand, no information about the ratings of subordinate

are given to people, since they might otherwise have concerns, such a

take on the task and give an evaluation.

As before, employees who are neither evaluated nor evaluated

If you want to take part in the evaluation system, you do not have to fear any disadvantages.

Due to the restructuring of the procedure, we are keeping it in its current

ellen form now for admissible.

Assessments by colleagues may be included in the assessment of the

work performance of employees if the process and content

is made transparent, personal data only to the extent necessary

be collected and stored and a permanent over-

security pressure is avoided.

8.2 Does data protection law limit the collection

tive rights of employees?

s

i

x

a

right

P

right

e

i.e

s

and

A

A trade union has a company agreement with its central works council

closed, by the addition to the legally standardized personnel representatives

executive bodies the position of a women’s and equal opportunities officer as well

was probably created at the district as well as at the federal level. After entry into force

enter into the General Data Protection Regulation (GDPR) was the union of

believes that she does not know this women's and equal opportunities officer

afterwards transfer personal data such as application documents

may.

The union took the view that for the transfer of

were no longer a legal basis. Only required by law

Committees such as works councils or representative bodies for the severely disabled should

receive these documents.

Both European data protection law and the Federal Data Protection Act

law (BDSG) allow the processing of data on the basis of collection

tive agreements, in particular to ensure equality and diversity

at the workplace, to protect collective rights and to exercise the

Rights of employee representatives.190

The works agreement in question here represents such a collective

agreement. The Women's and Equal Opportunities Officers are, albeit

not required by law, in the internal context with rights

permitted staff representatives. In the company agreement, these were like

Works council members are sworn to secrecy. This will protect

the personal rights of those affected are taken into account. From the data protection

law, there are no restrictions on the rights of employee representatives

ments nor limitations to statutory bodies.191

If additional employee representation through collective agreements

set up, data protection law restricts the work of these

not and in this respect the participation of employees in the

not counteract the process.

8.3 Data breach or tactic?

Over the course of a year, a recruitment agency sent data from job

through unencrypted e-mails to third parties and explained that this was done

hen because you have lost control of the technology.

We have received a large number of indications that companies and

requested by a recruitment agency CVs of applicants by

received an e-mail - often with a picture, age and a variety of other

your personal information. The recipients of the e-mails have

Some of the recruiters were asked to do this several times, no more

Sending more e-mails, but this was unsuccessful. At our request

The recruitment agency could not explain these data transfers.

A

and

s

i.e

e

right

P

right

a

x

i

s

190 kind . 88 para. 1 DS-GVO and § 26 para. 1 sentence 1 BDSG

191 See § 26 para. 6 BDSG

It turned out that the company saved the application data in a

outdated database on barely secured servers. an ak

Technical documentation of the system could not be submitted. It did

cannot determine whether individual employees or outsiders

men wanted to harm or whether the indiscriminate sending of these e-mails even dated

company itself was desired in order to reach as large a circle of recipients as possible

draw the attention of jobseekers to those looking for work.

Even if there had been a technical error, it would have been anyway

been very worrying that the recruitment agency, despite knowledge of the

leme went on with her job for months without doing anything

Companies.

Application documents may only be sent by recruitment agencies under strict

stipulations are passed on to third parties. Usually the basis is a

approval of the applicants. However, such declarations of consent must

formulate exactly what they are used for, such as the transmission of

Documents to a single company or to different companies

a single industry. Since consent can only be effectively granted

if those affected understand what is at stake, they must always

be made as concrete as possible. Anyone who does not know to whom their data is transferred

can also not effectively agree to this transmission.

It is recommended that recruitment agencies submit applications in a two-

step-by-step procedure: First, to interested companies

only general and, if possible, anonymous information about the candidate

or communicated to the candidate. This can include information about the skills,

on professional experience or similar be. Is the company due to this general

Information interested in a specific person can be obtained in a second stage

- i. i.e. R. on the basis of the consent of those affected - the complete evaluation

training documents are sent. This can prevent unnecessary

a lot of personal data is sent to companies that take part in this

have no interest at all.

In this case there was also the problem that the recruitment agency

has sent personal data to companies that have already done so several times

indicated that they did not wish to receive this information. In addition, is

it is problematic to send such documents unencrypted by e-mail.

A recruitment agency must ensure secure transmission paths for these companies

serve. We use the process to check a fine procedure

submitted to our sanctions office.

Recruitment agencies are particularly obliged to carefully

deal with the data of the people who want to convey them.

8.4 Welcome Back Conversations

At a logistics site, employees are killed after they have been

illness, regularly with a so-called "Welcome-Back-Ge-

speak" greeted. Here it was initially questionable whether the employer

health data are collected.

The talks always take place when employees report an illness

return conditional absence. They are to be given to the employees directly

are offered after their return and are only conducted on a voluntary basis.

The purpose of the talks is to maintain the employees' ability to work

and to secure the job in the long term. Reference should be made to the

conversations, however, not about the illness, but exclusively about the work

situation, the work activity and the working atmosphere.

A

and

s

i.e

e

right

P

right

a

x

i

s

The logistics location has an agreement with the works council on the exact details

course of the talks. Hereafter there are two types of conversations:

In the case of an absence of up to seven days, the supervisors greet the

employees and inquire about their well-being. The second conversation

typ is offered for absences of more than seven days and within

half of the first five days after return. The topic here is whether operational

compelling reasons for which downtime is responsible. Such reasons will

possibly documented. Unless there are operational reasons for the absence

are responsible, the conversation will not be continued and also not

documented. If there are operational reasons, the supervisors should

try to eliminate them as much as possible. All supervisors who have these talks

lead, receive instruction on how to conduct the conversation.

129

With regard to the type and structure of the discussions, we could not

determine the data protection law. The company agreement regulates the

course and purpose of the talks clear. As part of the duty of care in

The described data collection is permitted in the employment relationship.

An employer is authorized to inquire about the general condition of their

or its employees in relation to the employment relationship.

However, health data may only be collected under strict conditions

will.

8.5 The employment relationship was terminated

because …

s

i

x

a

right

P

right

e

i.e

s

and

A

Again and again we receive complaints that employers

Communicate reasons for termination of employment to third parties. Just

if the person concerned has been dismissed, informing the workforce,

of customers or third parties related to the company about the cancellation

to displeasure.

In one case of dismissal that became known to us, the employee left with a

action against unfair dismissal. The lawsuit was

ended with a comparison. Shortly thereafter, the management sent to approx

Dozens of company employees issued a unilateral statement on the

outcome of the proceedings. The letter also contained the reasons why the

From the point of view of the employer, the person could not continue to be employed. deducted

The letter was closed with the note that the information is within

passed on to the company and the content also to other companies connected

to which persons may be informed. The person in charge wanted her

Data with the information to restore peace in the company and doubts

clarify whether the termination was justified.

Data from employees may only be processed if this is necessary for the

maintenance or termination of the employment relationship.192 For

192 § 26 para . 1 sentence 1 BDSG

because ...

however, it is not necessary to terminate an employment relationship,

that other people are informed of the reasons. The notification

of the other employees is also not responsible for the performance of their

contractual relationships required.

In the present case, the employer's interest was through information

restore peace in the workplace. This is a legitimate interest. the

Informing the workforce can of course serve to clarify ambiguities

to clear away. However, this is usually the overriding interest

towards the person who has to leave the company. divorce people

from a company, they usually have no way of making theirs

present perspective. Especially if the employment relationship is not consensual

was terminated, often any further information about the termination of the

employment relationship by those affected as a serious violation of their own

see it. A dismissal is often preceded by lengthy conflicts.

A publication of the reasons for termination and, in principle, the

sion is likely to raise serious doubts about the integrity of the dismissed person

to let arise.

Thus, with such notifications, the interests of the data subjects that are worthy of protection

fenen regularly severely impaired. The employer

must therefore restore industrial peace in other ways. only in

In extreme exceptional cases, it would be conceivable to provide more detailed information. in the

present case was the procedure for determining whether a fine was imposed

should be handed over to our sanctions office.

From the point of view of the employer, it may make sense in individual cases

be to publish reasons for dismissal in the company. Despite it

is usually the information that the employment relationship with one or

an employee was terminated at a certain point in time, the

what an employer communicates to employees

may.

131

9 housing

9.1 No data protection in the event of misuse?

s

i

x

a

right

P

right

e

i.e

s

and

A

A district councilor drew our attention to

that there are deficits in the protection of the data of those persons who, after

residential uses prohibited by the Misappropriation Prohibition Act (ZwVbG).

Show.

The law addresses the housing shortage in Berlin and prohibits it

e.g. B. under certain circumstances, to use an apartment as a holiday home

and thus withdraw it from the regular housing market. Responsible for the implementation

The district offices are responsible for the implementation of this law. These also take hints about

from the neighborhood if there are signs of prohibited use

an apartment as a holiday home. Such a display can be either direct

at the district office or via one of the Senate Department for Urban Development

and housing offered internet portal.

In the case described by the district councillor, a tenant had one of these

Opportunity exercised and a putative holiday home in his

rental house shown. As part of the procedure that now follows, the district

office the owner of the presumed holiday home in the context of the file

have disclosed the name of the complainant. That was for this one

highly problematic, since the owner is also his own

gene landlord acted. In addition, he did not point out in his

been informed that his data may be passed on to the landlord

would give, otherwise he might not have filed a complaint.

We got involved in the case and were able to establish that the

This procedure was a common practice in the district office. on our

the district office has promised that persons who file a complaint

allow to be properly informed about the data processing in the future.193

193 See Art . 13 General Data Protection Regulation (GDPR)

This includes, in particular, information about which recipient

district their data are transmitted.194 It must also be clarified whether

that you can also object to data transmission.195

If the person filing the complaint is aware of this fact, nevertheless

provides data, it may have to expect that this will also be

of file inspection requests to those involved in the proceedings and third parties

will give. See the relevant provisions on file inspection

a balance between the information interests of an applicant

Inspection of files on the one hand and the confidentiality interests of those concerned

person on the other side.196 This consideration is carried out in each individual case

to carry out the district office. The district office must be on the one hand

take into account whether those filing complaints may have to fear reprisals,

especially if they turn against their own landlords. On the

other side contains the Information Freedom Act (IFG) applicable here

a rule presumption according to which the name and address of informants

in case of doubt, information is to be provided.197

The district office has assured us that this consideration will be carried out in the future

becomes. In addition, the Senate Department for Urban Development and

Housing offered Internet portal the opportunity to be introduced ads

also to be reimbursed anonymously.

Persons who advertise a holiday home should be aware that their data

passed on to those involved in the proceedings as part of the inspection of files

Need to become. The district office is obliged to clarify this and

In the event of an inspection of files, a weighing up of the confidentiality

esse of the person filing the complaint and the information interest of third parties

to perform. Other district offices should also check whether the reimbursement

ter of ads are duly informed in accordance with Art. 13 DS-GVO

the.

194 Art. 13 para. 1 letter e GDPR

195 Art. 21 GDPR

196 § 6 para . 2 VwVfG Bln i. v. m . § 6 para. 2 Freedom of Information Act (IFG)

197 § 6 para . 2 no. 1 letter b IFG Bln

9.2 Household surveys on milieu protection

command

s

i

x

a

right

P

right

e

i.e

s

and

A

For some time now, the districts have had the option of creating so-called milieu protection areas

determine. This is to ensure that the residents there

can stay where the infrastructure is available that they need in everyday life.

This is to prevent expensive modernization measures,

through changes in the structure of an apartment, through the conversion of

Apartments in commercial or the conversion of rental into owner-occupied

genes changed the composition of the resident population through displacement.

To check whether a certain residential area is classified as a milieu protection area

can be,198 the district offices carry out household surveys. In doing so

a large number of individual details are collected, such as e.g. B. age, gender, nationality,

Profession, highest level of education, monthly household income and

about the living situation and the people living in the apartment (alone, residential

community, couple, adult or minor children). Participation in a

Although such a household survey is voluntary, you still have to

the data protection requirements are met.

In this regard, we have a household survey by a district office

several deficiencies noted. The hardest thing was that those affected

were not correctly informed about the data processing.199

met, in particular, incorrectly informed that the information was collected anonymously

will. Due to the detailed queries, certain conclusions were drawn

on those affected is possible, especially since the survey was carried out in blocks of houses. Except-

the district office used a private company that

asked. While this is generally permissible, it must be

an order processing contract is concluded with the company,

which regulates the secure handling of the data.200 There was no such thing here.

198 See § 172 para. 1 no. 2 Building Code (BauGB)

199 See Art . 13 GDPR

200 See Art . 28 GDPR

We have pointed out these shortcomings to the district office. It showed cooperation

rativ and had already summarized the data in question in such a way that

it was no longer possible to draw conclusions about the persons concerned. Except-

we were assured that in future those affected would be informed correctly about the data

Data processing clarified and corresponding order processing contracts

would be completed. For this purpose, the responsible specialist office will

have worked more closely with the district legal office and data protection officer

work together to prevent a recurrence of such an incident.

eat. We have therefore decided to issue a warning in this case

to leave.

In the case of household surveys, it must always be carefully checked whether the individual

information allow conclusions to be drawn about those affected. As far as this is possible

is, it is personal data, so that the data protection law

legal obligations must be observed. All districts should pre-

always check carefully during the surveys whether these are being complied with.

9.3 Who comes home when? – smart cards

as a key

Residents of an apartment building complained to us about

that digital key cards are increasingly being used to access the property

would be used and access with physical keys accordingly

be restricted. They feared that their stay would be monitored

and reported access problems.

A

and

s

i.e

e

right

P

right

a

x

i

s

The residents complained that at some entrances to the house

there was no longer any possibility of using physical keys. No

complained about the unreliability of the system in the event of power or internet failures

They also noted the company's lack of transparency with regard to the

Handling of the data collected by the digital locking system.

135

The property management in question was initially not aware of any problem. the

Lock cards did contain RFID201 transponders, each of which was assigned to an apartment

assigned codes to a corresponding reader. The rights

however, is administered on just one PC in the company office,

which is protected by a virus program, a firewall and a

known password is protected. A decision was made in favor of such a system

in order not to be confronted with data protection problems.

However, this wish did not come true. Only the collection of usage times

individual cards or the associated readers at the respective residential units

ten constitutes processing of personal data, regardless of whether

these are then actually read out by the company or

Not. Thanks to the theoretically possible creation of a presence profile

e.g. in the case of a one-person household, significant insights into the

win the home sphere of affected persons. Since the data processing for

Management of the lease is not required, such a system can only

be used voluntarily.

Prerequisite for the voluntariness of consent by data subjects

is the possibility to alternatively opt for a system without such a data

to decide on processing. We have therefore urged the company to

permanent physical locking devices in properties managed by her

Offer alternative and data processing related to digital solutions

exclusively based on consent.

The processing of personal data in the context of electronically

nized access systems to residential buildings can only be

be permissible if they are based on the voluntary consent of the resident

ners based. The prerequisite for this is that other access options

are available that avoid unnecessary data collection and processing.

201 RFID systems consist of a transmitter and a receiver that are non-contact

can exchange information.

9.4 Data protection in the housing industry – developments and problems

The work area housing and housing industry takes part in the

official practice an ever-increasing share; over 120 procedures were carried out

initiated in this area by the end of November.

The vast majority of procedures in the area of housing will continue to be carried out

Complaints from tenants about rental or property management companies

take or trigger private landlords. Also advice from both

fathers as well as tradesmen and companies from the residential

economics have increased numerically in the period under review. A

growing part of inputs also refers to a new development in the

Housing structure in Berlin: Informing more and more apartment owners

or complain about data processing in the context of housing

gentumsgemeinschaften (WEG).

A

and

s

i.e

e

right

P

right

a

x

i

s

Especially in this newly developing area of the WEG, many seem to be too

underestimate how tight the contractual commitment of the members of a condominium

each other and what insights into consumption and financial conditions

inevitably exist in the immediate vicinity within a WEG.

The legally permissible control of the annual consumption bills and that
In most cases, it is only possible to create housekeeping overviews
if the numbers of the housing units billed with are also known,
what not insignificant and sometimes unwanted insights into the neighborhood
allows. For the reasons mentioned and with the owner of the apartment, this is
tumsgesetz as the legal basis, however, cannot be objected to in terms of data protection
stood. Also the use of online portals for retrieving the required
Documents are permitted as long as their access is restricted and
are secured. A general obligation to provide more than the necessary
data within a WEG (e.g. the e-mail addresses
of all owners for all WEG members) is not permitted.
The complaints from tenants continue to relate mainly to ex-
cessive data collection in the rental application process and on not or not

Correct or incompletely processed requests for information or deletion.
In addition, the input volume increased, especially with regard to the
from January 1, 2021, smoke alarm devices that are required to be installed,
which can often be serviced by radio. Many people feared one here
Monitoring by means of the devices provided for installation, especially since these
Have sensors that can measure distances, for example, in order to cover up the
Recognizing and avoiding alarms. However, these sensors are
unable to collect personally identifiable information in the form of movement profiles or
to collect sound recordings, let alone tell them about the built-in
ten less powerful radio transmitter to transmit to the outside.
However, a personal reference is assigned to a specific residential unit
device number and the relevant maintenance records. to

However, we have not yet received any reports of the unauthorized processing of this data

Complaints.

A distinction must be made from these cases of installing smoke detectors

the use of radio-based devices to record heating costs, since there

Recording of the consumption data always a personal reference with the possibility

of exploring living conditions.202

We expect a further increase in the number of cases in the residential

economics. Not just because the issue of housing given the scarce

offer and the resulting power imbalance again and again space

provides for excessive processing of personal data. Also the in

Rent caps that have come into force and the discussion about how homeowners

social conditions in Berlin are or should be

will also affect data protection aspects in the future.

202 JB 2016, 4.4

A

and

s

i.e

e

right

P

right

a

x

i

s

9 .5 Excessive data collection in rental application processes

9.5 Did you break up? – Excessive data

surveys in rental application procedures

During an on-site inspection of an Internet portal that is related to its business

Emphasis on placing ads for sale or rent

apartments, the various processes within the

commandments of the internet portal.

In the tested portal there are different offers for different

usage needs. For example, providers can B. when creating a

Rental offer different categories of personal data from

choose which prospective tenants should fill out. Vice versa can also

apartment seekers create a profile and enter a wide variety of personal

specify gene data, which will then be transferred if you are interested in a specific offer

can be averaged. This included, among other things, the most intimate information as justification

tion for the planned move, e.g. B. the “separation of a partnership”

or the "enlargement of a family", which can be answered under different

are to be selected. It is suggested to the user that

they have the best chance of getting the apartment if they provide as much information as possible

ben.

The operator of the portal was of the opinion that within the registered

th user has the right to use such data for

collect and process performance of the contract. However, this is not the case.

The purpose of the contract in the example given is to promote the

ses of a rental agreement. For the conclusion of the rental agreement, landlords may

e.g. B. However, do not collect information on family planning from the tenants.203

Consequently, such information cannot be used to implement a contract.

be required, which has the aim of informing providers and apartment seekers about the

to merge the Internet. Also from an effective consent could here

can hardly be expected, since many prospective tenants, among other things, due to the

203 See DSK guidance on “Obtaining self-disclosures from rental

Essentinnen” from 30 . January 2018, p. 4; available at https://www .datenschutz-ber-

lin .de/infothek-und-service/veroeffentlichungen/orientation aids

generally tense situation on the Berlin housing market from the

Messengers are dependent on performance and work to increase their chances of getting the

housing market to provide relevant information.

In the context of rental application procedures, only such

personal data are collected, which are necessary for the conclusion of the rental

contract are required. This principle must not be circumvented thereby

that an online platform is interposed.

9.6 My house – my extract from the land register

s

i

x

a

right

P

right

e

i.e

s

and

A

In a civil or construction law dispute, a law firm commissioned

re clients the owners of several properties of a

henhaussiedlung sued. The law firm has an extensive list of complaints

Attached is a bundle of installations, including the complete land register pages

or land register excerpts for all properties of the relevant terraced house

settlement. These extracts from the land register contained personal data on the

23 property owners, including their names, dates of birth and

Addresses, existing charges and restrictions as well as information on

Mortgages, land charges and annuity debts. After delivery of the complaint

All defendants obtained a letter with the annexes from the Berlin Regional Court

knowledge of this data.

Land register sheets are basically in the inscription, the inventory

and the first to third departments.204 The various

separate, self-contained sections of a land register sheet

net, in which certain information is to be entered.205 In the first section

the ownership structure is recorded and, among other things, name, date of birth and

letter of the owner and the basis for the

transfer of ownership noted. In the second department, property

encumbrances and limitations (e.g. easements, real encumbrances) and in the third

204 Section 4 Land Register Order (GBV)

205 The more detailed setup and the filling out of the land register page results from

§ 22 GBV from the model contained in Appendix 1 GBV.

Department of property liens, such as B. Mortgages registered. At the in the

The information contained in each department is personal

Data. The office has the land register sheets in the context of the civil process as

evidence presented.

However, the data processing by the law firm was unlawful, since neither

consent of the persons concerned was still a legal basis

was evident. In particular, data processing cannot be based on Art. 6 Para. 1

Sentence 1 lit. f GDPR. After that, processing is lawful,

if they are to protect the legitimate interests of the person responsible or

of a third party is necessary, unless the interests or fundamental rights and

- freedoms of the data subject, which require the protection of personal data

demand, prevail. Although the processing of personal data is

opposing party to enforce legal positions of the client

fundamentally a legitimate interest in the practice of a legal profession

to see a lawyer. The submission of the complete basic

In the present case, however, book excerpts were used as evidence in the civil proceedings

against the owners is not required. A data processing agency

cannot invoke legitimate interests if the data has any

meaning for the specifically pursued processing purpose is missing.206 The data processing

Rather, the processing must be objectively suitable to achieve the purpose and

the person concerned must either not have a less onerous alternative

gene or must not be reasonable for the person responsible.207

By submitting the complete extracts from the land register, the law firm wanted to prove

that the persons concerned are the right opponents. for proof

that they actually own the property

however, only a copy of the first section of the respective land register

ter would have been sufficient, since the ownership structure is stipulated therein

are.208 The information from the second and third sections of the land register

However, in the context of the statement of grounds of claim, no such moves were required. It

would have been possible without any problems, from the complete excerpts only

206 See Kühling/Buchner/Buchner/Petri, DS-GVO, Art. 6, recital . 151

207 See Schulz, in Gola, DS-GVO, Art. 6, recital . 20

208 See § 9 GBV

lich to copy the sheets of the first section and attach them to the statement of claim.

What is characteristic of the three sections of the land register is precisely that

they are self-contained. In the separation of z. B. from the responsible basic

imprints of the land register received from the registry office or a notary

to see a "manipulation" that constitutes the forgery of documents i. S.v.

§ 267 of the Criminal Code (StGB) is misguided and must be used as a protective claim

be evaluated by the law firm.

As part of our entire review process, the law firm has the legal opinion

sung represented that the introduction of the complete extracts from the land register in the

lawsuit was lawful. Against this background and in view of the

large number of data subjects we have the data protection breach as

assessed as extremely serious. Therefore, our sanctioning body now has a

fine proceedings initiated.

Lawyers must ensure that they

ment of processes only process personal data that is used for proof

leadership are required. A law firm cannot claim that

the data processing was necessary to protect legitimate interests,

if the personal data introduced as evidence in civil proceedings

related data any meaningfulness for the pursued processing purpose

is missing.

9.7 Debtor wanted

s

i

x

a

right

P

right

e

i.e

s

and

A

In order to locate a client's debtor, a law firm had to work together

with a letter to the residents of a residential building

fluent. In it, the law firm stated, in addition to the name of the person sought,

that this was officially registered in the house, but the name was not on

entrance panel. Try to find the person through property management

to make digs, to meet them personally on site and to deliver mail are

failed. The law firm asked the neighbors to let them know whether

the debtor wanted because of outstanding claims at one of the tenants

live. In the letter, the initiation of a forced deregistration

Chapter 9 Housing 9 .7 Debtor wanted

threatened by the registration authority if there is no positive feedback from the tenant

should come to the wanted person.

Disclosure of information about the debtor to householders

residents was not permitted. In particular, the sending of the letter

with the personal data of the wanted debtor neither for protection

legitimate interests of the law firm nor to protect legitimate interests

of the client as the creditor of the claim.209 Necessity is

to accept if the legitimate purpose pursued by the data processing

Interest can actually be achieved and there is no other equal

effective, but with a view to the fundamental rights and freedoms of the affected

gives a person less drastic means. This means that the

The necessity is only to be assumed if the intended purpose

not just as good with another, economically and organizationally reasonable

can be achieved by means that are less encroaching on the rights of the person

intervenes.

For the legally effective assertion of the present claim or the

Delivery of the lawyer's letter of demand exist other, equally

suitable and less encroaching on the rights of the debtor concerned

phone The law firm could have initiated legal dunning proceedings. According to

§ 693 Para. 1 Code of Civil Procedure (ZPO) the dunning notice is issued in a formal

proceedings or by the office of the court ex officio

provided.210 The court office can appoint a person according to Section 33 (1) of the Post

Entrepreneurs or judicial employees entrusted by law (PostG) with the

order delivery to be carried out. In individual cases, the delivery is through

the office or the post office is not possible, the chairperson of the

appoint a bailiff to serve the court.211

Lawyers should, when processing data

check the opposing party closely to see if all are legally available-

the possibilities have been exhausted, e.g. B. a letter of demand

209 See Art . 6 para. 1 sentence 1 lit. f GDPR

210 See § 168 ZPO and § 166 para. 2 Code of Civil Procedure

211 § 168 para . 2 Code of Civil Procedure

be delivered. On the other hand, it is not a permissible means to

to reveal information about a wanted person to neighbors and neighbors

to locate their whereabouts. Rather, law firms must address themselves

hold the forms of service intended for civil legal proceedings, too

if previously various investigative measures (e.g. in person or

postal contact attempts) were unsuccessful.

9.8 Data processing by notaries

"Apartment package sales"

s

i

x

a

right

P

right

e

i.e

s

and

A

In the context of real estate sales, notaries do not

only processes personal data of the contracting parties, but re-

Usually also data from tenants of the sold apartment. background

is that the real estate purchase contracts to be notarized as an annex

Documents for the rented apartment are often attached. With a so-called package

sale in which several properties are sold at the same time with a purchase contract

are bought, numerous tenants are often affected accordingly.

In connection with such package sales of residential real estate, we

reached several complaints about notaries.

As part of the certification and processing of the parcel transaction, the notaries

Purchases of large residential complexes Purchase contract documents with extensive

personal data to all tenants of the residential buildings

sent to inform them about the existence of a right of first refusal.212 The

The parties to the purchase contract had commissioned the notaries to

Inform tenants of the sale of the property and formally notify them

212 If there is a right of first refusal for a residential property, a seller is at the

conclusion of a purchase contract obliges the to the

to be presented to persons entitled to pre-emption. If the person entitled to the advance purchase

If you want to exercise your right of first refusal, you can use the contract of sale in place of the original

Buyer or the original buyer take over, including all already

agreed conditions, and thus becomes a party to the purchase contract for the seller or

of the seller .

to ask them to comment on their right of first refusal.213 In order to fulfill this

The notaries then sent a letter to those entitled to pre-emption

and at the same time sent copies of the purchase contract including numerous

cher systems to the tenants. Attached were e.g. B. tenant, deposit and

Lists of balances, which include the names and account numbers of all tenants

of a residential building, the rent to be paid in each case, the amount of

paid deposits and information about rent arrears. in the rental

In some cases it was even noted which persons were under legal

care are available, so that conclusions can be drawn about their state of health

could become. Since the notaries are the same for all persons entitled to pre-emption

documents and they sent the data to the other tenants

If you didn't make people unrecognizable, the neighbors were extremely successful

sensitive information about each other.

The acting notaries were responsible for the mentioned data processing

processing and not just as a processor.214 Because at the

Mandatory engagement of a notary by law

the conclusion of real estate contracts is not a matter of

solution-related processing, but the use of third-party specialists

performance with a responsible person.215 notaries

essential own decision-making processes within the scope of their work

clear in relation to the purpose and means of data processing. Also in the

cases examined by us, the activities of the notaries were not exhausted in the

mere certification activity was still a pure execution activity. Much more

also included the commissioning by the contracting parties

upcoming tasks in connection with the execution of the contract.

213 § 577 para . 1 set 3 i . v. m . § 469 para. 1 BGB regulates the obligation to notify the

persons entitled to pre-emption about the content of the concluded contract. the lesson

The obligation to exercise the right of first refusal results from § 577 para. 2 BGB. Both mandatory

ten actually has to be met by the seller.

214 See Art . 4 no. 7 GDPR and Art. 4 no. 8 GDPR

215 See also brief paper no . 13 of the DSK, p. 4; available at https://www .daten-

schutz-berlin .de/infothek-und-service/veroeffentlichungen/brief papers

145

For the transmission of the data of the tenants by the notaries to

there is no legal basis for all persons entitled to pre-emption.216

In particular, the notaries could not rely on this when processing data

fen that this is necessary to fulfill a legal obligation of your own

was.217 Furthermore, it could not be assumed that the data

Transmission to protect the legitimate interests of those responsible or

third party would have been necessary and at the same time would have been considered more serious

than the privacy-related interests, fundamental rights and freedoms of the

persons affected by it.218 The statutory obligation, upon the occurrence of the

In the event of pre-emption, to inform the tenants of their right of pre-emption

and informing them of the content of the respective sales contract does not constitute a reason

to also transmit the sensitive data of the other tenants to them. He-

it is only necessary that the persons entitled to pre-emption are aware of the

receive the consideration agreed with the third-party buyers.

Data on other people who are required to make an appropriate decision about the

exercise of the right of first refusal have no meaning whatsoever, may not transmit

be told. Notaries must, as part of the notarial accompaniment

execution of real estate sales contracts to ensure that

the personal data of the tenants in accordance with data protection regulations

are processed. This also includes that in the case of contractual takeover
of the information and notification obligations219 the data protection
ensure compliance with these obligations. This can e.g. B. by sending individual
due copies of the contract to the tenants who are entitled to pre-emption
take place in which the personal data of the other tenants and
be made known.

Since the cases examined by us are of far-reaching importance for the activities of
had, we turned to the Chamber of Notaries in Berlin,
to discuss practicable solutions and recommendations for action. The chamber
has informed us that some expert opinions of the German Notary Institute our

216 See Art . 6 para. 1 sentence 1 lit. a to f GDPR

217 See Art . 6 para. 1 sentence 1 lit. c GDPR

218 See Art . 6 para. 1 sentence 1 lit. f GDPR

219 Pursuant to section 577 para. 1 sentence 3 BGB i . v. m . § 469 BGB and § 577 para. 2 BGB

support opinion. However, since the legal situation has not yet been conclusively
clarified, she sent a rather reserved circular to the Berlin Nota-
mentors and notaries.

When designing real estate purchase agreements, notaries should
ensure or work towards that only such personal
drawn data are added to the purchase contract to be certified, the
for the execution of the contract and the fulfillment of legal obligations
are actually required. You must also ensure that no personal
transfer related data to tenants who are entitled to pre-purchase
be made that are not necessary for the exercise of the right of first refusal.

This can be done, for example, by blackening such data before sending

documents are made.

147

10 economy

10.1

Internet identity abuse

orders

s

i

x

a

right

P

right

e

i.e

s

and

A

This year, too, it can be seen that companies do not

far-reaching measures to identify people during ordering processes

seize. As before, either complete identities or con-

Death data of those affected misused for fraud cases.

Already in 2017, due to a large number of cases of fraud, we had to

deal intensively with the topic and had changes in the business

from online traders.220 Now we had to realize again that

Online traders in the event of anomalies that indicate possible fraud

(e.g. if there is a discrepancy between the billing and delivery address), after how

have not taken adequate controls to prevent identity abuse

impede. A first order on account with one of the billing

a different delivery address is still possible with many companies,

without this leading to more rigorous controls or at least a risk awareness

design of the dunning and collection procedure.

Admittedly, in most complaint cases, the reminders were not issued

sent by email only. However, it also happens that wrong

Billing addresses are given, so potential victims still

only through the first letter from the collection agency after its address

research about the dunning procedure and ultimately about the misuse of identity

gain.

From companies that place initial orders on account with a different delivery

Allowing an address and not carrying out an identity check would therefore not only be

220 JB 2017, 1.3 and press release from our authority from 8. Sep 2017; available

at https://www .datenschutz-berlin .de/infothek-und-service/pressemitteilungen/

press release archive

148

Chapter 10 Economics 10 .1 Identity abuse when ordering online

to demand that these be submitted to a debt collection agency at least one

undertake their own dunning attempt by mail, but also that they return mail

in such cases as an opportunity to independently identify a misidentification

need to check. The long transit times of mail returns are also increasing

note - in such cases it must not be two weeks after

after the postal reminder, the goods will be handed over to a collection agency.

If the company's check does not indicate an identity

misuse, the company should nevertheless first find the right

determine the writing of the person concerned and repeat the postal reminder

to the actual address in order to clarify the facts

enable.

In any case, an objection by the data subject in the dunning procedure must

measured are taken into account. Because the transmission of personal

Data to a collection agency is not for the purpose of debt collection

required and therefore not according to Art. 6 Para. 1 lit. b of the General Data Protection

ordinance (DS-GVO) permissible if the claim asserted at all

does not exist. In such cases, a transfer can be considered

the collection agency on the basis of legitimate interests pursuant to Art. 6

Paragraph 1 lit. f DS-GVO.221 However, if identity abuse is obvious for the

obviously, there is no legitimate interest in the disclosure of personal

Personal data when using a debt collection agency. applies the affected

fene person a misuse of identity, a data transmission to the

Debt collection companies only take place if the demand for this

turn has been carefully checked. In one of our complaints

the verification was omitted despite multiple objections, so that we

Procedure of our sanctioning body for examining the initiation of a fine

have presented driving.

In cases of identity abuse, the question often arises as to whether the

made a claim for information about their illegally used order

have dates

221 See 10.7

According to the legal definition, personal data are all information

ones that refer to an identified or identifiable natural person

pull and can thus be assigned to it.222 By a third party

The data generated will be processed by the respective company of the identity

assigned to the affected person and thus processed. After the

of the concept of personal reference in the case law of the European

Court of Justice (ECJ), the reference to a person is also given if

if "the information, because of its content, its purpose or its effect

linked to a specific person".223 This is the case with an identification

Abuse of activity evidently the case. It is therefore personal

Data of the respective natural person.

In the event of (also suspected) identity theft, those affected must be aware of all

receive information about the data stored on them without exception. Included in this

are all data relating to the customer account, account transactions and order history

concern, since this data is assigned to the identity of the person concerned

related to this. Therefore, they provide personal data of the data subject

fenen, even if they are made by third parties under the pretense of a false identity

have been caused.

The data subject's right to information cannot be overridden either

be countered by third parties. A need for protection of personal data

third party does not exist, as they knowingly process the personal data of the

affected person to assign their actions to them. in particular

dere they have the situation that their and data subjects' data

collapse, self-induced.

We are still in contact with to avoid identity abuse

the companies in order to ensure a risk-aware design of the ordering and

work towards dunning procedures. The lawfulness of the processing of your data

affected persons in the event of (suspected) identity theft

only check if they receive information about all data that their customer

222 Art. 4 no. 1 GDPR

223 ECJ, judgment of 20 . December 2017 – C-434/16, para. 34, 35 (Nowak case)

account or your customer number. As this is according to the law

concerns personal data of the victim of identity abuse,

companies are obliged to provide comprehensive information.

10.2 And the address trade greets you every day

Over many months, we have received numerous letters from citizens

reached who complained that they repeatedly received advertising via

Received an e-mail from a company without a corresponding

to have given consent or other consent. Many of the affected

Neither was the provider of the e-mail advertising known to them. on information

Requests from the persons concerned were often not made at all or only

responded with a long delay. The same was true when those affected

with requests to block or delete your own data to the

bidders have approached. We have investigated the matter in detail and

asked the provider for a statement.

A

and

s

i.e

e

right

P

right

a

x

i

s

In our cover letter, the provider informed us that he had the e-mail addresses

of the persons concerned, often through their participation in sweepstakes or

obtained by renting an address. According to him, this happened either

by being co-sponsor of the Sweepstakes

accordingly also access to the names and e-mail addresses of the participants

received or this by renting large amounts of data via so-called

list owners, particularly from Great Britain.

Often there was no effective consent on the part of those affected to

stop advertising communication. It was also noticeable that the provider

Obtaining the data often only after persistent pressure from the Berlin authorities

contributed to data protection and freedom of information sufficiently disclosed and many

of the sweepstakes had already ended several years ago, the

However, the responsible body only sent the customer in the last twelve months

had written to for advertising purposes.

In principle, consent is not subject to an expiry date. Before the

Background of the principle of transparent data processing according to Art. 5

151

Paragraph 1 lit. a DS-GVO recommends the European Data Protection Board (EDPB)

however, to have the consent renewed at reasonable intervals.224

If all information related to the data processing is then given again
this helps to ensure that the data subject is informed
remains, how her data is used and how she can exercise her rights.
If, as here, no contact is made for a longer period of time,
followed, the consent can no longer continue to exist without further
res to be assumed. A period of ten years or more without contact
In this respect, admission can no longer be considered appropriate.
In addition, in the present case, the responsible body often only after
responded to inquiries for several months. According to Art. 12 Para. 3 Sentence 1 DS-GVO ha-
information requested by the person responsible for the data subject immediately
be made available, but in any case within one month after receipt
process of the application. Within this period, the information must be given or it must
at least be told why this is not possible within the deadline.
We have pointed out to the provider that his behavior is subject to data protection
is legally questionable and the procedure should be changed. It should be noted
in particular that the rights of those affected to information, deletion and
The blocking of their data must always be maintained and implemented quickly. also
We have a clear view of the transparency of handling customer data
calls for significant improvements.
Although our review is not yet complete, we have the
already clearly pointed out to the bidder that we accept such misconduct
ten and this must be stopped immediately. The person in charge has
promised to observe and implement our instructions.
We will continue to monitor the provider closely in the future.
Irrespective of the measures already taken, we also reserve these
imposition of corresponding fines against the responsible body.

224 Guidelines 05/2020 on consent in accordance with Regulation 2016/679 of 4 . May 2020, no.

111; see https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-

052020-consent-under-regulation-2016679_en

152

Chapter 10 Economics

A

and

s

i.e

e

right

P

right

a

x

i

s

10 .3 Automated retrieval from an intermediary register

10.3 Automated retrieval from a

Intermediary Register

The Association of German Chambers of Industry and Commerce e. V. (DIHK) leads for the

Chambers of Commerce and Industry have a register of intermediaries in which, among other things, the data of approx.

400,000 insurance intermediaries are registered. insurance

keep information from the register by means of an automated retrieval

the Internet.225 They need this information because they only deal with insurance

Intermediaries may work together who have the appropriate permission

own.226 The register includes the surname and first name of the

intermediaries, the register number, the address, but also the scope of the

activity.227 The DIHK was concerned that some insurance companies had more than

Thousands of queries per day. To ensure data protection

Affected and to ward off computer attacks was therefore the number of

possible queries reduced. Sometimes the insurance companies were only given the

Possibility given to recognize in a "traffic light procedure" whether a version

security agent is included in the list or not. The Restrictions

led to a dispute between the insurance industry and the DIHK.

Since the DIHK referred to data protection regulations for its restrictions,

our authority was asked to settle the dispute.

In principle, there are no legal rights when accessing the public register data

some concerns if it is earmarked. You can of this when calling

assume insurance, as this is an interest and even a legal one

Obligation to have the authorization as well as the scope of the authorized activity of

to check registrants. At large insurance companies

it is also not surprising that sometimes more than a thousand queries per day

take place, since insurance companies always use the current

state, i.e. also a trade ban that has just been made,

must be taken into account.228 To reduce the amount of information that can be accessed

e.g. B. by a traffic light indication there is no data protection requirement

225 See § 11a para. 1 and 2 trade regulations (GewO)

226 See § 48 para. 1 Insurance Supervision Act

(VAG)

227 § 8 Insurance Mediation Ordinance (VersVermV)

228 See § 11a para. 3 sentence 1 GewO

ability. There are no objections to the insurance companies taking the full

Receive a data record that shows the scope of the permitted activity

and not just a yes or no. The legislator has decided to protect insurance

policyholders decided to make the agent register data public

to make accessible. The verification of a legitimate interest is not

required, it should only be ensured that no computer attacks

or abusive calls are made. We have recommended that the large ab-

Make contact persons available to inquiring insurance companies, if at

DIHK needs an explanation due to the large number of queries.

Contrary to what is often claimed, the data protection authorities prevent this

not only, but enable many things: works through our mediation

meanwhile the data query of the insurance companies at the register of intermediaries

the.

10.4 Unwelcome "Welcome Email"

s

i

x

a

right

P

right

e

i.e

s

and

A

Again and again we receive inquiries from people who send them by letter or e-mail

Receive ads from companies you haven't worked with in a while

have been in a business relationship. As part of the hearing

Responsible bodies then often refer to an existing customer account

and are of the opinion that the sending of advertising is in such cases

constellations permitted without time restrictions. Many complaints reached

us in this respect in connection with the takeover of an online fashion retailer

by a Berlin company. In many cases, data from

former customers of the online fashion retailer from inactive customer

accounts processed in order to send them to the recipient with a so-called welcome e-mail

bot of the new company. At the same time for

created a new customer account.

Art. 17 Para. 1 lit. a 2nd alternative GDPR obliges each person responsible for the processing

responsible for the relevant data to delete the data immediately,

if they are no longer necessary for the purposes for which they were processed

are agile. A request or a request from the data subject is sufficient for this

not mandatory.

This application-independent obligation to delete requires that the responsible

literal authority to fulfill its deletion obligations independently and continuously

check has. However, the GDPR does not contain any specific specifications

in terms of time. It is therefore the responsibility of the respective company, depending on the type and

Scope of the data processing carried out a specific deletion concept

as well as to develop functioning deletion routines and to use suitable technical

implement technical-organizational measures (and the people concerned

within the framework of the data protection declaration in accordance with Art. 13 or 14 DS-GVO

to inform about the specific deletion deadlines). In the case of a customer account,

Determination of the period after which the deletion must take place, the regular

Permitted use by the data subject is decisive.

The processing of personal data must be appropriate for the purpose

and to achieve it significantly229 as well as for the purposes of the processing

be limited to the extent necessary for processing (principle of data minimization).230

Personal data may not be stored longer than is necessary for the

purposes of their processing is necessary (principle of storage limitation).231

In particular, this requires that the storage period for personal data

is limited to the absolutely necessary minimum. To be sure-

ensure that the personal data is not stored longer than necessary

responsible bodies are obliged to independently set deadlines for the

research and the regular review of the data.232 If the

Purpose achieved through the process of data processing or is this

In this way, the data must always be completely deleted. If only

part of the data is no longer required for the stated purpose, may also

partial deletion may be required.

The decisive factor is whether, due to the nature of the business relationship, the responsible

Verbatim passage can be explained in a comprehensible manner that further use

229 This means that the responsible body basically only accepts such personal

personal data may be collected and processed for the specified

suitable for a purpose; see BeckOK data protection law, Schantz, DS-GVO, Art. 5,

marginal 24 .

230 type . 5 para. 1 letter c GDPR

231 Art. 5 para. 1 letter e 1 . Hs GDPR

232 EC 39 sentence 9 GDPR

of the data is required. The law has a specific time limit

not intended for this purpose.

An orientation for storage and deletion periods is given by the conference

independent data protection supervisory authorities of the federal and state governments (DSK)

on the 7th/8th November 2018 adopted "Orientation aid for the supervisory authorities

to process personal data for direct marketing purposes

under the General Data Protection Regulation (GDPR)".233 Depending on

Type and industry of responsible bodies time limits of six

months up to two years. Within the by the responsible

Place a fixed period of time after the last active business contact

to a person concerned, their data can in principle be used for the customer

NEN recovery can be used. After this period has expired,

to assume that there is no need to store the data.

So if a responsible body processes data, but this is for the original

original purpose are no longer required and also no legal ones

or contractual retention periods234, these may no longer exist

used and must be deleted. Unused customer accounts and

the personal data stored therein must therefore no later than

be deleted after two years of inactivity.

In the case of the online fashion retailer, the inactive customer accounts have long since existed

must be deleted. The data takeover by the new company and

the creation of new customer accounts using this old data was therefore

allowed.

Responsible bodies are obliged to process personal data regularly

and to delete them without separate request as soon as they are necessary for the purposes for which

which they were collected or processed are no longer necessary. at

unused customer accounts, this is after two years at the latest

Case.

233 See https://www .datenschutz-berlin .de/infothek-und-service/veroeffentlichungen/

decide-dsk, in particular Chapter 4.8

234 See Art . 17 para. 3 lit b GDPR and Section 35 Para. 3 2 . old . BDSG

10.5 Data retention after the end of a contractual relationship

Even after the end of the contract or after termination of a customer relationship

Responsible persons are legally obliged to pass on certain documents

to keep. When processing corresponding complaints, in

been found in several cases that the design of the storage

These documents by those responsible do not comply with the provisions of the GDPR

was compatible.

A

and

s

i.e

e

right

P

right

a

x

i

s

In principle, personal data must be deleted if they are used for the purposes

for which they are processed are no longer required.235 A deletion can

consequently, among other things, omitted if the further processing of the data for the fulfillment

fulfillment of a legal obligation on the part of those responsible is still necessary.236

However, this only legitimizes data processing that is necessary for the fulfillment

of the respective legal obligation are actually required.

According to the principle of data minimization237, the personal

Data appropriate to the purpose and relevant to its achievement as well

be limited to what is necessary for the purposes of the processing. ver

responsible must take the necessary technical and organizational measures

take measures to ensure compliance with the requirements of the GDPR

afford.238

Regarding the legal obligations that require further storage of personal

may allow the data collected include, in particular, the obligations to

Storage of documents according to commercial and tax law. the dorti-

General regulations for the storage of documents such as commercial letters and

235

As a rule, the legal basis expires with the end of the contractual relationship

for the processing of personal data; see type . 6 para. 1 sentence 1 lit. b

GDPR .

236 art. 6 para. 1 sentence 1 lit. c GDPR

237 art. 5 para. 1 letter c GDPR

238 art. 24, 25, 32 GDPR

157

Audit documents entitle or oblige those responsible in detail to

Storage of the following documents beyond the end of the contract:

• the commercial and business letters received for a period of six years

ren,239

• Reproductions of commercial and business letters sent for the duration

of six years,240

• Accounting documents for a period of ten years241 as well

• other documents, insofar as they are important for taxation, for

the duration of six years.242

However, these regulations only provide for the retention of certain documents

before, which may then contain personal data of customers. Not on-

On the other hand, such documents from which these documents only exist must be preserved

were created, as well as other communications that are not intended as commercial or

Business letter is considered, for example, because it does not relate to the preparation, execution or

rescission of a commercial transaction, or because it is a

internal communication or telephone notes. The one about that

End of contract maintenance of a database in which personal

Data of former customers such as master or communication data

are stored, these regulations do not provide for them. From such databases are

the personal data of the customers in the absence of another

Legal basis to delete after the end of the contract.

The legal obligations to keep certain documents

with personal data after termination of a contractual relationship

do not entitle or oblige those responsible to

Notification data of former customers still in after the end of the contract

to store in their databases. Those responsible must keep their data

adjust accordingly.

239 § 257 para . 1 no. 2, para. 4 Commercial Code (HGB); § 147 para. 1 no. 2, para. 3 exhaust

ordinance (AO)

240 § 257 para . 1 no. 3, para. 4 HGB; § 147 para. 1 no. 3, para. 3 AO

241 § 257 para . 1 no. 4, para. 4 HGB; § 147 para. 1 no. 4, para. 3 AO

242 § 147 para . 1 no. 5, para. 3 AO

A

and

s

i.e

e

right

P

right

a

x

i

s

10 .6 Engagement of collection agencies

10.6 Commissioning debt collection companies -

Why am I getting mail from them?!

Many citizens who have received dunning letters from collection agencies

contact us and inquire about the legality of women

Creditors pass on their data to the debt collection agency.

If there is a contract with the data subject, creditors can

either collect the claim yourself or use a debt collection agency

instruct. In the latter case, it is necessary for the collection agency

also receives the information justifying the claim and the collection

enabled by the collection agency.

If a debt collection agency is commissioned, the transmission of the

hung the claim required personal data on the basis of

Art. 6 (1) sentence 1 lit. b GDPR permitted. Consent is also conceivable

of the data subject,243 although in practice this legal basis

meaning, since consent can be revoked at any time. Besides that

arrives as the legal basis for the transfer of personal data

a debt collection company Art. 6 Para. 1 Sentence 1 lit. f GDPR into consideration. After that is

the transfer of personal data is lawful if "the processing

to safeguard the legitimate interests of the person responsible or a third party

ten [is] necessary, unless the interests or fundamental rights and fundamental

freedoms of the data subject … outweigh". The legitimate interest of

transmitting company is that the open claim by the

debtor is settled.

If a data subject agrees with a company to provide a

agreed performance against payment agreed and the resulting

If the claim has not been settled or has not been settled in full, the company is after

careful examination, therefore fundamentally entitled to use the contract data of the

person concerned to collect the debt to a collection agency

admit.

243 See Art . 6 para. 1 sentence 1 lit. a GDPR

159

Since the data transmission should serve to collect the debt, i. i.e. Smoke

not assume that interests or fundamental rights and freedoms

of the data subject prevail.

This also applies in principle in cases in which the existence or the amount

of the asserted claim is disputed by the person concerned.

However, if there was no claim from the outset, for example because a claim from a

so-called subscription case is asserted or there is identity theft

a data transmission for the collection of receivables cannot be justified, since yes

just one requirement is missing. In this case – in addition to the typical

do not have consent - only Art. 6 Para. 1 Sentence 1 lit. f DS-GVO as

legal basis to consider. For this, however, a legitimate intention

interest of the person responsible or a third person. A

Such a legitimate interest can also lie in the entitlement of the

determine the alleged claim. But is for a supposed believer

If you can see that the claim does not exist, a legitimate inter-

esse on the transfer of personal data due to the engagement

of a debt collection agency cannot be affirmed. Does the person concerned bring such

The alleged creditor or the alleged

Creditors therefore the entitlement of the claim before the involvement of an internal

scrutinize cash offices particularly closely.244

If the requirements of Art. 6 (1) sentence 1 lit. f GDPR are met,

the debt collection agencies, i.e. those necessary for the fulfillment of their order

process data and may also collect any additional data required

ben.

Creditors can also use collection agencies without the consent of the

instruct the persons concerned to assert their claims

and transmit the necessary personal data.

244 See 10.1

10.7 What are collection agencies allowed to do?

tell credit bureaus?

is the subject of numerous inquiries and complaints that we receive

also the legality of registering claims with economic

futures agencies by collection agencies.

The power of collection agencies to transfer data from debtors to business

credit bureaus, such as SCHUFA Holding AG or CRIF Bürgel

GmbH, is based on Article 6 Paragraph 1 Clause 1 Letter f and Article 6 Paragraph 4

GDPR. The consent of the persons concerned is not required for this

lich.

A

and

s

i.e

e

right

P

right

a

x

i

s

A transfer of personal data to another body or to a

another purpose is possible, insofar as this is for the perception of a legitimate

interests of the transmitting body, the recipient or the recipient

Data or by third parties is required. The legitimate interests of the affected

person may not override this legitimate interest.

to weigh. In addition, the new processing purpose must match the original

chen purpose in a context.245

From a legitimate interest in the transfer of data to a credit agency

can be assumed from debt collection companies if there is a reason

third parties about negative payment experiences with a data subject

to protect these third parties from payment disruptions. while having to

the occasion is based on verified facts. Purely subjective assessments

so not enough.

In 2018, the DSK decided on the following five alternative

ven case groups who, within the framework of the weighing of interests according to Art. 6

245 Art. 6 para. 4 lit. a DS-GVO, EG 50 sentence 6 DS-GVO

161

Paragraph 1 sentence 1 lit. f i. V. m. Art. 6 Para. 4 DS-GVO an indicative effect for the permissible

possibility of registering with a credit agency:246

1. The claim is legally enforceable or provisionally enforceable

"

declared judgment has been established or there is a debt instrument according to § 794

of the Code of Civil Procedure.

2. The claim is established according to Section 178 of the Insolvency Code and not

disputed by the debtor at the examination date.

3. The person concerned has expressly acknowledged the claim.

4. After the due date of the claim, the person concerned is at least

been reminded twice in writing, the first reminder is at least

four weeks back, the person concerned is earlier, but at the earliest at the first

ten reminder about a possible consideration by a credit agency

been informed and the person concerned has not disputed the claim.

5. The contractual relationship on which the claim is based can be

of payment arrears can be terminated without notice and the person concerned

previously informed about a possible consideration by a credit agency

been judged."

The person concerned must be informed in advance by the collection agency about the

probability of registering with a credit agency, since

this may only take place if the data subject at the time of collection

of the personal data and given the circumstances under which they

follows, can reasonably foresee that processing for this purpose

may occur.247

It should also be noted that negative payment experiences

gene there is no de minimis contribution limit. So even the smallest

be reported slowly, provided that the aforementioned transmission requirements

are met.

246 Resolution of the DSK of 23 . March 2018: "Entry more open and undisputed

Claims to a credit agency under the GDPR"; available

at https://www .datenschutz-berlin .de/infothek-und-service/veroeffentlichungen/

decide-dsk

247 See EG 47 sentence 3 GDPR

For the correctness of the content of the registrations and for the existence of the

The debt collection agency is the transmitting agency

responsible.

Insofar as the data transmission was inadmissible or subsequently proved to be inadmissible

proves significant, data subjects have, for example, claims for correction, deletion

investigation and compensation. In such cases, the collection agency is

In addition, obliged to the credit agencies to which the data was transmitted

notify, in order to have a correction or deletion of the

stored data.248

Debt collection companies may (only then) transfer data from debtors to business

to credit bureaus if certain requirements are met

are. The consent of the persons concerned is fundamental for this

not mandatory. However, the persons concerned are informed in advance about the

possibility of registering with a credit agency.

10.8 Data protection officers are not part of the customer service

In some companies, requests are addressed to the privacy policy

specified data protection officer or the specified data protection officer

not directly or not only forwarded to this named person, but

otherwise to other places, in particular to customer service.

The data protection officer is responsible for fulfilling his or her duties

were obliged to maintain secrecy and confidentiality.249 These

There is also a duty of confidentiality towards those who named her or him

Job. It is therefore not permissible for inquiries that are based on trust in Ver-

confidentiality to a data protection officer, to others

departments of the company are forwarded.

A

and

s

i.e

e

right

P

right

a

x

i

s

248 See Art . 19 sentence 1 GDPR

249 Art. 38 para. 5 GDPR

A breach of the statutory confidentiality obligations therefore constitutes, for example,

if the e-mails addressed to a data protection officer are sent to a

distribution list to which, in addition to the data protection officer

IT management and customer service also belong. For contact to

the data protection officer may not use the same contact form

be used as for contact with the company. Incoming mail or

E-mails to the data protection officer may be sent by the company -

for example in the post office or by the administrators - not open or

to be read.

However, it is possible and intended that the data protection officer

trage is supported by employees in the fulfillment of tasks. This

may therefore according to the specifications of the data protection officer and under

compliance with confidentiality obligations in their work

will.

We have contacted the companies concerned due to the breach of confidentiality

warned or sent a case to the sanctioning authority for further prosecution

delivered.

The acknowledgment of mail and e-mails to the data protection officer

must be in the exclusive decision-making authority of the

respective data protection officer. Everything else contradicts that

Principle of confidentiality and secrecy of data protection officers

wore Therefore, separate e-mail addresses and contact forms for

Company and data protection officer required.

10.9 Business: Control Inbox

and ensure the rights of those affected!

s

i

x

a

right

P

right

e

i.e

s

and

A

Anyone who no longer receives advertising or information from a company

wants or wants a customer account to be deleted, answer for it

often just an e-mail from the company concerned. But will

che often refuses to make contact, pointing out that it is a

"No reply address" or the mailbox is not viewed. loading

are often referred to a specific communication channel. It

it can also be stated in general that the incoming messages – in particular

via e-mail - are insufficiently controlled in many companies.

Those responsible have to take technical and organizational measures to ensure

ensure that all data protection inquiries that are received are sent to the responsible specialist department

division and processed there.250 This includes that too

E-mails that do not go through the channels provided for this purpose by those responsible

arrive, forwarded to the correct contact persons for further processing

will. The persons concerned cannot be required to first

to seek a declaration of compliance from those responsible for data protection

ask to find out the intended contact address. Affected people leave

usually assumes that all matters relating to their customer account, too

are to be regulated via the e-mail address with which the company communicates with you in

contacted the past. Accordingly, the GDPR also allows it

not to refer those affected to certain communication channels.

On the contrary, Art. 12 Para. 2 Sentence 1 GDPR even obliges those responsible to

to make it easier for affected persons to assert their rights. so-called no

Reply email addresses where replies to the sender address are not

will be read, are therefore a data protection problem in any case

if at least one address is not given in them, to the customers

can contact and in the case of incoming data protection inquiries

be worked. As a result, those responsible must process all applications for

process the realization of data subject rights, no matter how they are received.

E-mails that are accepted by the mail server as supposed spam

but have been sent to a spam folder and not read are considered as

to be evaluated.251 The same applies to e-mails to still technically active, but

mailboxes that are not (or no longer) actively used. E-mails received there, through the

Data protection rights are asserted must also be processed in a timely manner

250 species. 24 GDPR

251 See Annual Report 2019, July 9th

will. Also spam folders and all technically active e-mail addresses must

therefore be monitored.

When using ticket or so-called customer relationship management

(CRM) systems252 care must be taken to ensure that inquiries are not automatically

be deleted if they are not assigned to an existing customer contact

net can be. Another problem can arise when about in the course

an e-mail communication with the customer service from a certain

time the data protection team is also copied, the CRM system

system is not adjusted to such constellations. In such a case

such an e-mail was only imported into the CRM system, but not into the data

protection team delivered. Customer service took care of answering the

not responsible for the data protection request, but initiated the request

not forwarded to the responsible office either, since the lack of setting of the

CRM system was not known.

When answering inquiries from data subjects, those responsible must

It is also important to ensure that those affected are actually aware of the answer

can take. For example, those responsible may not automatically assume that

go that the previous email address is still active and owned by the concerned

person is, if this z. B. by post to the company.

Companies must ensure that all incoming data protection law

Inquiries can reach the responsible office and be answered by them

will.

252 A CRM system is software for managing customer relationships

gen .

A

and

s

i.e

e

right

P

right

a

x

i

s

10 .10 Identification when asserting rights of data subjects

10.10 Identification when Claiming

data subject rights

Although the GDPR only requires an identity check if there are reasonable doubts about the

identity, we have received a large number of complaints because those responsible

necessary for the assertion of data subject rights (in particular

chen) have requested further information, evidence and actions.

We had to realize that some companies to delete customer

accounts from those affected further information (e.g. customer number,

Billing address, delivery address, [old] order number, [old] invoice number

mer and the date of birth) have requested, although the concern with the same

e-mail address registered with the respective company

was. Even after providing this information, the extinguisher had to search

also partially confirmed again. Some companies charge for

the deletion of customer accounts even copies of ID cards, although when

create the account itself no verification of data was carried out and in the event

free accounts, only name and e-mail address were collected.253

What was particularly bizarre was a company's request to send a

certified photocopy of ID card to prove identity – as

Scan to email.

In the event of justified doubts about the identity, those responsible may

request information needed to confirm the identity of the data subject

are required.254 However, those responsible have to follow the principle of data

nification to be observed.255

The merely abstract danger of falsifying sender addresses256 must not be added

result in inquiries initially being sent across the board for further data comparison or

a confirmation will be rejected and thus processed with a delay. In the

253 For information on obtaining copies of ID cards, see Annual Report 2018, 9.2

254 art. 12 para. 6 GDPR

255 See Art . 5 para. 1 sentence 1 lit. c GDPR

256 so called . “Mail Spoofing”

cases before us there was no indication that the respective

E-mail addresses could have been misused by third parties. Part-

The e-mails were even sent by the responsible sending e-mail server

provided with a valid electronic (DKIM) signature257 so that

it was proven that the e-mail actually came from the specified mailbox

came from. Sometimes there was "back-and-forth communication" with the affected

person, so that access to the e-mail inbox is also

was instructed. And sometimes even then and in spite of were required

Logins additional evidence requested when making the request using the

contact form from the respective customer account.

In particular, the obligation for those responsible is laid down in the GDPR

to make it easier for the data subject to exercise their rights

tern.258 As a result, no substantive or formal hurdles in the

Assertion of data subject rights are set up. through a constant

standard data comparison when asserting the rights of data subjects

even if there is no justified doubt as to the identity of the applicant, the

Exercising the rights of data subjects more difficult. This is also the case when

additional confirmation of the request is required. This applies in particular

if information is sent to the address of the requesting party stored in the data record

to send to the person.

As long as there are no indications to the contrary or a particular risk

stands - for example in the case of particularly confidential data or persons at risk - is

to be assumed in principle that a requested self-assessment to the

address stored in the data record can be sent without a

additional proof of identity is required. If there are already customers

accounts, these are regularly the first choice to identify those affected. New

Online services enable remote identification not only through the

257 DKIM stands for Domain Keys Identified Mail. This is a method of

Email Authentication . DKIM adds a digital signature to emails that

sender domain and is used for all outgoing emails. This

is a technique that forges the e-mail sender or the content of e-mails

makes recognizable . Wrong or forged e-mails can thus be automatically rejected

or treated separately, unadulterated e-mails are accepted and treated as genuine

be traded .

258 Art. 12 para. 2 sentence 1 DS-GVO, so-called. relief requirement

eID function of the identity card, but also, for example, via the online bank

king.

Since companies systematically and without reason in a number of cases exercise the

have made the rights of those affected more difficult, in particular by unlawfully denying

further proof of the identity of the data subjects have requested

we hand these cases over to our sanctions office for further examination.

Requesting further identifying information, evidence and confirmations

genes without reasonable doubts about the identity provides for those affected

represents an additional hurdle and can prevent them from exercising their rights as data subjects

to assert. However, the assertion of data subject rights should

be as simple as possible. Requesting further information must therefore

Cases of justified doubts about the identity of data subjects reserved

stay.

10.11 The Eternal Battle for Information – Here:

Credit Data

When examining a case, it turned out that the company responsible

regularly take credit reports from a credit agency when the contract is concluded

obtained from the respective customer. The credit data

are then stored for the duration of the contract. This practice is specifically

case also permissible and presented accordingly in the data protection declaration.

puts. However, the company did not contact those affected at their request

informed of the information received from the credit agency. specifically

In most cases it was the score calculated by the credit agency

re value, the rating level,259 if applicable, previous addresses and the respective place of birth of the

A

and

s

i.e

e

right

P

right

a

x

i

s

259 credit bureaus collect information about people, specifically about

their economic situation and their payment behavior . From this they calculate

A numerical value that indicates the solvency (creditworthiness) of the person concerned

should depict the so-called score value . Depending on this score value, the affected

assigned a probability with which they open demands

settle the so-called rating level . This information can companies

retrieve before they enter into contracts where they rely on future performance

the contractual partners have to leave .

169

concerned. At our request, the company justified this practice

with the general terms and conditions of the credit agency. After that the un

company is not authorized to pass on the data received to third parties.

The refusal to provide information about the data communicated by the credit agency

unlawful.

Those affected, in this case customers, have the right to information about everyone

personal data that a company processes about you.260 This

basically summarizes all stored information, no matter where it or the

Responsible has this information.

Each person should have the opportunity to check whether the data stored about them

guaranteed information is correct and processed lawfully. This is

particularly important for information about creditworthiness. Because it acts

This often involves data that the data subjects do not themselves give to those responsible

made them available, but who obtained them from external sources (e.g. from

credit bureaus) have received. Based on this information, companies

whether and under what conditions they enter into a contract with a customer

contract with a customer. If this information is not (anymore) correct

are or are being processed in an unlawful manner, this may result in a no

justified refusal of contract conclusions or worse con-

conditions in contracts. This can have far-reaching consequences for those affected

to have.

The right to complete information is therefore mandatory in the GDPR

wrote. Any restriction on this right must be contained in the GDPR itself or

exceptionally in other legislation of the European Union or

of the member states to which the person responsible is subject

be.261 Private contracts that restrict this right constitute a violation of

gen the DS-GVO. In German civil law are also agreements that the

260 kind . 15 para. 1 GDPR

261 Art. 23 GDPR

Restrict the rights of non-participating persons262, generally inadmissible

and therefore ineffective.

The general terms and conditions of the credit agency could

In the present case, therefore, we are not exempt from the obligation to provide complete information

release.

When we spoke to the company, it received information from information

has now received by default in his provision of information

taken.

In principle, companies are obliged to provide all information on request

to disclose that they store about the person concerned. This also includes

Information obtained from a credit reporting agency. A restriction

Any exercise of this right through a contract with the credit agency is not permitted.

262 so called . Contracts at the expense of third parties

171

s

i

x

a

right

P

right

e

i.e

s

and

A

11 finances

11.1 Unlogged Bank Account Access

We received a complaint from a bank customer who had reasonable suspicions

had that an employee of the bank had unauthorized access to the contents of his bank

had taken account. The bank's response to the customer's request for

Research remained very vague and indefinite.

The same thing happened to us with our requests for comments. In several

In writing, the bank avoided answering our specific questions.

words. Instead of a clear statement as to whether and, if so, who has access to the account movements of the

customers had accessed in the period in question was generally acknowledged by the high

security awareness of the bank and extensive measures for IT security

safety spoken. Only gradually did the statements become a little more concrete.

So the bank finally went so far as to say that the

No access, apart from "technical" access, to the relevant

current account could be determined. What is meant by technical accesses

be, we of course questioned it. These are the necessary algorithms

We were informed about rithmic accesses, for example to trigger transactions. in the

In the last reply, the company had to admit that requests

of employees on account and transaction data not logged at all

be lled.

At this point we conducted an audit of the company. at

this revealed the following: A significant proportion of employees in

higher positions, but also those employed in customer service

Access to the account master data and the transaction data of the respective account

ten. This is generally not inadmissible if the employees concerned

who need access rights to do their daily work. In service is

this is understandable if customers have questions about certain bookings, for example

ben.

The data that can be accessed is quite sensitive. Based on

Account movements can meanwhile - in particular due to the

greater use of cashless means of payment – a significant part

of private life can be understood. Also according to Art. 9 Data

General Protection Regulation (GDPR) data that requires special protection, such as B.

Party memberships or trade union membership would be so easy to determine

telable.

There are a number of measures to prevent improper data access

to take. Of course, this includes the number of access rights

are to be reduced to a minimum and the employees concerned

are obliged to maintain data secrecy. had this obligation

However, the company already informed its employees before our audit

imposed. In addition to other conceivable technical measures for access

restrictions are also a logging of such accesses and a re-

Regular, at least random, review of the recorded programs

protocol data in a defined, data protection-compliant procedure

necessary.

This insight also continued during the audit of the corporate

step through slowly. In the meantime, the bank has the necessary

Detailed logging of access to account and transaction data by employees

implemented. Our sanctioning body is currently checking whether and, if so, which ones

Sanctions for years of disregard of basic data protection principles

pien are to be imposed.

Controllers have access to personal data

to limit the minimum necessary for the normal case. who

cess number of employees opened access to personal data,

The determination of unauthorized access must be made via access logging

enable. Unfortunately, we could not give the complainant a

proof of his suspicion, and also the possible abusive

che use of access rights could not be prosecuted due to a lack of evidence

the. But we were able to ensure that data protection awareness increased

gene and the technical and organizational processes of the credit institution

have now been redesigned in accordance with data protection regulations, at least in this respect

prevent such cases as far as possible in the future.

11.2 Dispute about the scope of the obligation to provide information

s

i

x

a

right

P

right

e

i.e

s

and

A

A customer informed his bank of his right to information

custom.263 In particular, he wanted to determine whether the bank

has unlawfully transmitted the data collected. Although the bank issued an

future, but only named the categories of recipients (e.g. service providers,

Credit service institutions, authorities), but not the specific recipients

coagulate. She justified this by saying that in the event of a request for information,

The person responsible has the right to choose whether to give the data subject the specific

catchers or only recipient categories. Also consider

the bank treats the data recipients as trade secrets; this must

not be disclosed when requesting information. The bank customer was with me

dissatisfied with this information and complained to us.

Affected persons have a claim against the responsible persons

Information about "the recipients or categories of recipients

where the personal data has been disclosed or is still being disclosed

become".264 Although the wording of this provision seems to suggest that it is

in the case of "recipients or categories of recipients" by equivalent alternative

ven acts and insofar as there is a right of choice of the person responsible

could. Restriction of information to categories of recipients

without disclosing their identity, however, would serve the purpose of the GDPR.

run counter to enabling data subjects to exercise legality

to be able to check the processing of their personal data265 and

their rights towards those responsible, in particular to rectification,

Deletion, objection and restriction of the processing of the data apply

close. The data subjects can assert these rights towards recipients

263 See Art . 15 GDPR

264 art. 15 para. 1 letter c GDPR

265 See EG 63 sentence 1 GDPR

but only then applies to their transmitted personal data

do if they know the identity of the addressee. A limitation

the right to information only to categories of recipients is sufficient

respect for the rights of the persons concerned. This would even

constitute a violation of European primary law.266 Our interpretation

also corresponds to the will of the legislature, because after that those affected have

People have a right to know and to know who the recipients are

of the personal data.267 Accordingly, an indication of categories

of recipients is only sufficient if transmissions are fundamentally

are also planned but have not yet taken place.

Nor can the bank successfully invoke the recipients

not having to identify the data as it represents a trade secret

ten. Business secrets of the person responsible can

reduce the claim of the person concerned, but the law has this only for

regulates the copy claim.268 In some cases, the view is taken that the

Legislators do not have the right to information if third-party rights exist

only want to limit the copy claim, so there is an unplanned lie

cke vor.269 But this view is not to be followed. While at the right to

Copy the impairment of rights and freedoms of other persons in particular

ders is obvious, it can hardly be assumed that an impairment of third parties by

the identification of the data recipients is to be feared.270

Since the bank also refused to give the complainant the

to name specific recipients, the process was forwarded to our sanctions

continue to examine the initiation of administrative offense proceedings

directed.

266 See Art . 8 para. 2 Sentence 2 Charter of Fundamental Rights of the European Union: "Every person

son has the right to receive information about the data that has been collected about you

and to obtain the correction of the data."

267 EG 63 sentence 3 DS-GVO

268 See Art . 15 para. 3, 4 DS-GVO, EG 63 sentence 5 DS-GVO

269 See Stollhoff in Auernhammer, DS-GVO/BDSG, Art. 15, para. 33; Harting, data

Basic Protection Ordinance, Rn . 684

270 See also Ehmann/Selmayr, General Data Protection Regulation, Art. 15, para. 2

In principle, data subjects must be informed of both the categories of

Notify recipients as well as the specific recipients.

11.3 Blocking of the credit card by family

relatives

s

i

x

a

right

P

right

e

i.e

s

and

A

A credit card owner wanted to pay for his hotel stay with his credit card.

pay, but this was not possible because his credit card had been reported as stolen

was. He applied for and received a new credit card from his bank. Although he

informed the bank that he had not reported his credit card as stolen,

the bank did not investigate the transaction. Three weeks later the person concerned

fene when going to a restaurant to find that his credit card has been re-assigned

was reported stolen. He suspected that a third party was the owner of his

Credit card issued (identity theft) causing card to be blocked

have.

The suspect's suspicions were not confirmed. After our request for information

The bank determined that in both cases the credit card was not considered stolen

had been reported. The card was blocked without a corresponding thief

steel report from an employee of a technical service provider of the bank

been caused. This could be determined. It was one

Relatives of the person concerned who resolve a family dispute in this way

wanted to. The bank has since fired the employee. Since the bank

conduct of the employee of their processor must be held accountable,

we warned the bank. Banks should, moreover, already at a first

determine the facts of the unauthorized credit card blocking.

Illegal interventions in banking systems are threatened not only by attacks

outside, but also from the inside.

12 Transport, Tourism and

credit bureaus

12.1 "Your job center notice, please"

citizens with little or no income

the Berlinpass offers discounted access to education, sports, culture and the like

Local public transport (ÖPNV) of the city. Due to the Corona Pan-

demie, these passports are not currently issued. reached us in the

complaints from eligible citizens in recent months

Citizens who reported that as part of controls in public transport

traffic to have been asked to submit a valid benefit notice in the original

to show off.

A

and

s

i.e

e

right

P

right

a

x

i

s

Expired Berlin passes were accepted by both the S-Bahn and the BVG

as a gesture of goodwill until December 31, 2020. However, demanding

authorized persons who have not yet received a Berlin Pass are asked to

requested to carry the original notification of benefits with them and their required

community number, the file number or the housing benefit number on a

Enter the purchased Berlin ticket “S”.271 The original notifications of benefits

served as proof of entitlement to travel with the Berlin ticket "S". she

contain a variety of personal data such as name, address, birth

date, marital status and sensitive data such as the underlying authorization

reason, e.g. unemployment, asylum seeker status or status as an op-

fer of the SED injustice.

Against the obligation to present the benefit notifications in the original, there are

serious concerns because, due to the large number of personal

personal data violates the principle of data minimization.272

According to this principle, the processing of personal data must

271 See https://www.berlin.de/sen/soziales/soziale-sicherung/berlinpass/

272 See Art . 5 para. 1 letter c GDPR

Purpose adequate and relevant and relevant to the purposes of the processing

necessary amount be limited. In the present case, the scope of the

the data to be disclosed in the benefit notification beyond what is required for

the specific case, namely proof of entitlement. Of the

Purpose, proof of authorization to use a Berlin ticket "S".

can be achieved with a significantly smaller amount of data.

Alternatives with a lower level of intervention would be, for example, issuing a

corresponding certificate by the service-granting bodies, which

finally contains the necessary data.

We took the complaints as an opportunity to contact those responsible

approach to discuss more privacy-friendly alternatives.

The process is still ongoing. The responsible senate administration and the

service-providing bodies should offer a procedure which

thriftiness into account and still gives the possibility to controllers

gives to check the eligibility for benefits.

12.2 Driving without a ticket – data transfer

to collection agencies

s

i

x

a

right

P

right

e

i.e

s

and

A

If you use local public transport without a valid ticket,

regularly an increased fare. A citizen complained in

in this connection with us that his personal data

was passed on to a collection agency after a ticket inspection

and beyond that for a period of one year with the transport company

be saved.

The complainant was found during a ticket inspection in the

S-Bahn with a ticket, but without the corresponding customer card.

hit. The absence of a customer card for the corresponding ticket

is considered invalid according to the conditions of carriage of the S-Bahn Berlin GmbH

Driving license.273 The personal data of the complainant were

273 Section 8 of the Conditions of Carriage of S-Bahn GmbH

recorded and to claim the increased fare to an in-

passed on to cash register companies. This made the increased transport

then applies to the complainant.

Driving on S-Bahn trains without a full ticket

Berlin GmbH authorizes inspectors to process personal data of the

to take in other people. The processing of the data takes place for the purpose of fulfilment

of the respective contract,274 according to the conditions of carriage of the S-Bahn

Berlin GmbH by using the ride offer also implicitly between

of the S-Bahn Berlin GmbH and persons without a valid ticket

will.275 The transfer of the processing of the increased transport

required data to a debt collection agency to safeguard the

legitimate interests of the transport company.

The General Data Protection Regulation (GDPR) allows the processing of data

among other things, if this "to protect the legitimate interests of the responsible

literal or a third party [is] required, unless the interests or

Fundamental rights and freedoms of the data subject, which include the protection of personal

of data related to the company prevail".276 On this basis, the

legitimate interests of the person responsible and the interests of each

because the person concerned are weighed against each other. The Berlin S-Bahn

GmbH is not obliged to assert a due claim itself, but

You can commission a collection agency to do this. Overriding Interests

of the data subject are not evident in this respect. Accordingly allowed

the data required for the purpose of asserting the due claim

be sent to the collection agency. Because without the appropriate

personal data, the transferred claim could not be collected.

Storage of the data for a period of one year at the S-Bahn Berlin

GmbH is also permissible.277 The transport company has an authorized

interest to check within a limited period of time whether individual

274 See Art . 6 para. 1 sentence 1 lit. b GDPR

275 so called . actual contract

276 See Art . 6 para. 1 sentence 1 lit. f GDPR

277 See Art . 6 para. 1 letter f GDPR

are often encountered without a valid ticket in order to possibly be penalized

to submit an application for so-called fraudulent promotion278.

Personal data, the assertion of an increased carriage

payment fee may be transmitted to a debt collection agency.

The transport company that charges an increased fare

may also store the relevant data for a limited period of time

chern.

12.3 "eTickets" at the transport association

Berlin-Brandenburg – Data protection

does not move

s

i

x

a

right

P

right

e

i.e

s

and

A

The Verkehrsverbund Berlin-Brandenburg has been driving for several years

(VBB) is advancing the switch from paper tickets to electronic tickets.

Many types of tickets are already issued on the electronic "VBB-fahr-

Card" provided. We accompany the project from the start with our

sighting activity This year, too, we had to identify deficits.

For several years, the VBB has been operating a technical system for its employees

affiliated companies (e.g. Berliner Verkehrsbetriebe – BVG, S-Bahn Berlin GmbH

and Verkehrsbetrieb Potsdam GmbH) in the Berlin-Brandenburg area

Switching of the transport companies from paper tickets and paper-based

which enable subscription certificates to electronic tickets.

This includes the VBB environmental card, the "10 o'clock card" by subscription, the

VBB subscription for trainees and the VBB subscription 65 plus, the

step by step to the "VBB-fahrCard" (driving authorization in the form of a chip card)

have been converted.

The VBB supports the operation of the system for the electronic fare

management (EFM) on the preparatory work and services of VDV eTicket

278 See Section 265a of the Criminal Code (StGB)

Service GmbH & Co. KG from Cologne.279 This subsidiary of the association

German transport company (VDV) has with the so-called VDV core application

tion standard laid the basis for electronic ticketing in Germany.

winds and maintains the entire system and operates its central components.

Unfortunately, we had to find out from multiple inquiries that despite the long

Gen history the data protection responsibility for the operation of the

EFM overall system and thus also the legal basis for all associated

which data processing has not yet been clarified.

Equally incomplete is the information about which process participants

ten to which usage data have access. This applies in particular to the

third-party providers with whom the VBB cooperates. That's how she can

VBB-fahrCard for charging electric vehicles at the Berlin charging station

infrastructure are used. So far, the VBB has not been able to support us

Describe in a comprehensible manner how such third-party providers deal with customer data

from the EFM, save them, use them and delete them again.

We also had to repeatedly point out that customers

who must be given the choice of attaching a photo to the chip card

want to leave or not. If the holders of the electronic tickets

ckets can also be identified as authorized users in other ways during checks

e.g. B. through their ID card, then there is no need for a photo

on the fahrCard if the person concerned does not want this.

As a positive development, we were able to note that the VBB is planning to

to reduce the data stored on the fahrCard. In the future, only the number

the tariff honeycomb, i.e. the larger, aggregated tariff area. This

strengthens data protection, since the previously stored exact location information ever

according to technical configuration, movement profiles of the customers

to create. Due to this innovation, however, only all

can be determined in general whether the person inspected in a tariff agreement

bid is on the road, for which a corresponding driving license has also been acquired

became. And only this can be the goal of a ticket inspection.

279 See https://unternehmen .eticket-deutschland .de

Another positive aspect is that the VBB has a technical solution

want to provide, with the help of which customers themselves can obtain driving data from the chip card

ten can delete. Because there are up to ten data records on the chip cards

Trip controls saved. So far, data from the chip cards can be transferred via

Read mobile devices free of charge, but only in the customer centers of the Ver-

transport companies (e.g. at BVG and S-Bahn Berlin GmbH) to self-service

devices can be permanently deleted. This would be due to the new technical

solution simplified at least in part. Deletion by customers

According to information from the VBB, it would be technically easy for all those people

can be implemented that have a smartphone with an NFC interface280. - We have-

asked the VBB to also clearly announce this option.

Electronic tickets offer customers increased convenience.

However, this must not be at the expense of data protection. The offering

Businesses need to be transparent about what data is under

which responsibility is processed and which bodies have access to it

to have. Only in this way can those affected exercise their rights. The responsible

The data protection supervisory authorities of the states of Berlin and Brandenburg are

who continue to jointly observe the developments in the "VBB-fahrCard".

and insist on the elimination of deficits.

12.4 Dealing with data subject rights at the

Booking of private holiday accommodation

s

i

x

a

right

P

right

e

i.e

s

and

A

Booking private holiday accommodation online is becoming increasingly popular

Ness. However, as part of such an online booking with the offering

collects personal data on the platforms. The GDPR makes it possible

the data subject, inter alia, to request information about the storage of this data

and, if necessary, to have them corrected or deleted. Complaints received by us

which show that the exercise of these rights, but also the use of the platform

often form themselves from these by requesting copies of ID cards

is made more difficult.

280 NFC stands for “Near Field Communication” . This is a technique

in which devices are connected to each other over short distances (usually a few centimetres).

can communicate via electromagnetic induction to exchange data.

We often receive complaints from citizens who

their right to information or deletion from the online platforms

wanted to assert and initially for the purpose of a reliable identification

asked for a copy of their identity card or driving license

the. But not only when it comes to asserting the rights of data subjects in the

course of the use of such offers, but also at the beginning of the

citizens are often asked to produce an ID card

provide pie.

When renting or booking private holiday accommodation via online platforms

may form an identity check of hosts and guests themselves

be legitimate interest; nonetheless, identity checks using copied

ter official photo identification to make high demands. A processing

The provision of a complete copy of an ID card is only lawful if it is used to obtain

performance of a contract with the data subject is required.281 The mere

Use of the platform cannot depend on the presentation of identification data

be made.

If citizens exercise their rights to information, correction or deletion

investigation, an identity check is only lawful if

if there are justified doubts as to the identity of the person concerned.282 In

In this case, however, only such additional information may

are required to confirm the identity of the person concerned

are.

If, exceptionally, a copy of an ID card is required to avoid an identity

theft can be demanded, the customers should be made aware of this

be that unnecessary data such as ID number or eye color

can be blackened.

We therefore recommend that those affected contact the respective company

are increasing against the practice of blanket requests for ID card copies

fight back

281 See Art . 6 para. 1 sentence 1 lit. b GDPR

282 See Art . 12 para. 6 GDPR

12.5 A man with fourteen birthdays

s

i

x

a

right

P

right

e

i.e

s

and

A

A credit agency had a large number of incorrect data in its database

stored for a complainant, including fourteen dates of birth. Of the

incorrect data in the database of the credit agency, the complainant learned

er when he made use of his right to information. For this he saw himself

prompted when a company paid him a debt from one of his namesakes

ter wanted to collect. This had stated that its data from the credit agency

to have received.

When the complainant found out about the data stored about him by the credit agency

data, the latter first informed him that she had no data about

would have saved him. However, when asked again, it turned out that

the credit agency had the relevant data in its database. the

The overview then sent to the complainant revealed astonishing things:

The credit agency had a total of fourteen birth dates in the "Date of Birth" section.

stored data, all of which were assigned to the complainant. This

fourteen dates of birth spanned a period from 1977 to 1997.

In addition, the data set contained 26 postal addresses at which the

complainant should have lived up to now. After we have addressed the matter

had taken, we learned from the credit agency that this data was accidental

had been saved due to an internal misunderstanding.

Credit agencies are authorized to process personal data for the purpose of

to process the provision of information if it is necessary to protect their legitimate interests

interests and does not violate the fundamental rights and freedoms of the

affected persons outweigh.283 At this point, the GDPR requires an interest

weighing of interests in the specific individual case. Fundamental rights and

Fundamental freedoms of the persons concerned, e.g. B. not regularly when the

Credit agencies transmit current address data to creditors.

A decisive criterion for the legality of the storage is the

correctness of the data. The stored data must be factually correct and

283 See Art . 6 para. 1 sentence 1 lit. f GDPR

updated if necessary.284 Accordingly, procedures are

to correct or delete inaccurate data immediately. at a

collection of fourteen dates of birth assigned to a single person

net, it follows that thirteen of these dates must be incorrect.

The 26 stored postal addresses would also give rise to doubts about the

have to justify the accuracy of the data.

This case also shows vividly what consequences incorrect data records can have.

to. It was certainly not pleasant for the person concerned to object to claims

to resist that a namesake would have had to pay.

The credit agency informed us as part of our investigation that the

affected data has been blocked in the meantime and then deleted

would. In addition, we were assured that this event was the occasion

will be taken to follow up the internal procedures technically and organizationally

mend

Credit bureaus may only process factually correct data and are

is obliged to use technical and organizational measures to ensure

ensure that incorrect data is corrected or deleted immediately.

284 art. 5 para. 1 letter d GDPR

185

13 video surveillance

13.1 Important Documents Regarding Video Surveillance

adopted

s

i

x

a

right

P

right

e

i.e

s

and

A

Two important documents on video surveillance were published this year

decided: On the one hand, at the beginning of the year, the European

ische Data Protection Board (EDPB) its guidelines 3/2019 on processing

personal data through video devices.285 Then in September, too

the German supervisory authorities and updated their guidance

help with video surveillance by non-public bodies.286

As we reported last year,287 our agency was involved in the creation

development of the guidelines of the EDPB and coordinated Europe-wide

the work as the main rapporteur. In terms of content, the guidelines state, among other things,

that any video surveillance involves an encroachment on personal rights

is bound. Therefore, you must always have a legitimate interest of the camera operator

are based on. This interest must be objective, i. h., at

video surveillance for security reasons must always include actual

There are indications of a danger to life, limb or property. the lead

lines make it clear that a purely subjective sense of security is not enough to

to justify video surveillance.

The guidelines also create a view to the processing of biometric data

Clarity. According to the General Data Protection Regulation (GDPR), it is private

in principle without the express consent of the person concerned

offered biometric data for the purpose of identifying specific individuals

to process. The guidelines now specify the strict requirements

According to the DS-GVO to the effectiveness of such consents. Also, they offer

285 See https://www .datenschutz-berlin .de/infothek-und-service/veroeffentlichungen/

guidelines

286 See https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/

orientation aids

287 JB 2019, 14.2.

practical assistance on questions of transparency in video surveillance

measures and to exercise the rights of data subjects.

In September, the conference of independent data protection

federal and state supervisory authorities (DSK) an updated version

the "Guide to video surveillance by non-public bodies".

The original orientation, which was created under the earlier legal

assistance has been fundamentally revised and adapted to the legal framework

Gen of the DS-GVO and to the above EDPB guidelines adapted. It also contains

Parts that go beyond the European guidelines, such as e.g. B. Sections to

Video surveillance of employees and for data protection assessment

from door and bell cameras, drones and trail cameras as well as dashcams. dar

In addition, a checklist for camera operators with the most important

Test points provided in advance of video surveillance.

Both documents on video surveillance not only make important contributions

for the uniform application of the GDPR. They also contain practical

Information for operators of video systems. Unlike the orientation

with the help of the German supervisory authorities, however, the European guidelines

lines not primarily to camera operators, but also contain

a separate chapter with information for data subjects on how to exercise their rights.

13.2 Südkreuz test station – “intelligent”

Video surveillance not so smart after all

After the federal police had used Südkreuz station as a test laboratory for years

used for biometric facial recognition, the German

sche Bahn use the station for their own tests.288 It worked – differently than with

the Federal Police tests – not about the processing of biometric data

for the purpose of identification, but for the automated detection of

dangerous situations.

A

and

s

i.e

e

right

P

right

a

x

i

s

288 See Annual Report 2018, April 4 and Annual Report 2019, January 11

187

Specifically, the following five scenarios were the subject of the test:

• People lying down (e.g. people who have fallen and need medical help

gene),

• Entering defined zones (e.g. people who are too close to the platform

edge are located),

• Gatherings and flows of people (e.g. detection of gatherings before

escalators or dynamic movement of groups of people),

• People counting (e.g. number of people in a defined area),

• objects parked (e.g. luggage left unattended for a long time

cke).

For the test, the video material was used, which is already

hof Südkreuz. Because like many train stations of the Deutsche Bahn

and the Berliner Verkehrsbetriebe (BVG) is the Südkreuz station with numerous

equipped with surveillance cameras. These primarily serve to

of domiciliary rights and the safety of passengers as well as in the case of

the incidents to assert any claims for damages

to be able to Therefore, the data processed with the video cameras

so high resolution that people can be recognized and, if necessary, identified.

Based on this video material, various software products were

tested to see how reliably they react in one of the above situations

ren. For the test, the technology was sent by three selected providers to the

connected to a conventional video surveillance system at Südkreuz station.

The tested software should now run through the automatic evaluation of the

available video material, whether incidents of the situations mentioned

lie. Then the security personnel in the video

be informed automatically. This should change the situation on the

Look at the screen and decide on further action.

The aim of the test was to inform the staff of the video control center in regular operation through the

Recognizing the mentioned scenarios in his daily work.

The results of the test available to us lead to considerable doubts about the

admissibility of the use of the technology tested here under data protection law

regular operation. It is true that Deutsche Bahn has a legitimate interest

in the above intervene in situations and for the safety of staff and the

To look after passengers or exercise their domiciliary rights at the station. However

the measures taken to achieve these goals must always be

be suitable, necessary and proportionate.289

There are already considerable concerns about the suitability of the "intelligent

genten" video surveillance. According to the information we have, it is

to assume that it is ready for the market for regular use in the complex environment

of a passenger station is not given at the present time. The systems

did not recognize many situations or generated false alarms. As a result, the

target hit rate of 95% of successful alarms from any system either

can only be approximately achieved. In some cases, the hit rate was only 27%.

As a result, there is a need for optimization in all systems.

Against this background, the question of proportionality also arises,

since in regular operation a large number of innocent passengers are caught by the video surveillance

would be affected, who use the station every day. Because of the false alarms

they would unduly become the subject of further scrutiny. Leads

the measure mentioned is not actually applicable due to the high error rates

an improvement in passenger safety, this is disproportionate

and therefore not compatible with data protection regulations.

It is all the more astonishing that the Federal Ministry of the Interior and the German

Bahn end of the year announced the possibilities for intelligent

Video analysis in practical application in the vicinity of the Südkreuz train station

to be explored over a project period of another three years, since despite all

lem in video analysis systems promising approaches for detection and

See notification of operationally relevant situations.

We will also closely monitor future tests and then check whether

in which the data protection regulations are complied with.

289 See Art . 6 para. 1 sentence 1 lit. f GDPR

s

i

x

a

right

P

right

e

i.e

s

and

A

After evaluating the test results available to us, we assume

that the use of such systems is currently not possible due to high error rates

reliable aid represents the Deutsche Bahn in perception

to support their tasks. The use of the tested software in general

operation is therefore not permitted according to the current status.

13.3 Even more in focus: video surveillance

in small business

We have dealt with a number of retail video surveillance cases

del and to do in the hospitality industry. This has been in previous years

a focus of our activities, since surveillance cameras are becoming cheaper and cheaper

and are available everywhere, the operators, on the other hand, often differ

are not clear about the data protection regulations. This year came

added that due to the corona pandemic, small businesses are more

than was otherwise the focus of the police and regulatory authorities. As part of

of checks, since the beginning of the pandemic, they have checked compliance

compliance with distance rules and hygiene measures in commercial units in the

entire urban area. This affected gastronomic facilities, such as restaurants

rants, restaurants, snack bars and shisha bars, but also other small businesses,

such as late purchase shops, hairdressers, nail salons, bakeries, casinos,

sports bars and betting shops. For our work, this had the positive

Beneffekt that the authorities mentioned in the control of compliance with the

Corona measures often also a suspicion of illegal video transmission

surveillance and forward the cases to us for further processing

could. Since we are different due to our low staff capacities

as the police and regulatory authorities - cannot be on site all the time, we are open

such assistance as well as information from the population.

These cases often concerned video surveillance that went beyond the borders of a

gene store also covered the public street area. Such

Monitoring is not permitted, since the operators are regularly informed of the

There is no interest in monitoring public space. exceptions

stand only in narrow areas and only if this is the specific case

is required, e.g. B. to counteract damage to property. So has the

case law in one case the extension of the scope to ma-

ximum one meter beyond the property boundaries is considered permissible, since

This was the only way to contain graffiti on the house facade.

The monitoring of one's own commercial premises is also subject to strict requirements

linked to this, as video surveillance regularly entails an intrusion into

moral rights of the persons affected by such measures.

In particular, the collection of personal data using video technology only

permissible, insofar as it is required to protect legitimate interests, among other things, and

unless the legitimate interests of the data subject prevail.290

The video surveillance of a business premises with regular customer traffic

is z. B. to prevent or to preserve evidence of theft only

negligent if objectively there is a dangerous situation. An indication of this is B. if it

actually to criminal incidents in the shop in the past

or came in the neighborhood. These incidents should be

be documented with the police with file numbers. A purely subjective one

A feeling of insecurity or fear of theft is not enough. Is there a

driving situation, the video surveillance must be switched off. Also not allowed

is video surveillance for behavior and performance control of the people working there

gene employees.

Other cases affected - until they were closed due to Corona - restaurants,

which are to be judged particularly as they are meant to linger and relax

and communication are intended. The consumption attributable to the leisure sector

Keeping guests in a restaurant involves a particularly high level of protection

of the personal rights of those affected. A video surveillance disturbs

the unimpaired communication and the unobserved whereabouts of the

restaurant visitors and thus reaches particularly intensively into the personal

privacy rights of the guests. Your legitimate interests therefore prevail

normally compared to the legitimate interest of the restaurateur

a surveillance.

In many cases, it was ultimately about the inadequate implementation of the

duty of transparency. Missing or inadequate information on the video surveillance

290 See Art . 6 para. 1 sentence 1 lit. f GDPR

are even the most common violations that occur as part of trade controls

be identified by regulatory agencies and the police. In this context

we always refer to an example of a sign that we have on our website

website,291 and explain in detail to the operators

what information to share with their guests, customers and employees

are.292

Because of our good experiences we have decided to continue our cooperation

with the police in this area. Together with the police

We have developed a guideline that police officers can use on site

should make it easier to recognize and document illegal video surveillance

animals. We hope that this will lead to a significant increase in efficiency in the

cooperation of both authorities.

The cooperative support of the police and the regulatory authorities enables

gives us a widespread review of video surveillance systems

in small businesses of the entire metropolitan area, which we previously discussed in this scope

couldn't afford. To have the admissibility of video surveillance systems

we have created a guide and a guideline that we have on our website

keep the website ready for retrieval.293

291 www .datenschutz-berlin .de/themen-videoueberwachung_dsgvo .html

292 Art. 13 GDPR

293 See 13.1

14.1 Developments in the Sanctioning Body

In the third year of the entry into force of the General Data Protection Regulation (GDPR)

GVO) we now mostly process cases according to the new fine

regulations. In addition, only very few cases refer to the old one

legal position.

This year we fixed 47 fines totaling EUR 77,250.00

set.

In addition, 38 penalty payment notices were issued.

In 5 cases we filed a criminal complaint.

14.2 Penalties for Unauthorized Use of

Police database POLIKS

A large part of the proceedings conducted by the sanctioning body are directed against

Police officers who, without authorisation, d. H. without an official

Reason, personal data of third parties from the internal police database PO-

Get LIKS.

POLIKS is one of the most important electronic work tools for the police and

accordingly holds a large amount of personal data, some of which is very sensitive.

The database includes data on suspects, criminals, victims

and witnesses recorded and stored. The police use POLIKS as information

onsystem for their legal tasks in the field of criminal prosecution and the

security.

Unfortunately, some police officers and police officers repeatedly

allows access to the extensive data contained in POLIKS for private purposes

catalog too.

193

In one case, a policewoman used POLIKS to find the new girlfriend's ex-girlfriends

to find partners and then open them up for talks

to search.

In another case, a police officer had the data of all neighbors

queried in their own multi-family house in order to

formations later in neighborly disputes against the individual

to play off the residents of the house.

In another case, at the request of various friends, a police officer

information from POLIKS and via a private instant

Messenger system sent. This was about data from teachers of the

of, from neighbors or even partners of the inquirer.

We have also imposed a fine on a police officer who

Used LIKS as a search engine for contact details of a seller. After this

he did not enter the correct telephone number when searching using the "Google" search engine

mer of the seller of a deck of cards, he tried about POLIKS, which

get meaningful data.

This year we have a total of 33 cases against police officers

Police officers initiated and already 9 fines against this group of people

enacted However, many methods have not yet been determined.

14.3 Data protection also needs district courts

first instance

With the "draft of a law to make the fine procedure more effective"294

the Federal Council wants the previously provided for in the Federal Data Protection Act (BDSG).

first-instance jurisdiction of the regional courts for

ordinance (DS-GVO) fines that amount to more than

exceed 100,000.00 euros, delete 295. If this were to be decided,

294 BR-Drs . 107/20

295 See § 41 para. 1 BDSG

district courts will in future decide on fines of this magnitude

the.

Administrative offense proceedings on the basis of the GDPR, which have very high

hen fines are concluded, indicate both legal and indicative

a special one in terms of the economic and technical context

Complexity and therefore require an assessment by a jury

collegial court, as is the case with regional courts, but not with district courts

are. Such procedures are comparable to economic criminal cases, which also

assigned to the regional courts. It is not without reason that the European

Legislators based on the fine provisions of the DS-GVO on antitrust law.

The stated goal of the draft law, to make fine procedures more effective,

would not be achieved with the intended change in jurisdiction

be enough. When drafting the law, the variety

layered nature of GDPR fines misjudged. A deletion of the regional

Moreover, the district courts would not have jurisdiction for these proceedings

relieve, but on the contrary burden even more than before, because the

complexity of such procedures the work capacities of the single judges

District courts would blow up completely.

The right of sanctions of the DS-GVO is - contrary to what the Bundesrat assumes - with

the sanctioning of conventional German administrative offences, such as

Road traffic fines, in no way comparable. Unlike there goes

the proceedings under the European GDPR are not about prosecution

of petty crimes, but about procedures that are highly relevant throughout the Union

Protection of the free movement of data and the privacy of citizens

eng. Millions of personal data and globally active

ing companies may be affected. For similarly complex administrative offences

in antitrust matters in Germany there is even a competence of the supreme regional courts given. This evaluation also comes in the extent clear Wording of § 41 Para. 2 Sentence 1 BDSG, which has a corresponding application of the regulations on the criminal procedure and thus also an occupation of the criminal courts as so-called large fine chambers according to § 76 court sungsgesetz (GVG).

195

With these procedures according to the GDPR, it really does not have to be one restriction of a district court's jurisdiction, but rather to consider whether these proceedings are not even complete in the first instance should be referred to the jurisdiction of a higher court, possibly also - at least partially - to a higher regional court based on the antitrust regulations.

The Berlin Commissioner for Data Protection and Freedom of Information has sitting of the working group sanctions a resolution of the conference of independent federal and state data protection supervisory authorities (DSK) of September 22, 2020, which stipulates the retention of the legal jurisdiction for DS-GVO fines over 100,000.00 euros.

The DSK passed this resolution.296

14.4 Fictitious job advertisements at the Federal Employment Agency

On the online job exchange of the Federal Employment Agency, presumably published job advertisements found in order to access applicant data for an il- to obtain legal resale. According to media reports, this should be about act around 120,000 fictitious job advertisements.

We already have this based on a note from the Federal Employment Agency

filed a criminal complaint with the public prosecutor in 2019.

After several months, the public prosecutor's office

shared that she intends to discontinue the criminal proceedings that have been initiated because

an unlawful act cannot be proven. This was justified

among other things with the fact that no concrete victims are known and both against

via the Federal Employment Agency as well as those affected the fraudulent

action was transparent.

296 See https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/

decide-dsk

The termination of the proceedings was incomprehensible to us. Given the

In our view, the alleged extent of data misuse is more

Investigations and a punishment of the incident with proof of the fact urgently necessary

agile. This also serves to deter potential imitators. In a

We have asked the public prosecutor's office for further investigations.

praying and asking them to keep us informed of developments. This

Letter has remained unanswered to this day. Finally, we got it from the media

learned of the discontinuation of criminal proceedings by the public prosecutor's office.

If this decision remains and the proceedings are decided by the public prosecutor

society is not reinstated, we will request their files and the

Check the initiation of administrative offense proceedings on your own responsibility.

Sneaking up applicant data through fictitious job advertisements

is not a petty crime.

197

15 Telecommunications and

media

15.1 “We know what you said last summer

have read” – Third Party Content and Tracking

on websites

s

i

x

a

right

P

right

e

i.e

s

and

A

This year, too, the tracking of individual behavior in the

Internet "kept busy". In addition to the ongoing proceedings in

text of the tracking, we have dealt with new case law, new design

characteristics of consent banners, other detail issues and the

next attempt at a European ePrivacy regulation. Also

if we encounter increasingly cooperative responsible persons, the the-

matik a mixed situation that takes a lot of time to check.

For many years it has been a growing privacy issue

if third-party services297 as well as cookies or similar on websites

Tracking techniques are involved by means of which personal data

processed by website guests. In particular, the use of

nisms with which website guests and their preferences about the individual web

can be recognized beyond the law, leads in practice to the formation of

catchy behavioral profiles.

15.1.1 Permanent construction site tracking

With several publications, the conference of independent data

protection supervisory authorities of the federal and state governments (DSK) have already

297 Such content from third parties can be visible on the one hand, e.g. B. advertising banners,

Maps, videos or interaction elements from social networks. on the other hand

there are also invisible elements, like tiny little pictures, which exist only for

ren, data about website guests or the use of the website to the respective

forward third-party service.

about the tracking and those responsible about the legal

general conditions.298 Due to the complexity of the

matics and as a result of new case law on individual aspects, the requirements

ments to be evaluated on an ongoing basis. It is still z. B. failed, the

EU Directive on the Protection of Privacy in Electronic Communications

cation (better known as the ePrivacy Directive)299 by a European regulation

regulation, which is in contrast to a directive in every EU member state

would apply directly without transposition into national law being required

would be nice.

In addition to the requirements of the General Data Protection Regulation (GDPR)

therefore still the national standard required for a European directive

onal implementation of the ePrivacy Directive.300 In Germany, this

connection, in particular, the question of whether this is actually

in accordance with the Telemedia Act (TMG). After a referral

ment of the European Court of Justice (ECJ) in the “Planet49”301 case

now the Federal Court of Justice (BGH) on at least one paragraph of a para-

Counts of the TMG.302 The subject of the proceedings was a dispute in which the

sued companies personal data about usage behavior

from consumers via cookies to pseudonymised usage profiles

processed and used for personalized advertising. Unlike this before

was evaluated by the DSK,303 the BGH’s decision assumes that

that § 15 para. 3 sentence 1 TMG can be interpreted in accordance with European law.

According to the wording of Section 15 (3) sentence 1 TMG, data processing would then be

permissible if the data subjects have been informed accordingly and

298 Information from the DSK on Google Analytics, see 15.4; position determination and orientation

DSK classification aid for telemedia providers, see Annual Report 2018, March 12 and Annual Report 2019, March 13

299 Directive 2002/58/EG of the European Parliament and of the Council of 12. July 2002

on the processing of personal data and protection of privacy in

of electronic communication

300 primary type . 5 para. 3 of the ePrivacy Directive

301 See JB 2019, 13.2.

302 BGH, judgment of 28. May 2020 – I ZR 7/16

303 See Regulatory Guidance for Telemedia Providers, as of

March 2019, p. 2 ff.; available at https://www .datenschutz-berlin .de/ infothek-und-

service/publications/guidelines

have not objected (so-called objection solution). The BGH now takes

indicate that already in the absence of an effective consent such a contradiction

statement could be seen and therefore active consent is required

be. On the basis of this interpretation, he applies the TMG regulation alongside

of the GDPR. This interpretation of the TMG, which conforms to European law, is however

difficult to understand in terms of legal dogma.

The mere fact that the national data protection supervisory authorities and

the German civil court of the highest instance in a very practice-relevant

Legal question in the result agree that a processing, such as

it has been submitted to the courts for a decision, requires consent

the derivation of this result differing opinions

occur, illustrates the extent of the existing legal ambiguity.

Shortly after the decision, the draft bill for a "Ge-

law on data protection and protection of privacy in the electronic

communication and telemedia as well as to change the telecommunications

Onsgesetz, the Telemediengesetz and other laws" (TTDSG).

The planned law is primarily intended to implement the "EU Directive on

the European Electronic Communications Code"304 – here-

but the regulations of the TMG are also rewritten. There

the previous draft also behind an implementation that conforms to European law

of the ePrivacy Directive and the requirements for an adjustment to the GDPR

lags behind, the DSK made a clear appeal to the legislature in November

ber published, the ePrivacy Directive is finally complete and in line with

to implement the GDPR.305

304 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11. de

December 2018 on the European Electronic Communications Code

305 DSK resolution of 25 . November 2020: "Operators of websites need

gene legal certainty . Federal legislature must comply with European law obligations

finally comply with the ‘ePrivacy Directive’”; available at https://www .datenschutz-

berlin .de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

15.1.2 Mixed situation in the complaints and

test procedure

Not only since the GDPR came into effect in May 2018 have we received regular

Numerous complaints from website guests, their behavior without legal basis

analyzed and further processed for various advertising purposes. While

we were originally confronted with cases in which website ads

drivers have not even attempted to obtain consent for consent

catching up on needy processes is now often the effectiveness of a

consent obtained.

A self-determined and informed consent requires, among other things, that the

Website guests must first be explained clearly which ones

Data processing should be carried out by whom and for what purposes. Also

the data subject must have a real choice and may (compared to

mood) have no additional effort to refuse the consent. Should

a consent for various processing purposes or for disclosure

must also be obtained from various third parties

easy ways are provided to configure in detail,

which data processing you agree to and which not.

Against the background of the developments that are also very present in the media, we were able

this year both on the part of those responsible and on the part of

met at least some movement. Already the DSK publication

clarification of the orientation guide for providers of telemedia and the ECJ judgment

in the "Planet49" procedure in the last quarter of 2019 had led to di-

Various website operators have evaluated the tracking topic. One more

greater thrust of changes was made after the above BGH judgment visible as

on many websites suddenly larger and more differentiated cookies

banners have appeared. Conversely, an increased sensitivity

increase in website visitors, which is noticeably more

have submitted complaints and test suggestions on this topic to us.

The consent dialogues that have been found more frequently since then are certainly a progress

step. The purposes of data processing are now at least increasing

roughly explained and often also the integrated services of third-party providers

201

calls. However, if this involves an unmanageable number of so-called "part

ner" is, the website guests remain at a loss - especially since

It is always difficult to estimate what information about one's own

ultimately accumulated through observation and profiling. and

there are still consent dialogues with overflowing information that

often does not refer precisely to the relevant data processing processes

hen. The resulting lack of transparency is sometimes accompanied by a conscious

grueling design on sometimes several levels, with the website

guests sometimes have to put in considerably more effort if they do not carry

wish. It is not uncommon to have such user-unfriendly designs

the unfortunate result that the tracking is ultimately accepted.

Appeals to develop data-saving forms of advertising have so far mostly been the case

dies away because it is ultimately beneficial to those responsible, the users

explore as comprehensively as possible. Consequently, those responsible also use

every supposedly available gray area to protect their (financial) interests

follow. And there are many of these gray areas. Our tests show i.a.

also very unsatisfactory results because the website operators

who try with the well-chosen design of their user interfaces

Seduce website guests into quick approval. This is how the button

with which a comprehensive consent is given, gladly very clearly

lifted. The option to refuse consent, on the other hand, is visually

kept conspicuous to barely visible and/or ambiguous labeled (if these

possibility than is contained on the first level of the banner). So

the reflex that has been trained for years by PC and Internet users becomes a way

ck of disturbing messages to sneak into a just uninformed

consent used. The limits of the legal admissibility of such methods

the courts will ultimately have to weigh this up.

Even in the case of obvious defects, the tests we have initiated prove

unfortunately often take a long time because we don't limit ourselves to just that

(can) view the design of the cookie banners, because this is only the tip of

is an iceberg. Even if complainants only have a lack of selection

possibility in the banner or the use of individual tracking programs,

Are there multi-layered chains of processing processes in the background,

which are to be clarified by us. Identify and evaluate these issues

is, on the one hand, enormously complex from a legal and technical point of view, since an almost

unmanageable number of third-party providers with the website and each other

which is linked. On the other hand, the processes on the websites are also changing

regularly in actual terms, e.g. B. Banner visually changed, the

integrated techniques added or removed and information rewritten

be practiced Each of these must be documented and analyzed in detail, moreover

those responsible for this must be consulted.

With the DS-GVO and some groundbreaking judgments, the

It is becoming increasingly clear to the users of web offers that it is no longer possible to access

time to play. The supervisory authorities can now with more legal certainty

take action against those responsible who continue to monitor the behavior of the website

track searchers online without prior informed consent

to catch up We also face this very labour-intensive task in order to

to ensure more equal treatment on the Internet. Due to legal and technical

However, due to the considerable hurdles, this is a long process.

15.2 Facebook Fan Pages

Caused by several court decisions of the ECJ and the Federal

of the administrative court (BVerwG) in the context of Facebook services and to

At the end of 2018, we had a number of shared responsibility306 issues

investigation procedures initiated.307 In the course of these procedures, Facebook

substantially revised version of its agreement on joint responsibility

provided verbatim with the fan page operators.308 Since these do not

was suitable for clearing up all previous points of criticism and open questions,

we have again asked several responsible persons for their opinion. the

Reactions were mixed.

A

and

s

i.e

e

right

P

right

a

x

i

s

306 ECJ, judgment of 5 . June 2018 − C-210/16; BVerwG, judgment of 11. September 2019 −

6 C 15 18 (Schleswig-Holstein Business Academy); ECJ, judgment of 29. July 2019 −

C-40/17 (Fashion ID)

307 JB 2018, 1.7

308 See https://de-de.facebook.com/legal/terms/page_controller_addendum

Facebook provides the operators of fan pages with so-called page insights.

This is statistical information about whether and how visitors

chers of the fan pages have interacted with the page and the content - what

So it goes down well with certain groups and what less. As the ECJ 2018

has determined, Facebook and the operators of the fan pages process here

for the personal data of the visitors in joint responsibility

wordiness. As a consequence, both actors are not only obliged to

of an agreement to transparently define who has which data with regard to this

Obligations according to the GDPR fulfilled. It is also everyone who

responsibility for the legality of the data processing

and, if necessary, to the responsible supervisory

authority to prove.

After Facebook sent the fan page operators a contract for the first time at the end of 2018

Agreement on the distribution of responsibilities for the page insights available

ment, a significantly revised version followed at the end of October 2019
Version of this Agreement (the so-called Page Insights Supplement). the
new agreement has some of the previously expressed by the regulators
ten points of criticism. As we already did in our last
have indicated, the supplement remains in decisive points
insufficient.309 Ultimately, the fan page operators become more and more
not yet sufficiently empowered to exercise their accountability
with regard to the legality of the processing of data from fan page visitors
to comply with chers.
In February we therefore again have six positions in the state administration, six
political parties and seven Berlin companies and organizations, e.g.
from the retail, publishing and financial sectors. While we have
on the one hand, concerns or doubts regarding certain components of the
ten-Insights-Supplement and suggested that we critically comment on the points in question
to clarify Facebook. On the other hand, we have the concrete implementation of information
tion obligations are reminded on the respective fan pages.
309 JB 2019, 13.6

After already in the first round of hearings, several of the political parties
has not provided any information with reference to our alleged incompetence-
ten, it was unfortunate but not surprising that even in this round only
one of them commented on our further questions. Others too
Although non-public bodies have expressed doubts about our jurisdiction,
however, they all reacted constructively and got involved in terms of content. So far
allowed the user interface on Facebook, several places have the opportunity

used to make their fan pages more transparent, e.g. B. Information

functions for data processing were made available with less effort.

Almost all those responsible have also contacted Facebook.

Among other things, this has led to Facebook including a passage in its information

corrected to the Page Insights data.310 It originally said that “You […]

always have the right to lodge a complaint with the Irish Data Protection Commission

(see www.dataprotection.ie) or contact your local supervisory authority

sufficient.” Since data subjects have the right to complain to any

to complain to any regulator (i.e. not just the Irish and the

own member state), this information had to be adjusted. To our rest

Hardly any concerns were raised about this, so we continued the procedures

still unable to complete.

The Senate Chancellery, which represents most of the public

some places, first contacted us with questions.

Our offer of a personal consultation, which we share with our

have sent replies have unfortunately not been accepted so far.

To a certain extent, the progress of our test series has led to a

Increased awareness of the problem among those responsible. It ste-

However, there are still unresolved points in the room, so that the procedures

be continued by us until the legal operation of the Facebook fan pages

is secured or their operation is discontinued.

310 See https://www.facebook.com/legal/terms/information_about_page_insights_data

15.3 Guidance: How safe can and

does email have to be today?

s

i

x

a

right

P

right

e

i.e

s

and

A

The Berlin Commissioner for Data Protection and Freedom of Information was responsible

rend involved in the development of an orientation guide, the requirements for the

Use of e-mails for the transmission and receipt of personal

contains data.311

E-mails are still an indispensable tool for exchange

of information between people and institutions. The advantage lies in the

Universality: Almost every institution can be addressed by e-mail and

The vast majority of private individuals can also be reached by e-mail.

The users can use a wide variety of programs for reading and writing

send the messages. The real work happens in the background.

Servers receive the messages and forward them - possibly via

several intermediate stations – on to the recipient.

Personal data are also prior to transmission by e-mail

protect against unauthorized access or manipulation.

Several methods have been established for this over time.

The so-called trans-

port encryption. Build the already mentioned servers and intermediate stations

a secure channel for data transmission. Are there safe

used312 and it is checked that the opposite side is ready to receive

right and is in fact who she claims to be, then the trust

transmission guaranteed. At the intermediate stations, however, lie

the news open.

311 Orientation guide of the working group "Technical and organizational data protection

ask": Measures to protect personal data during transmission

by e-mail, status: 13 . March 2020; available at https://www .datenschutz-berlin .de/

infothek-and-service/publications/orientation aids

312 The Federal Office for Information Security has issued a corresponding

corresponding catalog published.

The so-called end-to-end

de-encryption. Here the encryption and decryption takes place directly at the

respective persons responsible or the persons involved in the exchange. In

This usually happens in the programs that the users use to send

and receive the messages. Either these already contain

the corresponding functionality or suitable extensions for

used the programs. However, controllers can also be centrally operated

Use information technology to encrypt and decrypt as well as

issue and check signatures. These signatures are for that

Protecting the integrity313 of message content.

For non-technical private individuals, however, the use of a

of the two available end-to-end encryption techniques

subject. Because every encryption and every signature includes cryptographic

cal key. You have to generate and manage your own keys, external ones

Keys must be accepted and checked. by those responsible,

in particular those who handle sensitive data must be required to

they make this effort. By individuals who are not responsible

are within the meaning of the GDPR, this cannot be expected.

In order to make it easier for those responsible to decide which security

measures to protect e-mail messages in their responsibility

are rich to meet, the DSK has, under our leadership, an orientation

help written.

The orientation guide clarifies the duty of care when using

E-mail service providers and the policies they must comply with. She lays

set out the requirements for those responsible for the safe receipt of

Email messages need to create targeted personal information via

to receive email. Because the security of the transmission depends

from both the sending and the receiving person or body,

313 Maintaining the integrity of data means protecting it from unauthorized access

alteration or removal, accidental loss or destruction and against

accidental adulteration; see type . 5 para. 1 letter f GDPR.

even if the responsibility for the individual transmission rests with the sender

person or place lies.

Those responsible for sending e-mails or the e-mail service providers responsible for them

act, must carry out a transport encryption. It is important

knowing that popular software regularly uses an unencrypted connection

established if no encrypted connection is established. That's at the

Transmission of personal data in the content of an e-mail message

allowed. On the other hand, the guidance also states that the

Transport encryption is sufficient with normal data protection requirements and

end-to-end encryption is not generally required.

In the case of high risks, the transport encryption must meet special requirements

suffice, which are described in the orientation guide. Basically is

end-to-end encryption is also required. From the

status of the individual case, in particular of the existing risks, the specific

th design of the transmission path and, if necessary, made compensating

It depends on the measures to what extent these requirements are deviated from

may.

Are the communication contents subject to special confidentiality regulations

ten, these must also be observed when sending e-mail messages

will. In particular, the sending person must ensure that only

Allowed recipients to take note of the content. This usually

moderate end-to-end encryption.

The orientation aid follows with more detailed explanations of the requirements

the individual procedures.

Beyond the requirements of the orientation guide, we advise those responsible who

communicate directly with their customers and thereby transmit sensitive content

to forego e-mail as a transmission path and to use alternative methods – the

Providing information via a secure web portal for example – too

Select.

Responsible persons must also send and receive e-mail messages

to maintain the security of personal data. the orientation

With the help of the DSK, the applicable requirements are compiled.

15.4 Notes on the use of Google Analytics

adopted

In addition to the orientation guide for providers adopted in 2019

of telemedia, the conference of independent data protection supervisory

authorities of the federal and state governments (DSK) in May information on the use of Google

gle Analytics published on the websites of private providers.314 As a result

earlier information from the Hamburg Commissioner for Data Protection

wraps. This was necessary because both the product and the legal

che frames have changed in the meantime. In this respect, a clarification

development takes place.

A

and

s

i.e

e

right

P

right

a

x

i

s

Google Analytics is a widely used tool for website operators.

With the help of this tool, comprehensive statistical evaluations of the

make use of the website. For this purpose, the user behavior is first

recorded by individual users. The individual recordings then become

calculates statistical data that is available to the website operator

be asked.

In addition to these statistical evaluations for the website operator or the

However, website operators reserve the right to use Google in their terms of use

also provides information collected by the tool about usage

consider individuals to also process it for their own purposes.315 Google is

therefore not exclusively on behalf of the website operator

active. Taking into account the current case law of the ECJ

Website operators who use Google Analytics together

314 See https://www .datenschutz-berlin .de/infothek-und-service/veroeffentlichungen/

decide-dsk

315 https://marketingplatform.google.com/about/analytics/terms/de/; Retrieved on

4 . December 2020, no. 6 .

responsible with Google for the associated data processing. About the

Details of joint responsibility is a separate agreement

to close.316

The processing of personal data via the statistical evaluation

genes for website operators, it makes it necessary for users

give their consent before information about their usage behavior is provided by Google

Analytics are collected and processed. Every website must give this consent

ten operator and every website operator who uses Google Analytics,

obtained from every visitor to the website. had on it

together with other German supervisory authorities on November 14

pointed out in a press release in 2019.317 The now adopted

The paper also contains some guidance on how to design an effective

legal consent.

As long as Google reserves the right to personal data from the use of

To process Google Analytics for their own purposes, website operators must

Obtain the consent of the users for this.

15.5 Publication of Postal Addresses and

phone numbers on the internet

s

i

x

a

right

P

right

e

i.e

s

and

A

A company published postal addresses and telephone numbers on the Internet

of private individuals from different countries on several country-specific

cific websites. For some of these deals was considered the company's headquarters

given a postal address in Berlin. Our office then reached

numerous complaints from data subjects from different countries

rapas.

The complainants complained that their personal data was stored there

had been published without their consent and that they too

316 art. 26 GDPR

317 See https://www .datenschutz-berlin .de/infothek-und-service/pressemitteilungen

not (or at least no longer) in other telecommunications directories

sen of their home countries were registered.

Our investigations revealed that the company at the address given in the imprint

given address had no branch. There was only through

an office service received mail for the company and to its

actual seat in Toronto (Canada).

We then contacted the local regulatory authority in Canada for the

Privacy - Office of the Privacy Commissioner of Canada (OPC) -

tet. The OPC was already conducting an investigation into the practices at this point

of the company according to the local data protection law due to complaints

those of data subjects who had contacted them directly.

According to German and European telecommunications law, the

Affected persons decide for themselves whether and to what extent their

Address data and/or telephone numbers in participant directories

become public. A publication of this data by third parties without consent

The agreement of the persons concerned comes according to the provisions of the GDPR

at best and only to the extent that this data already exists

are lawfully publicly available elsewhere.

The Canadian Data Protection Authority has offered us, regardless of the ones there

ongoing investigations, a deletion of individual data records of affected persons

obtain from the company if they are not (or no longer) in

Telephone directories of other providers are listed. We have affected

persons for their consent to the transmission of their data to the

nadian data protection authority and the data of those complaint

transmitted there to guides who have given this consent. The data

of these persons concerned were then removed from the company's offer

mens removed.

After completing the investigation there, the OPC informed us that

that it instructed the company to also include the data of other affected persons

Persons who were also not published in other telephone directories

ren, from his offers and, where this was not possible, the data

211

remove inventory for the entire country. The company then

removed some of its country-specific websites from the Internet. These included

also the offers for the countries of origin of those persons concerned who

complained to us.

A publication of address data and/or telephone numbers in

directories may only be made with the consent of the person concerned

take place. An exception may be considered if this data

are already legally accessible to the public elsewhere. Enforcement

the rights of data subjects - such as their right to erasure in accordance with this

Art. 17 DS-GVO - towards persons responsible based outside the European

nical Union is made much easier if in the respective country of domicile

There is a comparable legal framework and a supervisory authority that enforces it

can be enforced directly on site.

15.6 Exemption from the license fee also with

blackened modesty

s

i

x

a

right

P

right

e

i.e

s

and

A

Recipients of social benefits can under certain

be exempted from paying the license fee under the following conditions. she

must go to the "ARD ZDF Deutschlandradio Contribution Service" ("Central Contribution

tragsservice" - ZBS) to prove receipt of the social benefit. an affected one

person had a partially redacted copy of the notice from the social

service provider sent there. However, the ZBS insisted on the approval

of the exemption on sending an unredacted copy of the decision.

We have the responsible broadcaster Berlin-Brandenburg (rbb) for that

Facts asked for comment. As a result, the official

Data protection officer of the rbb a reassessment of the application of those concerned

person through the ZBS. After re-examination, the latter submitted the application

based on the complaint originally sent by the complainant

pie, since the information relevant to the exemption is also on this

blackened copy of the notification.

212

In addition, the ZBS has published information on its website

which shows which information can be derived from the evidence for the exemption

ung from the broadcasting fee, e.g. B. Certificates from authorities or permits

payment notices must be issued. These are the names of the service recipients

or the recipient of the service, information on which service is granted,

and the period of performance.318

Even when sending proof of receipt of social benefits

for exemption from the broadcasting license fee is the extent of the data collected

ten to those data that are necessary for the decision on the

exemptions are required. Additional data can be

affected persons are blacked out.

15.7 Deletion of personal data in Individual documents at Rundfunk Berlin–Brandenburg

Unsolicited, a person concerned sent the Rundfunk Berlin-Brandenburg

denburg (rbb) together with a request for information a copy of their personal

identification card with the note that rbb should send this copy after identification

delete the quality check immediately. As part of the provision of information to the

affected person turned out, however, that the ID copy together

with the application for information from the Central Contribution Service (ZBS)

had been stored. The rbb rejected a request for their deletion

towards the person concerned.

A

and

s

i.e

e

right

P

right

a

x

i

s

In its statement, the rbb initially also opposed our authority

about a deletion of the copy of the identity card, because the storage

tion deadlines and also a deletion of individual pages

technically not possible with the transaction management system without the entire

incoming document (the request for information) and the outgoing document (the

318 See https://www .rundfunkbeitrag.de/buergerinnen_und_buerger/information/

recipient_of_social-benefits/index_ger .html

letter of future) to delete. Incidentally, this is disproportionate

effort involved.

Already the permanent storage of the ID card copy via the identity

However, beyond the scope of the audit, it was unlawful. For that reason alone, the rbb would be from

and even more so upon the request of the data subject for deletion

obliged to provide a copy of the identity card.319 A right to deletion

In the present case, it also resulted from the fact that further storage of the

ID card copy no longer required after completion of identity check

320 The copy of the identity card sent by the person concerned

is not subject to any statutory retention periods.

Also the objection of the rbb, a deletion of individual parts of a

scanned document is not technically possible, does not release him from the obligation

Legal obligation to delete: Rather, rbb is obliged to

to create the technical and organizational prerequisites for

comply with legal obligations to delete personal data

to be able to.321

We have informed rbb of our data protection assessment. This

has then developed a process with which individual pages can also be

scanned documents can be deleted from the database there.

The deletion of the ID card copy was - as originally requested -

implemented and confirmed to the person concerned.

Requests for information about personal data according to Art. 15 DS-GVO should

ten in principle without presenting a copy of the identity card

since ID card copies are not regularly required. a compulsory

ment to delete data can also apply to individual parts of stored information.

documents exist. Those responsible are obliged to meet the technical requirements

to create conditions to ensure that they comply with their legal obligations

Deletion of this data can comply. This doesn't just apply to the ones here in

319 See Art . 17 para. 1 letter d GDPR

320 See Art . 17 para. 1 letter a GDPR

321 See Art . 24 para. 1 GDPR

Deletion in question in individual cases, but also for a regular

tomatic deletion after expiry of retention periods. shortcomings of

set software cannot justify "data cemeteries".

215

16 political parties and

company

16.1 Information about evaluation sheets for

scholarship applicants

s

i

x

a

right

P

right

e

i.e

s

and

A

The scope of information about personal data that a responsible

authority must issue upon request is regularly the subject of complaints

the and decisions. In the specific case, the complainant had

an organization for the promotion of gifted people, one financed from public funds

scholarship applied for. In the course of the selection process, an evaluation

drawn up in which the various competencies of the complainant

were evaluated. This arc provided the basis for the decision on the

acceptance of the complainant into the study grant. After completion

of the selection process, the applicant asked the agency responsible for the promotion

Information about the data stored there about him, in particular about a

Copy of the evaluation form. The carrier refused to disclose the

evaluation sheet and referred to the copyright of the members of the evaluation

electoral commission and protection of trade secrets.

The right to information basically includes all personal data that

the responsible body has stored for the person concerned.322

Personal data are not just objective information such as name, address

resse, age, etc., but all information about a person. These include

also subjective and/or objective assessments. Also references, appraisals

Gen or opinions about people contain personal data about which

a responsible body must provide information.

The right to obtain a copy of such documents is limited only to the extent

thereby disclosing information which in turn is legally special

are protected from disclosure, e.g. B. Trade secrets or information

322 Art. 15 para. 1 GDPR

about third parties. In this case, the interest in information of the affected

be weighed against the respective interest in secrecy.

But even if the interest in secrecy prevails in the specific case, may

the responsible body does not refuse the release of the copy across the board,

but may have to redact the relevant passages.

The responsible body has asserted here that the evaluation form

The underlying form contains protected business secrets. sex

According to the Business Secrets Act (GeschGehG), business secrets are

generally protected from disclosure. However, this presupposes, among other things, that

this is information that is neither generally known nor unknown

Other are accessible and additionally of economic value. This could

However, we do not determine this with the form used.

In addition, the responsible body has asserted that through the

Information on the copyright of the people who created the evaluation sheet

ben, would be hurt. Here, however, the weighing of rights showed that the origin

Berrecht, if it should exist at all, at most minimally affected

would. Because the evaluation sheet should only be given to the person concerned

and not published or even commercially exploited. In

In this case, the interest in information of the person concerned outweighs a possible

possibly existing copyright of the members of the selection committee.

The funding agency has now provided the requested information.

Evaluations and assessments of applicants for the purpose of

Selection procedures are created, represent personal data. About

it is to be provided upon request by the data subject. This information can

only be restricted if information is thereby disclosed,

which in turn are protected by law from disclosure.

217

16.2 Talent promotion only with sensitive

Declarations?

s

i

x

a

right

P

right

e

i.e

s

and

A

In one case we had to decide what information the carrier

of a scholarship program from applicants.

The provider used an online form that applicants could use to

had to register. Among other things, they had to provide information about their religion

and make it their origin. Religious affiliation was for selection

according to the sponsor, however, is not an acceptance criterion.

Information about ethnic origin as well as about religious beliefs

In addition to some other data categories in the DS-GVO, testimonials are

ders protected.323 In connection with their processing, significant

Risks to the fundamental rights and freedoms of data subjects (e.g.

discrimination) occur. Therefore, they may only be used under strict conditions

gene to be processed.324

These conditions are z. B. if the person concerned in the process

processing of this information consented, d. H. has voluntarily consented to it.325

Such consent is only voluntary if the data subject

is sufficiently informed about how this data is further processed. Except-

which it must have the opportunity to object to the processing without doing so

suffer disadvantages. When filling out the online form, the applicant must

Berlin or the applicant can decide for themselves whether they want to provide information

want to do these sensitive topics or not. This possibility was in

present case not given. There was therefore no effective consent in the

within the meaning of the GDPR.

Even if the data subject does not consent, the GDPR allows in some cases

cases the processing of sensitive data. In our case, only the following

gender permission plays a role: Sensitive data may be processed by a political,

323 See Art . 9 GDPR

324 See Art . 9 para. 1 to 3 GDPR

325 Art. 9 para. 2 letters a i . v. m . kind . 4 no. 11, art. 7 GDPR

ideological, religious or trade union oriented foundation, association

agreement or other non-profit organization within the framework of lawful

internal activities, such as membership administration including

acceptance of new members.326 The sponsor has argued that

he works on the basis of an ideological-religious worldview and

therefore, to the extent necessary for this, also information on the religion of his

members may process.

With regard to data on ethnic origin, this justification applied from the outset.

one didn't, because ethnically the wearer had no specific orientation

tion. The obligation to provide this information was therefore inadmissible.

Also with regard to religious affiliation, the survey was at the time

the first registration is not required in the present case. Because the carrier

had made it clear that a specific (formal) religious affiliation

is not a prerequisite for acceptance into the scholarship program. Much more

according to the carrier, it will be discussed in the subsequent interview whether

the applicant to the image of man represented by the institution

close. It is sufficient for this if the applicants in their personal

be asked about their views during the interview. In particular the processing

of this sensitive information from all applicants who are not personally

Being invited to a private conversation is therefore not necessary and contradicts

the principle of data minimization.

The result was the collection of mandatory information on both religion

and ethnic origin in the online mask is unlawful. We have

warned the wearer. He then announced that he would close his online for-

mular will adjust accordingly.

When designing online forms (e.g. for application processes)

those responsible must ensure that they only

obligatory query, for the respective purpose and at the respective time

326 Art. 9 para. 2 letters d GDPR

of the procedure are required. This applies all the more, the more sensitive the information

are. In addition, those affected can provide information voluntarily.

However, such fields must be marked accordingly.

220

Chapter 16 Political parties and society 17 .1 Berlin Data Protection Amendment Act EU passed

17 Europe

17.1 Berlin Data Protection Amendment Act EU

passed – deficits in the area

of the data protection supervisory authority continue to exist

More than two years after the end of the implementation period, the law on the

Adaptation of data protection regulations in Berlin laws to the

General Data Protection Regulation (Berlin Data Protection Amendment Act EU)

passed by the House of Representatives.327 As in our

resbericht 2019 reports, this is a mammoth project through which

approx. 80 Berlin laws to the European data protection basic regulation (DS-

GMO) have been adjusted.328

A

and

s

i.e

e

right

P

right

a

x

i

s

We closely followed the legislative project. Ironically with that

most important data protection regulations, the Berlin Data Protection Act

(BlnDSG), there are still significant shortcomings. This is especially true

in the field of data protection supervision and control.

Control deficits continue to exist, among other things, in the important area of

public rights. The right to information about the stored personal data

Data is a fundamental principle of the GDPR. Should the information in individual cases
may be refused, citizens should in principle be required
that corresponding information can be provided at least to the responsible
be granted by the data protection authority. Through this substitute information
the supervisory authority and the resulting control should be ensured
that the processing of the data in question takes place in accordance with data protection.
Even this alternative information can, however, continue after the now
applicable statutory Berlin regulation denied by the authority concerned
if it believes that doing so will jeopardize federal security
or a country would be endangered. Such a restriction of those affected

327 See GVBl. 2020, p. 807 ff.

328 JB 2019, 14.1

rights is not comprehensible, since the data protection authority is a
independent, supreme state authority, whose employees are subject to strict
confidentiality of the information that has become known to them in the service
are Not only is this regulation an important control function of the
Berlin data protection supervision overturned. This regulation can lead to cases
in which citizens exercise their most important right, namely the right to
information, is entirely discussed. This restriction of a fundamental right
is highly questionable in terms of the rule of law and especially against the background of
Strengthening of the rights of those affected by the GDPR can hardly be justified.
A well-known control deficit in the portfolio of the House of Representatives
was even tightened with the new BlnDSG. Because although the data
protection regulations for the Berlin Parliament are still unclear,
The law that has now been passed further expands the possibilities, including sensitive ones

to transmit personal data to the House of Representatives. After
recent case law of the European Court of Justice on reach
the validity of the GDPR for the work of the Petitions Committee of the Hessian
In Germany, the Landtag329 decides on the direct application of the GDPR for
the parliaments discussed. However, even if one assumes that the
lament is not directly subject to the regulations of the DS-GVO, the
such personal data of effective and reliable protective measures
and control mechanisms based on comprehensible regulations. This
was last in connection with the project initiated by the AfD parliamentary group
"Neutral school" clearly, which showed that legislative bodies quite
process sensitive personal data. Affected citizens stand
against such initiatives in Berlin so far without any possibility of control. The-
This condition must be remedied urgently. Even in Parliament, one of the
DS-GVO corresponding level of data protection can be ensured.
The expert committee promised that as part of an evaluation specifically
of this law in this electoral period on points that we have criticized
should be spoken once.

329 See ECJ, judgment of 9 . July 2020 - C-272/19

In the area of the police and judiciary, data protection supervision is also lacking
effective enforcement powers as before. The Berlin Commissioner for Data
Data Protection and Freedom of Information (BlnBDI) can be used against police and judicial
authorities continue to make no binding orders, but - how
before the new European regulations came into force – violations detected
objection only without obligation, which corresponds to the clear wording of this

chen regulations. This deficit is very serious because the police and
Judicial authorities often process particularly sensitive data about citizens,
such as data from witnesses in criminal investigations.
In all other areas of public administration, the Berliner Daten-
safety supervisors may issue formal orders. Here, however, the da-
associated enforcement options. Without the possibility of fines
to determine or to arrange for a substitute performance, such orders can
measures - for example to delete illegally stored data - ultimately not
be enforced. Effective data protection supervision is
not guaranteed by throughout the public administration. Come in addition,
that the data protection authority does not issue any fines against authorities or other
term public bodies can impose. In particular, these other public
institutions, such as hospitals or in-house operations or under private law
ized companies that perform public administration tasks and themselves
are mostly in state hands, are thus in no justifiable way
privileged compared to purely private positions with comparable tasks.
The adaptation of the Berlin laws, which was carried out in a hasty procedure
to the GDPR has left some gaps, some of which are very sensitive.
senior Fortunately, the deputies of the data protection
expert committee announced that the Berlin Data Protection Act would
gig of the Amendment Act to be evaluated in this legislative period.
We hope that the announcement made true and the existing shortcomings
be eliminated.

17.2 From the service center for European affairs
units – number of cases, trends, focal points

s

i

x

a

right

P

right

e

i.e

s

and

A

The GDPR provides for close cooperation between the European data

protection supervisory authorities. It is primarily about cases that have a borderline

involve excessive processing of personal data. The BlnBDI

processes cases as the lead authority if the data-processing entity

company has its headquarters in Berlin and transmits the ones it receives

Cases to other lead supervisory authorities, provided that the headquarters of the company

company is located in another member state. The

internal service center for European affairs as a hinge between the eu

European data protection supervisory authorities and the specialists at the

BlnBDI.

Both all complaints that we receive and all cases that we receive from

take up official action, as well as the data breaches reported by companies

are first checked by us to determine whether the processing

processing of personal data takes place across borders. This is above all

This is the case if the responsible person is in more than one member state
is established in the EU and the processing is carried out in several of these establishments
done. However, even then, cross-border processing
tion exist if the processing is only carried out in a member state of the EU
takes place, but they have a significant impact on data subjects in more than
has or may have in a member state.
In the past year, in particular, were procedures for determining the spring
leading supervisory authority is a focus of the work of the Euro-
couple matters, in 2020 we were able to use this as a basis to
complaints to the European supervisory authorities, which have now been found to be responsible
transmit them or process them yourself as the lead authority. So we have to
a large number of the
needy cases. On the one hand, this happened because we
submit their own investigation results to a vote in draft resolutions
and were able to conclude them with final resolutions. To the
others we have against the draft resolutions and thus against the

objections to the results of other supervisory authorities, if necessary, and
In this way, aspects of content are introduced into the process, which in part
in the revised draft decisions and in the final decisions
were taken into account.

17.2.1 Determination of the lead supervisory authority

If cross-border processing is suspected, then the case will be den
other European data protection supervisory authorities via the digital internal

market information system (IMI). As part of the cooperation

a lead supervisory authority will be appointed to carry out the investigations in

the respective case. Other data protection supervisory authorities may act as

so-called affected authorities if they assume, for example, that the

work has a significant impact on data subjects in their country.

Around 741 methods for determining the spring-

reported to leading and concerned regulatory authorities. All procedures

were checked in the Service Center for European Affairs for a possible

checked by the BlnBDI. In 388 procedures, so a little more

than half of the procedures, it was determined that our authority was affected

so that we have to deal with the content of the respective facts-

ten. Such concern is given quickly: Set up an online shop, for example

its offer to German customers too, then we have to assume that

that citizens in Berlin can also be affected by the situation, so

that we get involved in the case.

This year, the BlnBDI opened 29 new cases in which they acted as lead

supervisory authority is active. Of these, ten cases are from other European

submitted to supervisory authorities.

225

Cross-border cases

With the participation of the BlnBDI

500

400

300

200

100

0

528

388

140

Affected Authority

reported by BIn

reported by other MS

29

10

19

lead authority

Figure 1: Cases checked by the BInBDI in the reporting period that were posted in IMI.

Not in all cases is the determination of the lead supervisory

hear smoothly. So we did after relocating the main office

of a person responsible in another EU member state together with the

insofar competent other European supervisory authority an on-site inspection

carried out in both member states. In this case, currently still

determines whether the decisions regarding the purposes and means of the processing

processing actually in a European branch or in a third country

to be hit. If these decisions are not made in a main office

be made and implemented in the European Economic Area (EEA),

the privilege of the one-stop shop would not be applicable. Consequently there would be none

Lead supervisory authority, which is the only contact person for the

Responsible would be responsible.330 Instead, there would then be responsibility for

the company with each European supervisory authority with appropriate

given cases.

330 See Art . 56 para. 6 GDPR

17.2.2 Transmission of cases and resolution

design

As already mentioned, the number of procedures for determining the lead

the and affected supervisory authorities slightly declining, since the responsibility

has now been established for many large companies. Instead, in the

Cases where we are not lead authority, many complaints directly

translated into English and then expeditiously to the lead regulator

be sent for further processing. This has

also have the positive effect that the processing time of their

ben shortened. The Service Center for European Affairs has a total of 140 cases

transmitted to other supervisory authorities. Even in these cases, however, we remain

contact person for the complainants and inform them regularly

moderately above the status of processing.

When a lead regulator completes its investigations

it shall submit a draft decision to the supervisory authorities concerned for filing

mood in IMI. Since in the second year after the GDPR came into effect

more and more cases are being closed by measures to end proceedings

the number of draft resolutions increased significantly in the reporting period

gen. This is particularly remarkable against the background of the corona pandemic,

since in many member states these lead to sometimes significant restrictions on the

has conducted administrative activities.

The Service Center for European Affairs examines all draft decisions on cases

where the BlnBDI has reported as the supervisory authority concerned. The KO-

Operational procedures of the DS-GVO provide that the supervisory authorities concerned

can object to draft resolutions if they

disagree with them. The BlnBDI has already been involved in several cases

made use of this option and raised objections to resolutions

charges filed by other regulators. As a result of such an objection

the lead authority must review the draft decision, e.g. with regard to

an incorrect interpretation of the facts, a lack of action according to the

determination of a data protection violation or an incorrect procedural

che adjustment of the procedure.

227

Total resolutions since the introduction of the GDPR

102

64

38

46

26

20

German-

country

Frank-

rich

42

32

10

GB

41

33

8th

37

23

14

Spain Lower

land

Final Decision

draft decision

52

30

22

14

8th

6

8th

6

2

7

5

Berlin Hesse NRW

6

5

2

1

Hamburg

Bathe-

Wuerttemberg

Figure 2: Total number of all draft resolutions and final resolutions of the five sessions

authorities in EEA member states or federal states with the most decisions since

Introduction of the GDPR

In the cases that concern us, we are often in contact with the respective European

partner authorities entered into a direct exchange in order to

decision-making process supported by authorities. In this context

sometimes different legal opinions meet, which are often

the different legal traditions are justified and then in terms of one

Compromise solution should be balanced if possible - this is how the alignment works

of the different legal systems in the field of data protection in professional

everyday life ahead of you. Based on the objections to draft resolutions, in the course

the revision of these draft resolutions and through the interpretation and

Application of the GDPR in the specific case shows the joint work of everyone

European supervisory authorities as a constructive struggle to standardize

update of the level of data protection in the EU.

Do all supervisory authorities concerned agree to a revised resolution

draft, the lead supervisory authority can issue a final

publish the final draft, the result of which is also communicated to the complainant

and communicated to those responsible.

Overall, the work of the Service Center for European Affairs has

questions of permanence more on the coordination of content during processing

of complaints and the determination of measures with regard to the

relocated data protection violations. We have objections in several cases

filed, in which the lead supervisory authority, despite established

not take remedial action against the person responsible for data protection violations

wanted to. Because according to the rules of the GDPR, in the event of data

effective measures are taken to prevent breaches of protection. A non-action sees

the GDPR does not exist. This is sometimes difficult for supervisory authorities to accept.

whose national data protection or procedural law is increasingly based on negotiated

development-oriented solutions.

Insofar as we acted as the lead authority, we have draft resolutions

published, against which the other European supervisory

authorities could appeal. Overall, our authority published

this year 24 draft decisions and 20 final decisions.

17.3 Data protection through technology design –

New guidelines of the European

Data Protection Board

The DS-GVO has the regulations of the so-called "privacy by design" and "privacy

by default" the demand for data protection through technology design and that

Principle of data protection-friendly default settings anchored in the law. We have-

to the guidelines of the European Data Protection Board (EDPB)

acts, with which the legal requirements are explained.

A

and

s

i.e

e

right

P

right

a

x

i

s

The GDPR stipulates that technology design should ensure that

that the data protection principles are observed. These principles

ck on the lawfulness and transparency of processing, their binding

to the purpose for which the data was collected, minimizing the scope

processed data and the time limit for their storage as well as the

229

ensuring the accuracy, confidentiality and integrity331 of the data. The A-

It must be possible to demonstrate compliance with the principles.

The technical and organizational measures taken by those responsible

meet should be appropriate and effective. Those responsible should and

A number of factors can be considered when selecting the measures

draw. Among them are the state of the art, i.e. the most effective on the

Market available technologies that pose risks to data subjects who are using

associated with the processing, but also the implementation costs and whole

general type, scope, circumstances and purposes of processing. With all that is

However, effectiveness is the key criterion, since only effective measures can

The rights and freedoms of the data subjects are protected.

As early as 2019, the EDPB had guidelines to explain the legal requirements

ments to data protection through technology design and data protection-friendly

attitudes formulated and the public to comment on the paper

called. As a result, more than fifty comments from business and

civil society submitted. This year, the guidelines were based

of the comments substantially revised. We participated in it.332

The guidelines explain each of the data protection principles listed above and

each lead key elements of its implementation through technology design

on. Examples will elucidate the application of these elements in a specific context.

Preferences are used to configure applications, programs, and devices.

The guidelines make it clear that these should be chosen in such a way that only the

required personal data are processed. These may only

processed as little as possible, only stored as short as possible

secure and accessible at all times to as few people as possible

be lich.

331 Maintaining the integrity of data means protecting it from unauthorized access

alteration or removal, accidental loss or destruction and against

accidental adulteration; see type . 5 para. 1 letter f GDPR.

332 See https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-

42019-article-25-data-protection-design-and_en (English version)

The guidelines emphasize that data protection by design is a continuous

eral task of those responsible, which already starts with the planning of the

data processing begins. Technological advances can both

additional risks, as well as opening up new opportunities, known risks

ken to mitigate more successfully. You are therefore involved in updating the measures

men to consider.

The requirements are aimed at those responsible. These are for it at the same time

responsible that the processing steps that are carried out by order processing

ter and subcontractors are carried out, the requirements

correspond to.

With the guidelines on data protection through technology design and data protection

friendly default settings, the EDPB gives those responsible important ones

Information on safeguarding the rights of data subjects. Also order

Processors and manufacturers are called upon to adhere to the guideline

orientated, since those responsible only use services and products

may take, which are operated in accordance with the law.

17.4 Other important guidelines of the European

Data Protection Board

The European Data Protection Board (EDPB) consists of the data protection

supervisory authorities of the individual EU member states. Also the Bln

BDI has the task of making contributions to the activities of the EDPB and works to

at closely with the other German data protection supervisory authorities.333

The aim of the EDPB's work is to ensure the uniform application of the GDPR in the EU

ensure. To this end, the Committee may, among other things, issue guidelines

which specify the abstract provisions of the GDPR. This is intended for

take and those affected, but also for the supervisory authorities themselves, the uniform

General application of the GDPR can be made easier. The EDPB has this year

A

and

s

i.e

e

right

P

right

a

x

i

s

333 § 11 para. 1 sentence 1 item . 7 and 11 BlnDSG

231

a record number of 12 guidelines were developed, which are briefly presented below

become.334

The guidelines deal e.g. T. with current social challenges

ments that also require a data protection solution; this year

primarily with data protection issues related to the corona pandemic.

The main focus was on the use of position data and applications

contact tracing, e.g. B. in connection with Corona warning apps,335 but

also to the processing of health data in research in connection

related to the pandemic.336

In addition, there was a focus on current phenomena of digitization, such as B.

the processing of personal data in connected cars,337 the subsequent

following activities on social networks338 and the right to be forgotten

in connection with Internet search engines339. In addition, it resulted from

so-called Schrems II decision of the European Court of Justice

ability to specify in a recommendation the conditions under which

Data transfers in third countries are based on standard contractual clauses

can.340

Guidelines have also been drawn up for some “classics” of data protection law,

such as B. on video surveillance341 and the concept of consent342. The need

334 In about half of the cases, the results of public participation are still

evaluates before they are finally dismissed.

335 Guidelines 04/2020 for the use of location data and contact tracing tools

tracking related to the outbreak of COVID-19

336 Guidelines 3/2020 on the processing of health data for scientific

Research purposes related to the COVID-19 outbreak

337 Guidelines 1/2020 on processing personal data in the context of connected vehicles

and mobility related applications

338 Guidelines 08/2020 on the targeting of social media users

339 Guidelines 5/2019 on the right to be forgotten criteria in cases relating to

on search engines according to the GDPR, part 1: version 2 .0

340 Recommendations 01/2020 on measures that supplement transfer tools to ensure

compliance with the EU level of protection of personal data

341 Guidelines 3/2019 on the processing of personal data by video devices;

see 13.1.

342 Guidelines 05/2020 on consent according to Regulation 2016/679, version 1 .1

the adoption of some of these guidelines resulted in part from the fact that

certain legal terms in the GDPR are worded or interpreted differently

than in previous data protection law. This applies in particular to the

lines to the concept of controllers and processors, the very

practice-relevant statements on the increasingly important legal institution of

contain shared responsibility. The same applies to the guidelines for

Privacy by design.343

In addition, the committee dealt with other data protection issues

Special topics such as B. the transfer of personal data to third countries

public bodies344 or the relationship between the GDPR and the second number

Health Services Directive345.

Finally, the guidelines on the concept of the

relevant and reasoned objection.346 These guidelines, to which the Bln

BDI was involved as rapporteur, are responsible for the cooperation of the European

ical supervisory authorities is of crucial importance, since they

regulate suspensions for the dispute settlement procedure before the EDPB. The EDPB

was this year with the first dispute settlement procedure in an individual case

dealt with,347 for which these guidelines formed an important basis.

All guidelines can be found on the EDPB website.348

If a German translation is available, we will also publish it on our

our website.349

343 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default; see also

in detail 17.3

344 Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for trans-

Transfer of personal data between EEA and non-EEA public authorities and bodies

345 Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the

GDPR

346 Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

347 See 17.5

348 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_

en

349 https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitli-

no

17.5 First dispute resolution procedure before European Data Protection Board – A missed chance!

s

i

x

a

right

P

right

e

i.e

s

and

A

More than two years after the GDPR came into effect, the EDPB has its first ten binding decision in a so-called consistency procedure. a sol

A dispute settlement procedure before the Committee is initiated when two or more supervisory authorities in the EU do not agree on how to to be dealt with in a specific case. In this case it was a data breach in the mobile app of the company Twitter, which resulted in not being able to Publication of certain personal data temporarily free on the Internet were accessible. Since this company is headquartered in Ireland, had the Irish supervisory authority has the task of informing the other supervisory authorities concerned shall submit a first draft decision.

With the draft decision submitted by the Irish regulator

a large number of European supervisory authorities do not agree and submitted the

verse objections. Since this was the first dispute settlement procedure,

first guidelines had to be created, as in detail with such

objections is to be dealt with.350 We have participated in the preparation of the guidelines

shares and could z. B. Enforce that also appeals in relation to the amount

a fine are possible. The nationwide coordination of the German

decision was the responsibility of the Hamburg supervisory authority, which we are involved in the proceedings

have worked. In terms of content, it was about the legal justification of the

draft decision and the amount of the proposed fine.

Unfortunately, for formal reasons, the EDPB has largely refused to deal with the

substantive arguments for legal justification. There-

down were very important questions, such as B. on integrity and confidentiality,351

on the responsibility of the person responsible352 and on data security353. This is on

350 Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679

351 See Art . 5 para. 1 letter f GDPR

352 See Art . 24 GDPR

353 See Art . 32 GDPR

understandable on the one hand. Finally, the dispute resolution procedure is

subject to deadlines and the Committee, in its first coherence

above all to prove his ability to act. On the other hand

With such an approach, the committee can fulfill its most important task

not adequate to ensure the uniform application of the GDPR.

A significant contribution could have been made to this end by

all legal questions raised would have been decided. Therefore have

the German supervisory authorities when voting against the decision of the

EDSA voted. However, this was accepted by the majority.

The only ray of hope is an aspect that the BlnBDI has overseen in terms of content. In which

We have a joint objection from the German supervisory authorities, in particular

dere criticizes the amount of the proposed fine, which is based on the

Resolution draft originally in the range between 0.005% and 0.01% of the

resales of the company concerned should move. According to the GDPR

However, in each individual case, a fine must be effective, proportionate and

be daunting.354 However, a fine in such a low range is for that

companies concerned are hardly noticeable, so that we

supervisory authority have lodged an objection to the amount. This part of the

appeal was successful, so that the Irish supervisory authority reassessed the fine

must calculate.

It is to be hoped that the Committee will

takes the opportunity to comment on content-related questions. On-

otherwise he can do his job for a Europe-wide uniform application

to take care of the DS-GVO, hardly do justice.

354 Art. 83 para. 1 GDPR

17.6 Impact of Brexit on European cooperation procedures

s

i

x

a

right

P

right

e

i.e

s

and

A

Great Britain withdrew at the end of the transition phase on December 31, 2020

from the European Union. Brexit has a significant impact on the

processing of complaints in cooperation between the European

Supervisory authorities (cooperation procedure).

In principle, complaints that involve cross-border data

arbeit355 is based, between the lead supervisory authority and

coordinated with the supervisory authorities concerned. This is the case when a

company has more than one branch in the EU or the data processing

(due to the Europe-wide activity) significant impact on those affected

fene in several member states. The lead authority is that

country in which the company has its principal place of business or only place of business;

she serves as the single point of contact for the company.356

From January 1, 2021, complaints against companies with

the main office in Great Britain, no longer in the so-called one-stop

Shop procedures agreed between the European supervisory authorities, so

if these companies do not have a new head office within the EU

have called. This means that from this point in time no procedures in IMI, the

serves as a communication platform for the European supervisory authorities,357 under

Participation to be led and coordinated by Great Britain. Any supervisory

authority is now responsible for the complaints submitted to it and

ascertained directly from the respective company in Great Britain. That

Privilege of having a uniform approach with the respective lead supervisory authority

It is not necessary for these companies to have a contact person for questions of data protection.

take from this point.

For the processing of complaints that were already submitted to the BlnBDI before Brexit

have been received, the BlnBDI is in with the regulator in the UK

355 See Art . 4 no. 23 GDPR

356 For further details on the cooperation procedure see also 17.2

357 See 17.2

Contacted to get important information about a

possible relocation of company headquarters to the EU

to get. In consultation with the regulator in the UK we have

also contacted the UK companies in question themselves to

determine whether they move their main branches to another member state

stores or have appointed a representative358 within the EU. We hope that

we thereby the threatening chaos, which the Brexit also in this area

caused, at least mitigated.

The BlnBDI was part of a European working group on the subject of

Brexits actively to answer many individual questions about cases in which the supervisory authority in

Great Britain has been involved up to now. On the one hand, this applies in

ments in which it was active as the lead authority and the processing

of the complaints could not be closed by December 31, 2020. other

On the other hand, this also applies to complaints filed by British victims

and processed by a supervisory authority in another member state

be served. The relocations to be expected as part of Brexit

Corporate headquarters and related change

the responsibility of supervisory authorities can lead to the processing

dealing with complaints against companies headquartered in the UK

delayed.

358 See Art . 27 GDPR

18 Duty to inform

data breaches

18.1 Overview and Individual Cases

After the sharp increase in data breach reports in 2019

The number of reports in the reporting period remained 1,017 cases at 925 cases359

on a high level.

Two things can be derived from this: on the one hand, the increasing awareness

of those responsible with regard to the lawful handling of data

on the other hand also the fact that altogether too many data breaches

occur, whereby a high number of unreported cases can be assumed.

This time the numerous reports of data breaches in the medical

zinic area. Here it was z. e.g. incorrect sending of diagnostic reports

ments, laboratory findings or X-rays by medical staff, for example because

an incorrect fax number was used. Since health data is about

data that is particularly worthy of protection,360 those responsible usually have it

already informed us in the notification361 that the affected persons

informed about the incident and independently of any legal obligation362

Measures have been taken to avoid such mistakes in the future. to

These measures included B. the introduction of the four-eyes principle

shipping process.

We received a large part of the reports from a nationally active medical

financial billing service. This was mainly about the unauthorized knowledge

359,821 reports in the non-public area, 104 reports in the public area

360 See Art . 9 para. 1 General Data Protection Regulation (GDPR)

361 According to Art. 33 para. 1 DS-GVO, the supervisory authority is to be

to be informed within 72 hours of becoming aware of the incident.

362 According to Art. 34 para. 1 DS-GVO, the person responsible must inform the data subject about the

Report incident if it poses a high risk to their rights.

Chapter 18 Obligation to provide information in the event of data breaches 18 .1 Overview and individual cases

acceptance of bills for private medical services. Cause for this

However, data breaches were not the fault of the billing service. A lot of-

more the error lay with the respective service providers who entered the address

sen of the persons treated had not verified, so that the bills the

could not reach the right addressees from the outset.

The correct handling of such a case of postal undeliverability

would, however, have to be returned to the sending medical service

have to lead. Instead, the invoices were sent by the delivering company

give it to the wrong recipients or put it in their mailbox

thrown. They then have the billing service via the incorrect delivery

informed, often after checking the content of the letter for their own concern

and thus has taken note of sensitive data of the person being treated-

ten. The billing service, for its part, reported the incidents to us and

informed immediately that he himself had informed the persons concerned in each case

or will inform you as soon as he has the correct addresses. This He-

approach is exemplary, because a possible and possibly lengthy dispute

about whether the service provider and/or the delivery company

bears the legal responsibility for the data breach and accordingly

must inform those affected by the breakdown of this, in favor of a

avoid informing those affected as quickly as possible. that a

subcontractor employs personnel who apparently do not comply with the contractual

main obligation, namely postal items only with correct addressing

to deliver is another matter.

Reports from a nationwide trade union were also relatively frequent

community, because in each case different state districts or departments

electronic mailing of union messages to its members

e-mail distribution list had used. Such data breaches, in which "only" the u. U.

personalized e-mail address for all other e-mail recipients

At first glance, they appear to be of little legal significance

to be, especially since the error is immediately obvious to all concerned. Nonetheless

is to be considered here that from the affiliation of a person to this

e-mail distribution lists can be closed directly to their union affiliation

can - a personal data particularly worthy of protection according to the law

239

tum.363 It is therefore important that the person responsible for the error

aware and acting appropriately. This happened in all cases reported to us

in that - this time with "hidden" e-mail addresses - a

another email apologizing for the data breach to the same distributor

ler was sent, combined with the promise in the future when sending

e-mails to ensure that the e-mail distribution list is not empty for all recipients

catchers is visible.

Banks have also increasingly reported data breaches to us for which they are responsible

were literal. This was primarily about false transmissions of credit

documents or the unauthorized disclosure of bank account information such as B.

the full IBAN or account balances. Initial disagreements with

individual banking institutes whether this poses a high risk for those affected

with the result that the bank compellingly informs those affected about the incident

had to notify,364 soon disbanded: in almost all reported

ten cases, the banks have opted for maximum transparency and the

the respective data subjects are informed about the data breach as a precautionary measure. Also this is

commendable from our point of view.

Overall, those responsible dealt with data breaches appropriately. Where

People work, mistakes happen. For us it is important that and how a missing

ler is "captured" in particular from those affected. This includes

on the one hand, the admission of the person responsible that a

data breach has occurred, and secondly, taking measures to

to avoid such mistakes in the future.

18.2 Data Breach Superior Court

Last year we reported on the malware infestation at the Kammerge-

directed, the elimination of which led to a month-long failure of the information technology

nik of the court.365 The attack and subsequent analysis revealed

363 See Art . 9 para. 1 GDPR

364 See Art . 34 para. 1 GDPR

365 JB 2019, 2.4

s

i

x

a

right

P

right

e

i.e

s

and

A

Chapter 18 Duty to provide information in the event of data breaches 18 .2 Data breach Superior Court

Security weaknesses of the previous infrastructure caused by a new construction

of information technology were eliminated with the support of ITDZ366.

The infestation of the computer networks of the Supreme Court with the malware Emo-

tet meant that overnight the entire information technology

had to be switched off and thus the digital work of the court

partially paralyzed for months. Gradually, the individual working

places back into operation, initially without any network connection. For

necessary connections to the outside were used as a data lock, so-called trans-

fer PCs set up. Regarding the safe design of this interface

we gave hints.

At the same time, external specialists carried out a forensic analysis of the attack

carried out and the previous IT infrastructure evaluated. The result revealed

serious weaknesses in protecting the sensitive data processed by the court

ven data. Since the virus scanners installed locally on the computers, the infection

had not noticed and the data networks of the court were not sufficiently

were sealed off, the Emotet malware could spread to a number

distributed from workstations and servers.

The operators of the malware thus gained access to the information

technique of the court. This access was used, among other things, to find traces in the form of

Delete log data so that it does not interfere with forensic analysis either

more reliably determine whether and which data may be in the hands

of the attackers have reached. The route of infection was also not certain

reconstruct. The first infection by such malware occurs when

however, often through a manipulated file sent to individuals by email

is sent.

The overall extent of the systems compromise and whether

The forensic analysis could not clarify the fact that data was leaked. Unfortunately

was also refrained from removing at least parts of the deleted files from the

366 The information technology service center (ITDZ) is a municipal

take the necessary information for the digitization of the Berlin administration

tion technology and secure networking.

241

restore the backup and get a more complete picture of the incident

to get.

Since the Court of Appeal did not have a system with which it could reliably

Malware-free old systems and the data stored with them

could determine, it decided to rebuild its entire network.

In this context, most were required by the Court of Appeal

Services relocated to ITDZ. The documents originally stored in the old system

genes remained isolated and only stood as an archive for a longer period of time

available for inspection.

The reorganization of the information technology of the Supreme Court opened up the

ability to improve the structure of the networks and applications,

than has been the case so far. The new system that has been set up has a

strict separation between the internally defined

used components and the external components for internet use and

email communication. The former are now administered in the ITDZ

SBC environment367, in which all programs and data are on protected

Servers are located and the workstations only as terminals, i. H. only for

ture input and screen output.

By sealing off the components connected to the Internet and a

By dividing the network into separate, separate areas, it is now

much less likely to be reinfected with malware

would have similar far-reaching consequences.

Another important step was to equip the judges

Judges with mobile service devices that allow them to work at home

allow environment.

Previously, this homework took place - on a legal basis - with private devices

took place and data was exchanged between these private devices and the official information

mation technology exchanged uncontrolled, primarily via USB sticks or

by sending it by email.

367 SBC - Server Based Computer

A sufficient number of mobile service laptops were gradually made available

provided or stationary home workplaces set up on request. Since
Fall there is also the option of accessing the internal via a mobile VPN solution
Information technology and thus on essential judicial procedures and central
access the court's stored case files. The document creation
Development and administration is now carried out via the forumSTAR judicial procedure. Of the
previously usual data exchange via USB sticks was also technically prevented
by deactivating the USB interfaces of the (mobile) service devices
and the use of mass storage devices is only permitted on transfer PCs.
In addition, employees are now back at their (mobile) workstations
business e-mail accounts available.
The security of the systems used is a prerequisite for data protection
former official activity. Therefore, it is imperative that the architecture
of the information technology used, also with regard to protection against
design malware. Private and business must be strictly separated.
The Court of Appeal took the incident as an opportunity to
IT systems to be fundamentally modernized and secured to a high degree.

19 Freedom of Information

19.1 Developments in Germany

The Conference of the Freedom of Information Officers in Germany (IFK) took place
this year for a special occasion under the chairmanship of the Hessian
mandated for privacy and freedom of information held because recently now
general access to information has also been standardized by law in Hesse
is.368 Members of the IFK are all freedom of information officers in German
country; they are located at the respective data protection supervisory authorities. the
The federal states of Bavaria, Lower Saxony and Saxony are due to the lack of their own

still not represented in the IFK.

19.2 Developments in Berlin

19.2.1 Amendment of the Berlin Freedom of Information

legal

s

i

x

a

right

P

right

e

i.e

s

and

A

Against the background of the new version of the Berlin Data Protection Act

(BlnDSG), with which in 2018 an adjustment to the basic data protection

regulation (DS-GVO), we had in the same year at the responsible

senate administration for interior affairs and sport also a change in the Berlin

Freedom of Information Act (IFG) with regard to the tasks and powers

the Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI) in

encouraged in this area.

An adjustment of the law was necessary because references

from the IFG no longer match the BlnDSG after its amendment. To the

Reason we had additionally pointed out that it was already due

the independent importance of freedom of information makes sense that the IFG

completely self-contained. This autonomy has

368 See Annual Report 2018, January 13

pealization of data protection law strengthened once again. We therefore have-

promoted, the regulations on the tasks and powers of the BlnBDI from the

Separating BlnDSG and including it directly in the IFG, which so far only

provided a corresponding reference to the BlnDSG. spoke for our concern

also that the freedom of information officers - unlike the data protection

commissioned - primarily as an arbitration board and in an advisory capacity to applicants

officials and bodies responsible for information become active, so that the new

gifts and powers of the data protection officer according to the DS-GVO

More could be transferred to the freedom of information officers.

The mere reference to the relevant regulations of the BlnDSG, as it has been up to now

was to be found in the IFG,369 therefore proved to be no longer appropriate.

However, our request was not already addressed when the GDPR came into effect

2018, but more than two years later, towards the end of the reporting

room, partially taken up: In the course of the amendment of the state law

Provisions for adapting to the requirements of the DS-GVO370 were also made

the IFG changed.371

Solely in relation to the establishment of our authority, the appointment and termination

of the official relationship and the legal status of the representative

itself is now referred to the provisions of the BlnDSG.372 On the other hand

is now expressly in addition to the data protection authorization for processing

personal data also the scope of our control options

authority in the IFG itself.373 This includes advice and the submission of

Recommendations as well as the duty of public authorities to inform us before issuing

Hear laws, ordinances and administrative regulations if they

concern freedom of information.374

369 § 18 para . 2 IFG a . F.

370 See 17.1

371 Art. 5 of the law for the adaptation of data protection regulations in Berlin

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

EU - BlnDSanpG-EU) from 12. October 2020, GVBl. 2020, p. 807 (808f.)

372 § 18 para . 1 IFG

373 § 18 para . 5 and 6 IFG

374 § 18 para . 2 IFG

Unfortunately, other regulations affecting the work of our authority

are expressly specified for the area of data protection in the BlnDSG

included in the IFG. Above all, it is about the right, at any time

to gain access to offices and information processing systems,

as to a definition of the extent of the opinions of administrations

where deficiencies in the area of freedom of information were identified.375 It would be

It would have been sensible to provide here that such statements also

Measures should contain the result of a complaint from our authority

were hit. In this regard, too, there would have been a change – not least in terms of the importance

of freedom of information - a harmony of both laws

messengers. We will address this request as part of the intended development

of a transparency law to replace the IFG.376

The amendment of the IFG with regard to the explicit regulation of the tasks and

Powers of our authority in the law itself was overdue.

19.2.2 Finally at the start - Draft for a Berliner

transparency law

s

i

x

a

right

P

right

e

i.e

s

and

A

In order to fulfill the coalition agreement, in which, among other things, the further development of the

IFG towards a transparency law,377 the Se-

nat decided on the cornerstones for such a law in the summer. we has-

given the opportunity to comment beforehand. Our partly massive

However, criticism was raised in the later draft bill of a "Law on the Further

development of information access for the general public" (draft of a report

Liner Transparency Act - BlnTG-E) of the responsible Senate administration

unfortunately not taken into account for the interior and sport. We also have this

We took a stand and expressed our criticism again and in some cases deepened it.

So we have highlighted as a key deficiency of the BlnTG-E that over

the area exceptions already existing in the current IFG a variety

375 See § 13 para. 4 and para. 2 BlnDSG

376 See 19.2.2

377 JB 2018, 13.2.1

number of other exceptions for various authorities. This would be a

mean a significant deterioration compared to the previous legal situation and

in this respect not a further, but a backward development of the IFG. This will not

balanced by the new proactive information access, which - as a core

part of a modern transparency law – public bodies

dependent on the provision of information on an electronic disk

shape, i.e. H. in a transparency portal. The list of exceptions from

Scope378 is so long that we asked for it, at least

to delete those that go beyond the previous legal situation. The GE-

make any planned exceptions, including the deletions we recommend

is therefore - analogous to the applicable IFG - as follows:

“There is no obligation to provide information under this law

1. for courts, law enforcement and criminal enforcement authorities, to the extent

they as organs of the administration of justice or due to special legal

writings have become active in judicial independence, for which for

Judiciary responsible senate administration, insofar as they act as a specialist supervisory authority

via the public prosecutor's office or in matters of clemency so-

as for processes arising from disciplinary proceedings and

procurement chambers;

2. for the Court of Auditors, insofar as it acts with judicial independence

has been; this does not apply to its annual reports;

3. for tax administration processes and internal audits;

4. for the protection of the constitution;

5. for the Berlin House of Representatives in relation to parliamentary

occasions;

6. Public service broadcasters with regard to journalistic-editorial

functional information;

7. for general education schools, school authorities and school supervisory authorities

—

with regard to information that enables the creation of a ranking

and are therefore suitable for the realization of educational and

to jeopardize food targets;

378 See § 3 para. 1 BlnTG-E

247

8. for university clinics, scientific and research institutions,

Universities, schools as well as for educational and examination institutions, es

unless there is information about the name of third-party funders who

The amount of the third-party funds and the term of the third-party funds

closed research projects affected;

9. for basic research or applied research; § 7

sentence 1 number 9 remains unaffected;

10. for self-governing bodies of the liberal professions with regard to information

—

information that is subject to professional secrecy."

It cannot be the task of a transparency law to

limit the flow of information further than was previously the case. Every

(further) scope exception diminishes the value of a modern transparency

law in public.

So e.g. B. incomprehensible why the Senate administration responsible for justice

in matters of clemency (No. 1) from a legally standardized transparency

renz should be completely exempt, there is a lot of general information

(such as pardon figures) that may be of interest to the public.

The same applies to the public procurement tribunals (No. 1 a. E.) with regard to their decisions

ments – Individual information from the companies should be replaced by the intended

Regulation for the protection of trade secrets must be adequately protected.379

Transactions of the tax administration (No. 3) should not be assumed from the outset either.

be attached, because they are also fundamentally of public interest,

e.g. B. with regard to tax calculation models in the tax offices.

Although it corresponds to the previous legal situation,380 it is not comprehensible

Whatever the reason, the protection of the constitution (No. 4) in the future none at all

should be subject to a transparency obligation. This is contrary to the regulations

who expressly have a duty of the protection of the constitution to provide information

the public and thus a possibility of control by the

379 See § 16 BlnTG-E

380 See § 32 para. 3 Constitution Protection Act Berlin (VSG Bln)

can be manifested by citizens and the media.381 The public can

undoubtedly general information about the tasks and powers,

Fields of work and procedures of the protection of the constitution made accessible

without affecting safety aspects. In addition, can and must

the protection of the constitution informs the public in the event of dangers to the free democratic

inform cratic basic order anyway. This includes, for example, the publication

clarification of information on current events in the extremist spectrum,

the information about the ideological foundations of Islamism, the legal,

left-wing extremism and foreigners, as well as the most important

current extremist groups. The regulation now envisaged would

As a result, not even the previously public reports from the Office for the Protection of the Constitution

to be placed in the transparency portal as information subject to publication

382 Otherwise, as in other areas of internal security

also - the exceptions provided for in the law383 are sufficient to

To ensure the need for protection of part of the work of the Office for the Protection of the Constitution.

A completely wrong signal goes from the overwhelming exclusion of science

scientific institutions, universities, schools and educational institutions

or general education schools, school authorities and school supervisory authorities

those from (No. 7 and 8). Especially in the field of science and education, transparency

particularly important with regard to information from the administration. So should-

students or parents of school children (possibly upon application) may find out

how many lectures or lessons in a certain subject

during a study or school year without replacement. That applies all the more

more in times of pandemic. The creation of a "ranking list" for schools may - whether

rightly or wrongly - not wanted by the school authorities, but it should be

not lead to existing information (e.g. in the context of school

inspection reports) are not disclosed from the outset: that individual

through disclosure “would be wrongly given a negative rating because

individual statistical values would be brought into focus”,384 is speculative and

carries out the evaluation by responsible parents and the general public

381 See § 5 para. 1 and § 26 sentence 1 VSG Bln

382 See § 7 para. 1 no. 8 BlnTG-E

383 Z. B. § 13 para. 1 no. 4 BlnTG-E

384 This is the justification for Section 3 No. 7 BlnTG-E

away. In addition, the subordinate clause in the above No. 7 too vague and harbors

therefore a considerable potential for disputes or lawsuits.

The university clinics (No. 8) also have general information

ments relating to hospital administration, which are not a priori secret

hold are A prominent example is the number of people suffering from Covid 19

called free beds.

An exception for the self-governing bodies of the free

rufe (No. 10) is not required because of paragraph 2 of the planned standard.

According to this, the obligation to provide information does not exist, insofar as other legal provisions apply

oppose

In addition to these sprawling area exceptions, we have the planned ones

additional restrictions on the publication obligation385. The this-

relevant list, including the deletions recommended by us, is being drawn up

as follows:

"The following are exempt from the obligation to publish:

1. Contracts with an object value of less than 100,000 euros if

between the contracting parties over the past twelve months

Contracts with an item value less than 100,000 in total

euros;

2. Subsidy and grant awards of a value less than

100 euros for legal entities or less than 1,000

euros for other organizations with partial legal capacity and natural persons

over a period of twelve months to a recipient

a recipient;

3. the granting of a building permit or a preliminary building permit to a

Applicant, provided that it is a purely residential

building with a maximum of five residential units.

385 See § 9 BlnTG-E

4. Expert opinions and services for individual cases, e.g.

—

sic examinations or laboratory examinations of products or

soil samples,

5. Opinions and services in which a publication from

would be inadmissible for data protection reasons,

6. Expert opinions and services that are only individual aspects of a total

—

discuss unfinished topics,

7. Reports and services that help the internal opinion-forming of the

nats in advance of decisions still to be made,

8. Opinions and services in connection with legal

—

other stipulations if their publication is in the interests of the state

of Berlin would affect and

9. Reports and Services Containing Confidential Business Data

—

or their publication against the confidentiality obligation according to § 395

of the German Stock Corporation Act would be violated.

The exceptions to the publication

obligation apparently correspond to the explanations of an existing since 2013,

Administrative regulation of the Senate Department for Finance, unknown to us,

i.e. a sub-statutory regulation that - at least questionable, if not

illegal - deviations from the previous legal situation, the IFG,

sees.

The necessity of these exceptions is not stated in the explanatory memorandum

placed; Incidentally, it is unclear for all the exceptions mentioned what the term der

“Services” includes.

In the case of No. 4, it is also unclear which individual cases are intended and from which

chemical reason not to disclose the apparently health-related information

are.

251

No. 9 speaks of “business confidential information”, which is not further defined;

the protection of trade secrets regulated elsewhere in the draft law

nissen386 is sufficient for this.

Further recommended changes to the BlnTG-E related to data protection

aspects. In principle, an anonymous application should be possible. Then

an individual application does not always have to be the identity of the applicant

Reveal the person, but only to the extent that the identity for the answer

of the request is required. However, it is not required if the applicant

The person concerned should only be informed that the desired information

functions are not available; it is also not required in cases of

fee waiver,387 because an appealable (fee) decision must then

not be granted. The name and the postal address are, however, then

required if a notification of fees has to be served.388

The disclosure of employees' core data389 upon request should be

"Telecommunication number" the e-mail address and the name of the

signing person include. Because the e-mail address is in the age of electronic

electronic communication is the most important contact date and should

not be in need of protection. Signing persons carry the substantive

responsibility, so that their names also do not in principle need to be protected

are.

We hope that the Transparency Act will be passed in good time before the end of the legislature

ture period will be adopted in autumn 2021. Until then we will

continue to critically but also constructively support the legislative process. Included

will also have to be ensured that the most recent changes to the IFG

together with our other recommendations390 in the new transparency

be taken over.

386 See § 16 BlnTG-E

387 See § 20 para. 1 set 2 BlnTG-E

388 Different § 15 para . 2 BlnTG-E

389 Previously permitted under Section 6 Para. 2 sentence 1 no. 2 IFG

390 See 19.2.1

19.2.3 A transparency barometer for Berlin

The Senate Department for Justice, Consumer Protection and Anti-Discrimination

sent us the draft bill for a transparency law

results of official controls in food control (development

draft of a food monitoring transparency law - LMÜTranspG-E)

as well as the draft for the regulation implementing the law, which also

includes judgment criteria. With this project, a corresponding coa

2016 litigation agreement to be implemented. Here it is stipulated that Berlin

campaign for more transparency in the area of food hygiene

and, if necessary, will also create its own state regulations.

A

and

s

i.e

e

right

P

right

a

x

i

s

We have already dealt with a precursor model in the past, the

Smiley project in the district of Pankow, and from the point of view of information

safety and data protection.391 For its part, it was based on corresponding

the models for restaurants in Denmark, but could not go further in this country

be led because there is a legal basis for the publication of the

official control results were missing.

This legal basis for the mandatory publication of the results of the

official food control is now to be created. core component is

the so-called transparency barometer, on which the control results are indicated by a colorful

bar chart can be displayed graphically. In it marks a point to green-

the arrow that the hygiene requirements are met, and a point to yellow-

the arrow indicates that these requirements are partially met. If the arrow is on red,

the requirements are insufficiently met.392 Below the transparency barometer

the assessment criteria and their assessment are listed in text form.

In order to ensure that consumers are informed prior to the visit, e.g. B. one

Inform the restaurant or a snack bar about the state of hygiene there

this company should be obliged to use the transparency barometer

ter immediately on or near the front door. In addition to

This on-site information opportunity is a publication on the Internet

391 JB 2008, 15.2.2; JB 2011, 13.2

392 § 5 para . 4 LMÜTranspG-E

the responsible food supervisory authority,393 so that the efficiency of the information

mation is increased.

The LMÜTranspG-E initially also provided that the transparency barometer

In addition to the business premises with addresses, the responsible foodstuffs

telecompanies by name.394 We questioned that by

we have asked the responsible Senate administration to clarify for us

what reason the mandatory disclosure of the name of the operation

Controllers - in addition to the mandatory disclosure of the names of the

Business premises – is deemed necessary. Apparently this was not

cash, because the draft law was then amended accordingly. Both out

The naming of the business premises is important from a transparency and data protection perspective

with an address in the transparency barometer is entirely sufficient.

We welcome the planned transparency model as a step that is overdue

to strengthen consumer information, especially with regard to restaurants

ten in Berlin.

19.3 Tutoring for the Senate Administration for

Environment, transport and climate protection

We received two complaints that the Senate Department for the Environment,

Traffic and climate protection related traffic management.

s

i

x

a

right

P

right

e

i.e

s

and

A

(1) The General German Bicycle Club Berlin e. V. (ADFC) complained

We spoke to us at the beginning of February about the fact that, upon his request for inspection of

the contract modalities of the city with Alliander Stadtlicht GmbH from Mitte

December 2019 I have not received any response despite reminder. For justification

of the request was submitted by the ADFC that in Berlin again and again

lead to massive delays and long implementation periods for the adaptation

solution of traffic lights by the company. The long war

times, especially at accident-prone intersections, repeatedly led to

394 § 8 para. 1 LMÜTranspG-E i . v. m . § 4 of the relevant Ordinance-E

dangerous situations for pedestrians and cyclists. Therefore went

the ADFC is specifically concerned with finding out which benefits and sanctions

mechanisms in the event of non-performance have been contractually agreed, such as those

Evaluation of the provision of services was regulated and which termination

possibilities of the contract had been agreed.

We then contacted the responsible Senate administration

and asked to take care of the matter and about the application now

immediately, d. H. without culpable hesitation,395 to decide396 as well as us one

send a copy of the notification. After a month of no response, we too

opposite, we had to get the Senate administration to deal with the end of March

matter remember. We then received a copy of the

decision of the Senate Administration, with which the application for access to information

was rejected. The main reason given was that disclosure

of the contract, the protection of company and business secrets397

stand. Such secrets are all facts related to a company,

Circumstances and events that are not obvious, but only a limited one

group of people are accessible and to their non-disclosure of the legal entity

have a legitimate interest. An interest in non-proliferation is

recognize when disclosure of the information is appropriate to avoid possible con-

access to exclusive technical or commercial knowledge

and thus adversely affect the company's competitive position.

flow or cause him economic damage in any other way.

Although the senate administration correctly used the current definition of legal

used to talk about company and business secrets;398 however

has it accepted the need for protection in relation to the entire contract, whether

the disclosure of the entire contract was probably not requested. Instead of this

the senate administration should have checked whether the specifically desired parts

Information from the contract that is worth protecting

represent mysteries.

395 See § 121 para. 1 clause 1 of the German Civil Code (BGB)

396 See § 14 para. 1 sentence 1 IFG

397 See § 7 IFG

398 Case law: see e.g. B. BVerfG, decision of 14. March 2006 – 1 BvR

2087/03, 1 BvR 2111/03; BVerwG, judgment of 28. May 2009 – 7 C 18.08

255

Against this background, we have recommended to the ADFC against the decision

to object. He followed this recommendation at the beginning of May. After a

Interim message from the Senate administration from the beginning of August to the ADFC, the

At the beginning of October, we decided to give priority to the objection “now”.

asked about the situation. We were then informed that the

decision will be made in the second half of October. This promise was

fills: The contested decision was revoked and the ADFC was given the

acceptance in the overall general contractor agreement for the management of

Planning, construction, operation and maintenance of the traffic signal system infrastructure

awarded, from which the essential services, the sanction and

the evaluation mechanisms as well as the regulations for the termination of the

ral takeover agreement. Furthermore, the right to inspect two

Appendices to the contract confirmed, from which additional performance obligations and

contractual penalties. Only the included "monetary amounts and pro-

cent figures” were made with reference to operating and business

secrets blacked out.

This is a prime example of our successful work in the function as

Arbitration board according to IFG.399

s

i

x

a

right

P

right

e

i.e

s

and

A

(2) A petitioner had contacted the Senate Department for the Environment, Transport and Climate

schutz an application for inspection of an exemption granted for the

temporary use of a special bus lane for loading and unloading activities

from a local car dealership. Access to the files was granted.

However, a fee of EUR 25.00 was set for this and around

Please transfer the amount in advance within three weeks. Against

the petitioner has lodged an objection and asked us for support.

We have informed the Senate administration that the requested in-

information is “environmental information” that can be inspected on site

is free of charge.400 Because the term "environmental information" is

ment of the Federal Administrative Court to be interpreted broadly; an even moderate

399 See § 18 IFG

400 See § 18a para. 4 sentence 3 no. 1 IFG

Accordingly, a connection between the individual data and the environment is sufficient.401

That was the case with the information in question. Because the car

exemption granted by the house for the temporary use of the special bus

lane for loading and unloading activities is objectively a complication for the

Bus and bicycle traffic, which according to general life experience lead to this

can prevent those affected from using these means of transport

and use your own car instead. But that would mean the one with the bus or

The purpose pursued by bicycle use in Berlin is to reduce environmental emissions in favor of climate

to minimize protection. Against this background, here at least

at least the indirect connection of the requested information with the

to affirm the world.

The petitioner later informed us that he had received a reminder regarding the pre-determined

fee (plus reminder costs). We have the Senate administration

pointed out that the decision is also illegal because the other

contested notice without further justification, i.e. a flat rate, for advance payment

obliged to pay the fee. This contradicts the case law of the OVG Berlin

Brandenburg,402 according to which an official handbook in the area of information

only in exceptional cases from the previous payment of the administration fee

can be made dependent. The prerequisite for this is evidence that

without the advance payment, the interests of the household would be jeopardized. This can be about

This may be the case if the applicant is unable or unwilling to pay.

Since there were no indications for this, the Senate Administration is of our opinion

solution followed and upheld the objection to that extent. Incidentally, was

he rejected: Even an indirect connection that was mentioned in the special

information contained in the approval file with the environment was not recognizable

bar. It was not measurable and the file contained no information on how

the environmental impact would be much higher if BVG customers or cyclists

because of the required detour due to loading and unloading activities

would no longer use the bus or bicycle, but would use their own car.

401 BVerwG, judgment of 23. February 2017 – 7 C 31 .15

402 OVG Berlin-Brandenburg, decision of 26. May 2014 – OVG 12 B 22.12

257

We have recommended to the petitioner that the matter be clarified in court

sen, because the indirect connection, which is sufficient according to case law,

hang of the information with the environment does not matter whether actual

Emission values are available or these are included in the file that is requested to be inspected.

were taken. It is sufficient that the requested information according to general

my life experience could have indirect effects on the environment

ten.

The senate administration went to great lengths to justify

so that she does not have to allow the inspection of files on site free of charge, but

only against payment of 25.00 euros. This is apparently intended to

be prevented, which in view of increasingly chaotic traffic

conditions in Berlin are not improbable.

258

Chapter 19 Freedom of Information 20 .1 Developments

20 From the office

20.1 Developments

The past reporting year was for the office of the Berlin representative

for data protection and freedom of information (BlnBDI) in several respects

special year.

As in many other areas of public administration, the environment was and is

the corona pandemic was also a special time for the BlnBDI office.

their challenge. On the one hand, the service had to be compatible with the pandemic

be designed, on the other hand, the necessary and comprehensive

structural measures to change the work organization the legal

disregard the official order of the BlnBDI and do not exceed the quality of the work

affect dimensions.

Through the procurement and use of mobile devices, it was possible for the

The employees have the opportunity to work, albeit with restrictions

be created in the so-called home office. The presence of employees

in the offices of the department, as far as technically possible and

within the scope of the job descriptions of the employees justifiable, significant

reduced. Presence appointments with third parties in the office, on-site appointments and

Tests outside the office were only carried out to the extent that this was

enough was required.

Working from home, the anti-cyclical presence of staff in

the offices and the waiver of (larger) group meetings

personal presence, the previous work organization and the inter-

n communication processes have changed significantly. Through the use of tech

niche tools and formats (e.g. video and telephone conferences).

this only e.g. T. be compensated. The impact on social and collegial

he cooperation between the employees should certainly not be underestimated.

259

As reported,403 the budgetary legislator with the double budget 2020/2021

to the new requirements and the significantly increased workload

entire department after the entry into force of the basic data protection

regulation (DS-GVO) and the BlnBDI for the years 2020/2021 a total of 21

new positions (13 positions for 2020 and 8 positions for 2021) approved. The Berliner

The legislature has thus given a strong indication of the importance of data protection

zes in Berlin in general and the strengthening of the rights of those affected

special set. As expected, the pleasing improvement in staff

However, this is not the case in the supervisory practice of the agency

immediately led to a change in the tense situation. The ones for the year

2020 approved positions had to be advertised, filled and the new employees

workers to be incorporated. But we are on the right track here.

Above all, with the approved increase in staff, our IT department

treatment (Department III) can finally be adapted to the permanently changed

challenges and tasks that are not only due to the GDPR, but also

through the comprehensive digitization of economic and public life

have arisen. In order to bundle competencies and increase efficiency

and to promote cooperation with the legal departments

previous unit structure in Department III dissolved and restructured in

Form of subject-related competence teams for examinations, laboratory activities,

Advice, data protection impact assessment / accreditation / certification,

difficulties and data breaches. The tasks in the competence teams are

because it is coordinated by a team leader who is also the external contact person

acts.

Cooperation with national and international committees and institutions

directions,404 parliamentary support for data protection-related

have both at Berlin and at federal level as well as cooperation with

political, social and economic actors and multipliers

to promote data protection and freedom of information is for

403 JB 2019, 18.1

404 Z. B. the national, the European and the international data protection conference, the

national and international conference of freedom of information officers, the

Berlin Group, the European Data Protection Board and its working groups, the

so-called . subgroups

the BlnBDI of considerable technical importance. To the due to the GDPR

extremely increased number of voting procedures in these areas

and to coordinate reliably across departments, this task was

combined and a newly created "Department for committees,

Press and Public Relations" assigned to the organizational structure directly

reports to the department head. This new paper aims to

increased press and public relations work will also be made possible in order to

our legal information obligations towards the public better

to be able to do justice.

On the other hand, the pleasing and urgently needed increase in personnel

led to enormous space problems. There is one for the office

Significant additional space required in the office building on Friedrichstrasse in

Kreuzberg cannot be realized. A move of the entire office in

larger premises is therefore essential. Looking for a new one

The location was assigned to us by Berliner Immobilienmanagement GmbH (BIM) im

offered a property in Alt-Moabit in the spring that meets this requirement.

After an extensive examination by the BIM and the Senate Department for

Finances, based on a previously prepared needs analysis

by resolution of the Main Committee of the Berlin House of Representatives in December

December the approval for renting the property by the BlnBDI. due to

catch-rich necessary measures for the preparation of the property can

Unfortunately, the move to the new premises will not take place until summer 2022.

In order to be able to cover the current need for additional office space,

It was therefore necessary to rent other rooms in November as an interim solution.

The – albeit temporary – division into two locations provides for the

entire agency an additional organizational and logistical challenge

demand.

20.2 From the work of the service center

Citizens entered - case numbers, trends,

focal points

s

i

x

a

right

P

right

e

i.e

s

and

A

The processing of citizens' complaints is not only one of our

work-intensive, but also one of our most important tasks, since we

received a lot of valuable information from them for our supervisory practice.

First point of contact for all data protection inquiries and complaints

from citizens is the service point Citizens' Entries. Their employees

accept submissions by post, fax, e-mail or electronically

Complaint form on our website, answer it in the

most cases directly or distribute them within the department to the respective

time specialist presentations.

Since the GDPR came into effect in May 2018, the number of citizen petitions

increased continuously and has remained at this very high level ever since:

we receive about 400 entries per month. Despite the restrictions imposed by

the corona pandemic, the service point for citizens' submissions has carried out its tasks

commonly fulfilled. The pandemic has led to a number of content priorities,

which have repeatedly been the subject of complaints from citizens. Numerous

Complaints and inquiries from citizens also concerned the relocation of many

all areas of life into the digital. The focal points crystallized here

The situation of employees in companies and the situation in schools

out.405 In the first half of the year in particular, there were a number of enquiries

Data protection and IT security of specific video conference systems.406

The rules for contact tracing also received a lot of attention. in the

As part of the infection protection regulations, the state of Berlin has

works, catering establishments and many other bodies are obliged to provide information

to collect functions for contact tracing of guests or customers. Us

received many inquiries about the general data protection admissibility of the

405 See 1.4

406 See 1.3

Contact tracking and specific complaints from those affected about open

accessible contact lists in restaurants and shops.407

A key topic outside of the pandemic was in the area

"Tracking", i.e. the tracking of Internet users, e.g. by means of so-called

cookies. The European Court of Justice (ECJ) ruled in 2019 that

Visitors to a website using tracking cookies and

other tracking technologies.408 Many internet

however, sites do not provide an acceptable way to disable cookies. To the-

accordingly, the complaints on this complex of issues have also become clear

increased.

As in previous years, the majority of complaints continue to concern the

Enforcement of the rights of data subjects, in particular the rights to information and

to delete your own data. This is what citizens complained about above all

about companies that responded insufficiently or

didn't react at all. Other focal points were in the areas of video

monitoring and housing management.

20.3 Privacy and Media Literacy

The BlnBDI has set itself the goal of increasing media and data protection

to promote special of elementary school children. As part of our media education

gogic work we have now for the first time project days at basic school

carried out. Our offer met with great interest and increasing

The need for training courses and accompanying teaching material is again clearly

been. For more workshops and projects in schools and educational institutions

to be able to carry out large-scale operations, in the future we intend to

also to train multipliers.

407 See 1.1.3

408 ECJ, decision of 1 . October 2019 - C-673/17 ("Planet49"); see also JB

2019, 13.2

In view of the corona pan-

demie even greater efforts in relation to the data protection

clarification for children and young people, but also assistance for teaching staff

and parents. To this end, we will constantly expand our media-educational

and offer comprehensive information and teaching material.

In addition, we are continuously expanding our digital offering at www.data-kids.de

expand the range of topics and increasingly include audiovisual ones

media and interactive games. Supplementary information material for children

We make it available for download free of charge for teachers, teachers and parents.

20.4 Cooperation with the Berlin House of Representatives

The Committee for Communication Technology and Data Protection (KTDat) met in

this year a total of eight times and dealt with numerous topics

Digitization and data protection apart. The BInBDI attended all meetings

participated and provided advice to the committee. important meeting

Points of improvement included the digitization of schools,409 the Berlin online

access law410 and the introduction of the electronic health record411. Of

Also of great importance were the consultations on the Berlin data protection

EU Amendment Act, with which the state law is adapted to the specifications of the DS-GVO

was adjusted.412 The BlnBDI has this adjustment process as far as possible

was, accompanied and in particular for the elimination of regulatory deficiencies

from the old Berlin Data Protection Act (BlnDSG). With the agreement

enactment of the law in question, however, not all were admonished

ten legal deficits remedied. We very much hope that this will

announced evaluation of the new BlnDSG.413

409 See 1.4

410 See 2.1

411 See 5.3

412 See 1.4

413 See press release of 2 October 2020: "Adaptation of the Berlin data protection

right – there is still a lot to do"; available at https://www .datenschutz-berlin .

de/infothek-und-service/press releases

20.5 Cooperation with other entities

The conference of the independent data protection supervisory authorities of the federal and

of the federal states (DSK) was chaired by Saxony this year. she met

on May 12th and on May 25th/26th November virtually. At the conference in November

vember was an anniversary meeting at which the DSK

100th time since it was founded - unfortunately, given the circumstances

also only digital. In addition, there were three interim conferences, each as

Video conferences on January 29th, June 16th and September 22nd. The DSK summarized

numerous resolutions and resolutions on current

Len data protection issues,414 u.a. to the use of Google Analytics, to

Use of thermal imaging cameras or electronic temperature measurement

in the context of the corona pandemic and for the use of Windows 10 Enterprise.

The BlnBDI also held on 13./14. October at the DSK working group “DSK

2.0” took part, which dealt with the strategic realignment of DSK

and works to improve decision-making processes within the DSK and its

to be optimized overall.

The Conference of the Freedom of Information Officers in Germany (IFK) met

chaired by Hesse on June 3rd and December 1st as video conferences

renz. The committee did not pass any resolutions this time; an all-

Common exchange of experiences on access to information at municipal level.

In addition, representatives of the Darmstadt regional council have inter-

interesting insights into administrative practice in environmental information law and in

Consumer information rights given regarding food. The IFK has itself

undertaken to develop a mechanism by means of which information

Obligatory bodies are responsible for compliance with and efficient implementation of the

Check information access rights yourself, i.e. carry out a "self-audit".

be able.

The Global Privacy Assembly (GPA)415 took place as a three-day video conference from 13.

until October 15th. The focus of the conference was the future strategic

414 All resolutions and resolutions of the DSK are available on our website at

https://www .datenschutz-berlin .de/infothek-und-service/veroeffentlichungen/

decide-dsk available .

415 Formerly the International Conference of Data Protection and Privacy Commissioners

gical direction of the conference. Another focus of the event

tion formed the challenges for data protection in the context of the Co-

vid-19 pandemic. The GPA adopted numerous reports and resolutions,416

including the transparent and non-discriminatory use of artificial intelligence

license.

Due to the pandemic, the International Working Group on Data Protection met in the

Technologie (Berlin-Group – IWGDPT), chaired by the BlnBDI, in which

not this year. Instead, ongoing work on working papers became the

Topics web tracking, data portability, sensor networks and language

identification software in a written procedure. A publication

is scheduled for 2021.

20.6 Public Relations

The media interest in the work of our authority was, as in previous

years, very high. This year we answered over 200 press inquiries.

In the press office, too, topics on data protection dominated during the

rona pandemic our work. By far the most questions reached us

Contact data collection by restaurants and other establishments.417 As concrete

To help, we published sample forms for those responsible so that

they fulfill their obligation to collect contact data in accordance with data protection

could. Furthermore, the topic of digitization of schools took on our

press work.418 In particular, our assessment of the learning

raum Berlin was the subject of various interviews and inquiries. Enormous

Regional media interest in connection with the pandemic generated additional

In addition, our notes and test results on data protection-compliant use

of video conferencing services. This publication is evaluated by a traffic light system

in a clear way whether and to what extent those responsible are subject to legal and

416 All GPA resolutions and reports are available on the GPA website at ht-

tps://globalprivacyassembly.org/document-archive/adopted-resolutions/ and https://

available at globalprivacyassembly.org/document-archive/working-group-reports/ .

417 See 1.1.3

418 See 1.4

from a technical point of view, common video conferencing services comply with data protection regulations

can use.419

Apart from questions about data protection during the corona pandemic

the Emotet infestation at the Superior Court and the use of the personnel software

Zonar by the company Zalando, important topics on which we have a variety

number of press inquiries reached. Our press office was for women journalists

and journalists on these and various other topics as a contact for disposal

tion, so that the sometimes difficult legal and technical data protection issues

genes are presented in a comprehensible and correct manner in media reporting

could.

With a total of 14 press releases, the BlnBDI also addressed its own

n topics to the public. We discussed e.g. B. problematic

developments in the field of legislation. For example, we pointed to regulatory

Deficiencies in the Berlin Data Protection Adaptation Act EU or in the

Senate published key points on the planned Berlin Transparency Act

hin.420 We also used the press release tool to publish our own

ments, such as a guide to smartphone security, the results

our review of video conferencing services or our assistance in

to publicize the gitalisation of the school. Besides, we informed on this

Ways about important current developments such. B. the so-called "Schrems II" judgment

of the European Court of Justice and always took a clear position.421

We published the following press releases this year:

• BlnBDI welcomes the decision on the European guidelines on video surveillance

(January 30, 2020)

• BlnBDI on the data breach at the Investment Bank Berlin (March 30, 2020)

• Annual Report 2019 (3 April 2020)

• Learn from the crisis (May 4, 2020)

419 See 1.3

420 See 17.1 and 19.2

421 See 1.2

• Berlin data protection officer for conducting video conferences

(May 25, 2020)

• Advice on smartphone safety for teenagers published (June 9th

2020)

• Contact data collection by traders - model forms of the Bln

BDI (June 24, 2020)

• Short review of video conferencing services - BlnBDI publishes results

(July 3, 2020)

• After "Schrems II": Europe needs digital independence (July 17, 2020)

• Berlin police refuse to clarify questionable queries in police

databases (13 August 2020)

• Data protection in day-care centers – BlnBDI publishes new brochure (August 17th

2020)

• BlnBDI on the key points for a transparency law (September 3, 2020)

• Berlin Data Protection Amendment Act – regulatory deficiencies persist

(October 2, 2020)

• Data protection is not an obstacle to digital teaching (December 4, 2020)

All press releases are available on our website at https://www.daten-

schutz-berlin.de/infothek-und-service/pressemitteilungen available. With a

E-mail to the address presse@datenschutz-berlin.de is an inclusion in our

ren press mailing list possible.

20.7 Public Relations

20.7.1 Events and Lectures

This year's central event on the occasion of the 14th European Data

protection day took place at the invitation of the conference of independent data protection

supervisory authorities of the federal and state governments (DSK) on January 28 in Berlin,

at the representation of the European Commission in Germany. the country

Commissioner for Data Protection and Freedom of Information Rhineland-Palatinate,

DSK chairman of the previous year organized this event. The topic

was “Artificial intelligence – between taming and promoting”. For the importance

development of AI solutions and algorithms in business and technology and the associated

associated challenges, representatives from politics, science

society, justice and practice.

Many other planned events have been canceled due to the corona pandemic

and the lockdown that lasted months were either canceled or took place in the

smaller frame instead. Some was carried out in digitized form. U.N-

Due to the changed conditions, it was no longer possible for us in all cases

attend events.

The lecturing activity was also initially significant under the new conditions.
slightly restricted. After a preparatory phase, the usual lively
communication of the national and international expert committees, working groups and
However, working groups continue to take place. Participation in expert discussions
Congresses and workshops were increasingly possible again. The events
mostly took place in the context of video conferences.
Some examples are mentioned here:
• Lecture "Is the works council responsible for itself?" for the GDD-Win-
terworkshop (from the GDD e.V., society for data protection and data security
e. V) on January 27, 2020 in Garmisch-Partenkirchen; Online lecture "Data
protection & staff council/works council" at the workshop for the BvD e. V. (Federal
Association of Data Protection Officers e. V.) on May 5, 2020. As part of this
Lectures discussed the question of whether an employee representation for their
own data processing is responsible or the respective company.
We assume the company is responsible;
• Discussion with heads of the rule of law program of the
rad-Adenauer-Foundation on the topic "The digital state. Use of AI - curse
or blessing? Targeted use of digital means to restrict free
heitrechte" on February 11 in Berlin;
• Lecture on "Enforcement of the GDPR in Berlin/Germany in Practice" on 25.
May 2020 as part of the online conference "GDPR Day 2020". With the "GDPR

Day 2020" was an independently organized conference in
related to the implementation of the GDPR in the CIS countries (Russia,
Belarus, Ukraine) brought together specialists from these countries
Has;

• Lecture as part of the "Interactive Roundtable" at the Bitkom Privacy Conference 2020 on September 29, 2020 on "Notes for those responsible in Berlin to providers of video conferencing services" that our authority as a published the result of a short review of the video conferencing systems. In addition we have basic requirements and recommendations as well as a check list for conducting data protection-compliant virtual conferences formulated. In addition, there were recommendations for the examination of contract processing agreements from providers of video conferencing services.422

• Lecture on “Big brother, privacy and public health – Effective enforcement of data protection regulation in times of COVID-19” on November 12 2020 as part of the (digital) German-Brazilian Democracy Forum the German Embassy in Brasilia. Brazil is currently in the process of shaping the data protection supervisory authority and was in this context at our interested in other experiences.

20.7.2 Publications

An important part of the public relations work of our authority are the publications to. The information center on our website contains a wide range of information lien, which can be called up digitally and in some cases ordered as a printed edition free of charge can become. The offer is constantly being expanded and updated, as well this year.

In addition to the activity report of the past reporting period, we have three Guide for data protection extensively revised, supplemented and in the new Have the design printed:

422 See also 1.3

• The guide “How safe is your

Smartphone?” was first released in 2008 and is now in the

3rd, updated and supplemented edition published. For the reissue was

it is particularly important to us that young people are not only aware of the known dangers

such as smartphone viruses, espionage and data theft, but

We also want to give you specific tips on what precautions you should take

can protect in the best possible way.

• The "credit agencies" guide from 2001 was in the past

already fundamentally revised several times. In the

In the current edition, the text has been adapted to the new legal situation (DS-GVO) and

been relaunched. In the guide, short, clear chapters

piteln among other things about the activities of the credit bureaus, the

requirements for data processing by credit agencies and that

Right to information and other data subject rights are described in detail.

• The guide “Handling Passwords” from 2000 was also published

this year in another updated and restructured edition.

With the increasing use of online services, it is particularly important

point out to users that data should be more secure. what is

a password manager? How is a person authenticated? which

Are there options for multi-factor authentication? What requirements

ments to a secure password should be considered? - In the brochure

These and other questions will be answered and assistance will be offered.

In addition, the brochure "Data protection for image, sound and

and video recordings. What has to be considered in the day-care center?”

in good time before the start of the new daycare year after the summer break in the 2nd edition

location appeared. With the newly revised brochure, the Senate

Administration for Education, Youth and Family and the Berlin Commissioner for
Data protection and freedom of information comprehensive about the current legal
Requirements. The above all to carriers, day-care center managers and pedagogical specialists
This brochure has already been made available to all 2,700 day-care centers in Berlin
provides.423

423 See also 4.2

Those affected and interested citizens can find information on our website
and citizens also tips on "private data protection". Here we show you how to
can avoid data traces on the Internet, what constitutes secure passwords or
how to safely use wireless networks (WLANs). We also offer help with
Asserting your own data protection rights, e.g. B. Sample letter for
sand to data processing offices. Affected persons can use these letters
contact the Berlin authorities and other bodies to obtain information about the
to obtain data stored by a specific person, correct them if necessary
or to have inadmissibly stored data deleted. We currently offer sample
write for the areas of regulatory tasks, internal security, address trading
and advertising, SCHUFA and telecommunications an.424

In addition to our own publications, we also provide information on our website
information on intensive cooperation with colleagues
other federal states and their results are available:

• The decisions of the Conference of Independent Data Protection Supervisors
Federal and state authorities (DSK): The independent data protection
Representatives of the federal and state governments meet regularly twice in the
year under the annually rotating chairmanship of a data protection
delegates to their data protection conferences. The results of these meetings

are disclosed to the public as conference decisions or resolutions

known. These documents of the DSK since 2005 as well as the joint

published papers on the practice of data protection in various

Subject areas (short papers, orientation aids and application notes)

are available to anyone interested in our information center.

• In the same way, we publish the guidelines of the European data

Protection Committee (EDPB). The EDPB is an independent European entity

direction that was set up when the GDPR came into effect in order to

to clarify rock-solid issues in the interpretation of the GDPR and thus the uniform

Application of data protection rules across the European Union

ensure. It is made up of representatives of the national

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

self-data protection/data check

data protection supervisory authorities and the European Data Protection Supervisor

wore The EDPB regularly issues guidelines on key issues of the GDPR

out of here. All documents will be successively translated into German. As far as she

have already been translated into German, these can be found on our

page to be downloaded.

20.7.3 Outlook

Due to the increase in jobs for the double budget 2020/2021, the domestic

necessary restructuring of the public relations department in our

authority to be carried out. The newly created department has been in existence since September

"Committee, press and public relations work", which can be obtained directly from the department

management.425 The individual work areas can now do better

be coordinated with each other. In particular, we now have a defined

responsibility for the supervision of the various committees and the coordination of the

countless voting procedures that have been carried out in extreme

have increased in a number of ways.

In order to get as broad a public as possible for the topics of data protection and information

to be able to raise awareness of freedom of information, in addition to the constant expansion

of our publications, in particular our digital offers

Remove. In addition, the exchange with politics and the media as well as with

citizens are intensified and promoted.

In the coming years we will also network at all levels

and strengthen cooperation, e.g. with civil society actors,

scientific institutions, schools and educational institutions

and implement new event formats.

425 See also 20.1

21 statistics for the

annual report

s

i

x

a

right

P

right

e

i.e

s

and

A

Both for the complaints submitted and for the reported data

The number of people at the Berlin Commissioner for Data Protection and

Freedom of Information (BlnBDI) received cases at a very high level.

This continues the trend of the past two years. This will be special

compared to the number of cases before the General Data Protection Regulation came into effect

(GDPR) clearly.

The presentation of the following chapter is based on the uniform criteria

teria that the Conference of Independent Data Protection Authorities of the

federal and state governments (DSK). In addition, the BlnBDI

with their reporting obligations from the GDPR and the Federal Data Protection Act

(BDSG) according to. It should be noted, however, that due to the corona pandemic

and the resulting difficult working conditions, not all processes have

are finally recorded statistically. The numbers given here stand accordingly

conditional.

21.1 Complaints

In 2020, the BlnBDI received 4,868 submissions from those affected, from which

2,430 were to be treated as formal complaints within the meaning of the GDPR.426

For the majority of the complaints, the BlnBDI opened proceedings on its own

permanence. There were a total of 1,909 procedures this year. of which

more than 80% opposed private bodies (1,656), the rest opposed public authorities

(253). In 521 cases, the complaints were not within the competence of the

BlnBDI, e.g. because those responsible have their German headquarters in a

their state had. The BlnBDI gave these complaints to the competent authorities

Colleagues in the other federal states or to the Federal Commissioner for

data protection and freedom of information.

426 See Art . 77 GDPR

274

Chapter 21 Statistics for the Annual Report 21 .2 Consultations

The number of complaints submitted to the BlnBDI has thus remained unchanged since validity

of the GDPR at a comparably high level. The graphic below shows one

Overview of the number of complaints submitted to the BlnBDI by

made towards public and non-public bodies as well as via

to other German supervisory authorities since 2017.

complaints

public bodies

non-public bodies

duties

1698

281

1222

195

2018

417

312

2017

17

88

Figure 3: Complaints 2017-2020

2455

523

2430

521

1684

1656

248

2019

253

2020

21.2 Consultations

The term consultations are all written data protection law

Information to those responsible, data subjects and the public

general administration. The focus here was on advice

affected persons, i.e. citizens, with 2,438 cases. In addition, the

BlnBDI numerous responsible persons. In addition, there is a large number of

information that is not recorded statistically.

Unfortunately, due to the corona pandemic, fewer statistically recorded

of those responsible take place.

275

Counseling of affected persons

2079

2402

2438

655

2017

2018

2019

2020

Figure 4: Consultation of affected persons

21.3 Data Breaches

In 2020, those responsible at the BInBDI will again have a lot of data

glitches reported. As explained in previous annual reports, this is due

the reporting and information obligations, which are significantly tightened in the GDPR.427 Im

During the reporting period, there were a total of 925 reports from those responsible. From that

821 were in the non-public area, i. H. mainly on private companies

take. Public authorities reported 104 data breaches to us.

Data breach reports

public bodies

non-public bodies

357

314

43

2018

52

45

2017

7

Figure 5: Data breach reports

427 JB 2018, 1.3; JB 2019, 15.1

276

1015

873

142

2019

925

821

104

2020

Chapter 21 Statistics for Annual Report 21 .4 Remedial Actions

21.4 Remedial Actions

If the BlnBDI determines a violation of the GDPR by those responsible,

it can take various remedial measures.428 In 2020, the Bln

BDI issued two warnings and 308 warnings. of the possibility

ability to revoke certifications or issue an order was

not used in the reporting period. In 47 cases, the BlnBDI imposed fines

imposed. At the end of the reporting period, the relevant procedures

however, not all of them have been legally concluded.

In addition to the cases mentioned here, a larger one was reported in the reporting period

Number of other procedures opened in which no decision has yet been issued.

Remedial Actions 2020

warnings

warnings

Instructions and Orders

Revocation of Certifications

Table 1: Remedial actions

2

308

0

21.5 Formal support for legislative project

According to the Berlin Data Protection Act, the BlnBDI has, among other things, the task the House of Representatives, the Senate and other institutions and bodies legislative and administrative measures to protect rights and freedoms to advise natural persons on data protection law. This includes both written statements as well as discussions with parliamentary groups and ordered and formal hearings in the House of Representatives and in its shot.

428 See Art . 58 para. 2 GDPR

277

In the reporting period, we advised on 33 legislative projects, e.g. B. in the event of changes to the Police Act429 and the State Hospital Act430 or in the creation of a legal basis for a citizen and Police Officers431. Some of these legislative projects were very extensive and sometimes included amendments to numerous individual laws, such as e.g. B. the Berlin Data Protection Adaptation Act EU, with which approx. 80 have been adapted to the GDPR.432

In addition, there were 12 consultations on legislative projects that would create and Amendment of legal ordinances and administrative regulations on the subject had. We also repeatedly took part in federal legislation projects together with the other federal and state data protection authorities Position, if these important projects such. B. the evaluation of the Federal data protection act concerned.

21.6 European Procedures

The GDPR stipulates that the European data protection supervisory authorities

cross-border cases.433 As part of the cooperation

On procedure, a lead supervisory authority is determined, which

investigations in the respective case.434 Other data protection supervisory authorities

den can register as affected authorities if the person responsible has a

establishment in their country or the processing has a significant impact

on data subjects in the respective country. The respective

ligated supervisory authorities closely with each other.435

429 See 3.2

430 See 5.1

431 See 3.3

432 See 17.1

433 See Annual Report 2018, January 1st

434 See Art . 56 para. 1 GDPR

435 See Art . 60 para. 1 to 3 sentence 1 and Art. 61, 62 GDPR

After completion of the investigations, the lead supervisory authority submits the

concerned supervisory authorities submit a draft decision for comment.436

In total, our authority published 24 draft resolutions this year

and 20 final resolutions. For coordination and cooperation, the eu

European data protection supervisory authorities the electronic internal market information

information system (IMI).

The table below gives an overview of the participation of the BlnBDI

the most important of these European procedures.437

European procedures

Art. 56 procedure (affected)

Art. 56 procedure (responsible)

Art. 60ff. procedure

Table 2: European procedures

388

29

44

436 See Art . 60 para. 3 sentence 2 GDPR

437 For more information and figures on European cooperation schemes see

17.2

279

280

Chapter 21 Statistics for Annual Report Appendix

Speech by the Berlin Commissioner for Data Protection and Information

ungsfreiheit, Maja Smoltczyk, on the Senate's statement

on the annual report 2018 in front of the Berlin House of Representatives

on October 1, 2020

Dear Mr President,

Ladies and gentlemen,

today we're talking about my annual report for 2018 – a little bit

later than usual, but appropriate insofar as you can also talk about the

tenschutz-Adaptationsgesetz EU, which also on today

is on the agenda – and both items on the agenda are connected by the fact that they

same event in 2018.

Because 2018 was the year in which the General Data Protection Regulation came into effect

and has brought with it enormous challenges for each of us.

But despite all the challenges, it cannot be stressed enough that

that this European legal project is a milestone

delt in a time of accelerating global digitization, in which

basic European civil rights can only be preserved

when you join forces at European level. It's a pro

project that we Europeans can be proud of - and for which we

be admired internationally.

My authority had prepared well for this turning point, but was

Increase in submissions and reports of data breaches almost overwhelmed. With

When the General Data Protection Regulation came into effect in May 2018, there was a

Triple to quadruple the number of complaints, which are still on the

has leveled off at three times the level. The number of reported data breaches

and the number of requests for advice has multiplied and is at a high level

level remains.

281281

Appendix At the same time, the professional demands on my employees increased

ners and employees extremely, as our work has now become a big one

Part in the European area takes place in close cooperation with the rest

EU regulators. And all this at first in 2018 only marginally-

slightly increased staff.

But we could see that my authority had prepared the content very well

was. In order to be prepared for this day, we had the structure of our

authority and our working methods have been fundamentally rethought and redesigned

and together with the other German and European supervisory

authorities have developed completely new methods of cooperation. And we have

done everything in our power to advise companies and authorities

and to accompany the transition to the regulation.

Nevertheless, the implementation of the General Data Protection Regulation represented a huge

tour de force for my house. It wasn't just the number of inquiries that

had to be taken, there was also the fact that the cases in 2018 were partly based on "old"

and partly to be assessed according to the "new" law. With the new sanctions

We have also been given powers to investigate violations of the

Effectively punish data protection, at least in the private sector

be able. The use of these new sanction instruments is also very high

Requirements for my authority.

I am very fortunate to have highly motivated experts at my side

who carry out their work with a great deal of commitment. For this use would like

I would like to thank my employees very much!

– At this point I would also like to thank you, the one with the last one

Double household provided for a staff reinforcement of my house from 2020

that enables us to meet the increased requirements better and better

to become right.

In terms of content, we were again busy with a colorful bouquet of topics in 2018:

The topics ranged from the illegal exchange of social data, the missing

Deletion of data in the clinical cancer register and in Berlin hospitals

sern, about video and audio recordings in the classroom, the storage of

data from delivery services to the scoring of judges and electronic

Appendix niche health record. Children's data protection rights have a lot of room

taken.

Especially in the field of day-care centers, due to the new European law,

Uncertainty about the data protection-compliant handling of personal data

big.

And some of the topics are still with us today:

One of them was the judgment of the European Court of Justice on the Facebook fan pages, with which the court found that the fan page operators together with Facebook a data protection responsibility for the carry data of their visitors processed on their pages. This affects many Responsible in this city immediately.

Another topic was the storage practice of the Berlin police and the usual access to the police database POLIKS.

One issue that has been very close to my heart since the beginning of my tenure is that Strengthening the data protection competence of children and young people. With our In the spring of 2018 we made an offer on the children's website www.data-kids.de starts, which meets with great encouragement from children, teachers and parents and for that we were even nominated for the German children's software award TOMMI.

In the area of freedom of information, I was particularly concerned with an issue which will certainly accompany us for many years to come: the digitization of the public Administration. Automated decisions are increasingly being made with the help of algorithms and artificial intelligence - and largely intransparent rent. However, an administrative decision must always be verifiable and therefore be traceable, controllable and understandable. The conference of information Federal and state commissioners for freedom of action have a groundbreaking position paper, which was later published in an abbreviated form by the International conference of freedom of information officers.

Finally, allow me a brief outlook on the data Protection Adaptation Act EU, which is also on the agenda today.

Appendix I limit myself here expressly to the points that relate to my year

have a report. – It is good that finally – two years after taking effect

of the General Data Protection Regulation - the adaptation of the Berlin state law

to European law. Unfortunately, there are important

which are not yet resolved by this law.

In my 2018 report, I pointed out that there are still none

Data protection regulations for the Berlin House of Representatives. Although here too

personal data is used in-house, there was and is no

ner kinds of control options and no regulations for data subjects, their

assert data protection rights. This problem is exacerbated with in-

entry into force of the Data Protection Adaptation Act because the Berlin Parliament

much more comprehensive powers are to be granted in the future, also with

handling sensitive data. This is an urgent need to

be served!

In addition, there are relevant amendments to the Berlin Data Protection Act

need for protection in the area of data protection supervision and effective security

of data subject rights. Several regulations do not meet the requirements

General Data Protection Regulation and should be reconsidered.

I very much hope that the coalition factions will announce this law

to be evaluated and adjusted separately before the end of the election period.

Ladies and gentlemen, there is still a lot to be done. Just recently, the European

Court of Justice stated in its “Schrems II” decision that the previous

Legal bases for data transmissions in third countries and in particular in

the USA can only be used to a very limited extent. That represents economy, administration

tion and us, who have to push this through, are facing huge challenges.

We face this task and at the same time promote it, also as a big one

Opportunity for more digital independence in Europe. Here we must

work together.

Thank you for your attention!

284284

Appendix Glossary

Table 3: Glossary

glossary	
2 factor	
authentication	
subscription trap	
customer relation	
ship management	
(CRM) system	
Anonymous/Pseudonymous	
Proof of an individual's identity via two of the three	
the following features:	
1. Possession of a device exclusively for this	
person has	
2. Knowledge of a secret (such as a password) that	
known only to her	
3. Biometric characteristics of the person like theirs	
Fingerprint.	
Colloquially refers to a dubious	
business practice on the Internet, among consumers	
accidentally subscribed to a paid subscription	
walk. Such an offer is usually structured in such a way	

builds that consumers in the mistaken assumption

be left that the services provided there

are free of charge, but actually incur costs. Before

Consumers using the Services must use their

provide personal information. A little later reports

the provider with them and requires z. T. high money

sluggish for the supposedly completed subscription.

A CRM system is a software for managing

management of customer relationships.

Anonymous data can no longer be assigned to a person

be assigned. In the case of pseudonymous data, this is a

agreed third party possible under pre-determined

Conditions.

apartment

Application program for mobile phones.

Art. 29 group

Chief Information

Security Officer (CISO)

cookie

Cookie Banner

dashcam

DKIM signature

Group according to Art. 29 European Data Protection Directive,

made up of representatives from all European

ic data protection authorities. She has

advisory function; primarily against the euro

European Commission, but also towards other

data processors within the European Union.

Responsible for the development of security

guidelines for alignment, planning and coordination

tion of measures to ensure safety

of information processed by an organization

as well as for the evaluation of the implementation of these measures

men and the remaining risks.

A cookie is a text file that is used to communicate with a

Website related information on the computer

to save the users locally and

to transmit back to the website server on request

tell This means that users can

Recognized and visited websites and times

of the visit.

Banners are graphic or animation files that are included in the

are integrated into the website and either appear at the edge

appear or lay across the webpage. in the

gel contain this advertisement. Cookie banner included

usually notes on the use of cookies and are

usually provided with a simple "OK" button.

A dashcam is a video camera that is

dashboard or on the wind

protective window of a vehicle is attached.

DKIM stands for Domain Keys Identified Mail. In doing so

is it a method of e-mail authentication

tion. DKIM adds a digital signature to emails that

assigned to the sender domain and for all

outgoing e-mails is used. This is a technique that

Forgeries of the e-mail senders or the home

makes recognizable from e-mails. Forged or counterfeited

double opt

in procedure

GDPR

DSK

In this way, e-mails can be automatically rejected or

t treated, unadulterated e-mails accepted and as

to be treated genuinely.

Double opt-in procedure refers to a process in which

the user after entering their contact data

th in a distributor this in a separate second

have to confirm the step again. Mostly this becomes

an email message asking for confirmation

sent the given contact details. Dane-

However, confirmation can also be sent by SMS or telephone

done phonically.

European General Data Protection Regulation − The data

General Data Protection Regulation (GDPR) is a regulation

tion of the European Union, with which the rules for
Processing of personal data by private
Companies and public bodies standardized across the EU
become light. This is intended on the one hand to protect personal
personal data within the European Union
ensured, on the other hand free data traffic within
guaranteed within the European internal market
will. The regulation replaces that of 1995
originating directive 95/46/EG for the protection of natural
cher persons in the processing of personal
data and free data traffic. She is already on
came into force on May 24, 2016, but was suspended due to a
two-year transitional period only effective on May 25, 2018
sat. Since then it has been in all member states of the Euro
European Union directly applicable.
The Data Protection Conference (DSK) consists of the independent
pending federal data protection supervisory authorities
and the countries. It has the task of data protection
to uphold and protect fundamental rights, a unity
application of the European and national data
to achieve data protection rights and work together for his
to enter into further development. This is done by name
through resolutions, resolutions, guidance
ments, standardizations, statements, press releases
decisions and determinations.

Glossary Glossary

EDSA

EC / Recital

oath

end-to-end

encryption

The European Data Protection Board (EDPB) is a

independent European body that contributes to

common application of the data protection regulations in the

whole European Union contributes and the cooperation

work between the EU data protection authorities

that. The EDPB consists of representatives of the national

data protection supervisory authorities and the European

Data Protection Officer (EDPS).

Recitals are declarations of the European

Legislature to the actual legal text, which this

regularly contributed to European legislation

be added.

"Electronic Identity"; this is one

electronic proof of identity (with chip), with its

Help electronic operations can be performed.

The content of a data transmission is encrypted in such a way

that only the recipient specified by the broadcaster

decrypt the data, d. H. readable again

can. intermediate stations such as B. E-mail offer

Users, on the other hand, only see encrypted data.

fan page

firmware

geodata

GovData

Facebook fan page: A Facebook fan page is the

sence of brands, companies, organizations and

Public figures in the social

Network Facebook, which serves the company

or the brand etc. in the network using the network

means of communication provided by the factory

to market, e.g. B. by the page of Facebook Nut

Zer*innen recommended or in the "circle of friends" of

users is shared. The fan page is also a public

public profile and can be viewed by people outside of the

network can be retrieved; it will be

indexed by major search engines, i. H. in the result list

listed. Unlike the profile page, which is used by private

people is used, it is not about the "friend-

den", but about using the page z. B. directly with

to communicate with customers in the network or "fans"

to collect.

A device's firmware is software stored in electronic

niche devices is embedded to their basic

to ensure function. It is by user

not or only with special means or functions

NEN interchangeable. Firmware is functionally fixed with the

hardware connected; one is not without the other

usable.

Digital geological data, e.g. B. in navigation systems

be processed.

Data portal for Germany, a central and

Uniform content-related access to administrative data

from the federal, state and local governments, which these in

made accessible to their respective open data portals

to have.

GPS / GPS transmitter

global positioning system; dt.: Globales Positionbe-

mood system.

hash function

hash value

IMI

informed

consent

integrity

A cryptographic hash function is

to a mathematical calculation rule that consists of

any output data such as a document

or just a word or a phone number

calculates a unique check value with a fixed length.

This calculation is not reversible - from the test

cannot recalculate the output data

become. When repeated calculation with the same

However, the output data is always the same

test value.

The hash value is the result (the check value) of the application

Creation of a [above] cryptographic hash function. at

this is a mathematical calculation

ment rule that can be derived from any output data such as

e.g. a document or just a word or

a phone number with a unique hash value

fixed length calculated.

The Internal Market Information System (IMI) is a multi-

language online tool that facilitates the exchange of information

between authorities facilitated at the practical

implementation of EU law. The data-

safety supervisory authorities of the EU member states

men thus cases where a cross-border

processing of personal data is based.

“Informed Consent” means consent

declaration of consent, in which the users

detailed, complete information about the planned

processing of your data, its type, scope and purpose

have then clearly consented to the processing of these.

Maintaining the integrity of data is understood to mean

their protection against unauthorized modification or removal

protection, against accidental loss or destruction and

against accidental falsification.

IP address

Internet protocol address = the address of a computer

ters on the internet.

IT architecture

coherence method

link

Market place principle

messenger service

metadata

Determining the composition of information technology

nical systems from different components and

their interaction.

If no consensus can be reached in the one-stop-shop procedure between

be found by the supervisory authorities involved

the European Data Protection Board meets

(EDPB) as part of the consistency mechanism

Decisions. In addition, in the coherence procedure

with the aim of uniform application of the DS-

GMOs also opinions of the EDPB − for example to determine

standard data protection clauses − coordinated.

Link or jump to an electronic document

ment.

The GDPR is applicable as soon as a company

Goods and services for people in the euro

European Union offers or the behavior of citizens

observed by the public and in this

menhang personal data processed. Of the

The scope of the GDPR also includes

Non-European companies based on the European

market are active even if they have no establishment in

of the European Union have. Through the market place principle

zip aims to level the playing field for all

companies are created that are based on the European

offer goods and services on the general market.

Telecommunications service involving two or more

Participating text messages (possibly also audio or

video messages and other files) so exchange

ensure that the news is as immediate as possible

reach the recipient.

The data arising from a data transfer

is divided into content data - e.g. the text of a

E-mail - and all other so-called metadata that the com-

relate to communication circumstances, d. H. time, absence

the, recipient, locations for mobile devices as well as

technical addresses/identification numbers of the

cation used devices.

Glossary Glossary

microblogging

Neural Networks

One stop shop

open data

Microblogging uses short SMS-like texts

created in a blog or short message service

to be set. It doesn't work with microblogging

rum to go thematically in depth, but within

short time and without much effort messages of all

way to produce.

Artificial neural networks are usually attached to the

organizational principles and the learning processes of

human brain oriented computer models.

The one-stop-shop principle is intended to ensure that

of the EU-based company in the data

protection authority on site a single point of contact

found. This should address the respective data protection issues

with the other European data protection authorities

voices. The companies should be so of the effort

be relieved to deal within the EU with different

the data protection authorities to deal with

senior For companies with branches in different

the member states is the supervisory authority at the registered office

head office is the central contact person.

However, the GDPR does not only see the one-stop shop for

the companies, but also for the citizens

citizen before. These too can be uncomplicated

their local regulator in their local language

also complain about foreign companies.

Databases that the citizens as well as

of the economy without restriction for free further distribution

be made freely accessible.

Open government

Opt In / Opt Out

opt-out model

pixel

"Open Government" describes open government and

Administrative actions in particular through:

• Transparency, e.g. B. about procedures and decisions

and access to information

• Participation, for example in the form of citizens' dialogues or

consultations,

• Cooperation between government and non-government

organizations as well as interdepartmental and cross-

grasping,

• Use of new technologies to improve the

governmental and administrative action.

Opt-in means that data processing is only permitted

is when the data subject expressly consents to it

has decided, i.e. usually given their consent

gave. In the case of an opt-out procedure, on the other hand,

the data subject take explicit action to

prevent data processing.

"Opt-Out Model" means a procedure that

A consent is accepted if this is not within a

objected to within a predetermined period of time.

Small graphics on websites, mostly only 1×1 pixels

measure and when calling up a website from a server

to be loaded. The download is registered

and can be used for evaluations in the field of online marketing

ketings are used.

Pre-recording function Denotes the recording and storage of a pre-

granted time range in an endless loop, i. h., it

is a recording function in which

just a few seconds before pressing the recording

button, the data is saved.

Privacy by default

Products are made with the most privacy-friendly

delivered with presets.

Privacy by design

profiling

pseudonymize

public consultation

The manufacturers already take data protection into account

in the manufacture and development of products.

Profiling includes any type of automated evaluation

tion of certain personal aspects of a natural

person to understand. About these aspects can

work performance, the economic situation, health

safety, personal preferences, interests, reliability

activity, behavior, whereabouts or possible

change of location belong to a person. The aim of the profiling is

it to carry out an analysis in this regard or a

to make prediction. Profiling comes z. B. in advertising

area and for the initiation of contracts,

but also the police, for example, is increasingly relying on

relevant prediction methods.

Pseudonymization is the replacement of identifying

information such as name, address, date of birth or others

clear identifiers or characteristics through an

their designation (e.g. a serial number) in such a way that

that an inference to the person without knowledge of

assignment rule not or only with disproportionate

is possible according to effort.

German: Public consultation. Before the adoption of

The European Data Protection Board provides guidelines

(EDSA) conducted public consultations to

views and concerns of all stakeholders and

to hear citizens. In general, guidelines

before their final adoption on the Internet

published on the EDPB website. Then there is usually

for six to eight weeks the possibility of the guideline

to comment. Mainly make economic

associations and companies benefit from this opportunity

need. However, the ESDA also receives feedback from

social groups and citizens. To

The EDPB decides during the consultation phase

which change requests are taken into account.

Source code

The program code (technical basis) of a software

were.

ring memory

score value

rating level

sensitive data

Social Plugins

A ring memory stores data continuously in a

certain period of time and overwrites it when it expires

a predetermined time again to free up the disk space

release for new data.

Credit bureaus collect information about

people, especially about their economic

situation and their payment behavior. Calculate from this

a numeric value indicating the ability to pay

ness (creditworthiness) of the person concerned should reflect the

so-called score value. Depending on this score value

the persons concerned then a probability

assigned, with which you settle open receivables

or not pay, so-called rating level. This information

tion, companies can retrieve before signing contracts

finalize them at a future performance

of the contractual partner leave

have to.

Special Types of Personal Data. for this purpose

hear information about ethnic origin, political

opinions, religious or philosophical beliefs

genes, union membership, health or

xuallife.

Connect social plugins or social media plugins

Websites or apps with social networks. operating

and operators insert a program code into the

Enter the source code of your website or app, which automatically

sends data to the operator of the social network

and retrieves from that data. The operators of the social

Network find out what the visitors are for

and visitors of the website are interested, and can

create personality profiles by means of profiling as well as

personalize advertising. For example, an operator can

show that acquaintances of the website visitor

of the website visitor the website with "Like"

have marked. In particular, social plugins can

their considerable number of visits due to network effects

for websites and subsequently regularly significant

sales are generated.

Software-as-a-

Service (SaaS)

social sphere

tracking

With Software-as-a-Service (SaaS), the provider operates

the servers and the software for the respective service.

Users only have access to the services

of this service, mostly just the surface, often im

Web browser is displayed. It's about

a typical cloud service. In contrast,

advertise users or their institutions in the classic

Model software and servers and operate the software

even.

The social sphere is the area in which man

in exchange with other people. of this

is both the private and the professional area

includes.

Tracking is in the understanding of the data protection supervisory

authorities the logging and evaluation of behavior

tens of visitors to websites

or apps for generally cross-website

tracking. The areas of application range from

a pure range measurement via statistical

evaluation according to browser, operating system, language

settings as well as country of residence and tests for

user-friendliness of websites up to de-

tailored observation and recording of all

mouse movements and inputs as well as for website

and cross-device creation of usage and

personality profiles for advertising purposes.

Tracking / Cookie Walls Preventing the use of a website if you do not

accept cookies.

behaviour rules

English: Code of conduct. It is an in-

instrument of self-regulation. According to Art. 41 GDPR

Associations and other associations can

draw up rules with which the application of the DS-

GMO is specified. task of the supervisory authorities

to encourage the development of such codes of conduct

and to approve.

traffic data

wearable

WIFI base stations

WiFi tracking

Technical information when using a

Telecommunications service incurred, such as a

phone call calling and called phone number,

Beginning and end of the connection and telephone calls in the

Mobile network also the location. Also as connection

called data.

Wearable computers, or wearables for short, are compu-

ter that are so small that they neither fill a space

len still need a desk, but z. B. as

bracelet and glasses worn or tucked into clothing

can be worked. During the application they are

attached to the user's body and often directly

connected to the internet. So e.g. B. a blood pressure

measuring device that is permanently or over a longer period of time

Period worn on the arm, quite as a device

be referred to as wearable computing.

device for wireless data transmission; is mostly at

wired Internet access to

allow nearby devices to use the Internet

enable without having to connect cables.

A technique with which the movement of people

can be tracked using location data that

using the smartphone of these persons

be caught.

Index D

302

303

Information desk of the Berlin Commissioner for Data Protection and Freedom of Information

Activity reports: The Berlin Commissioner for Data Protection and Information

heit submits an annual report to the Berlin House of Representatives and Senate

to present about their activities. In addition to current technical and legal developments

developments is about key issues and individual cases from the respective

reported to business areas. The activity report is also available as a brochure

re published for the citizens.

Guides and leaflets on data protection: In these publications we have

practical information on recurring questions in everyday life together

set. We want to enable people to use their data

to exercise property rights or their right to access information independently.

Legal texts: General Data Protection Regulation, Federal Data Protection Act and

Berlin Data Protection Act as a printed version or to download.

Brief papers, guidelines and application notes: The independent

Federal and state data protection officers deal intensively with

the new legal bases and their requirements and agree on a uniform

common point of view. The results of this process are common short

piere to the GDPR, guidance and recommendations that the conference of

independent data protection supervisory authorities of the federal and state governments (DSK)

released.

Guidelines: The European Data Protection Board (EDPB) consists of representatives

of the European data protection authorities and the European data

protection officer. It publishes guidelines, recommendations and so-called best practices

Proceedings on key issues of the GDPR. As far as these are already in German

che translated, they can be downloaded from our website.

All information material is available on our website and some also in

available in printed form. You can find an overview at www.datenschutz-berlin.de.

We provide a comprehensive range of media-educational information at our

available on the website www.data-kids.de. There you will find children, teachers and parents

extensive materials to help you better yourself in the world of data protection

to find your way around.

The 2020 Annual Report includes the following key areas:

Data protection issues related to Corona; International traffic

after the "Schrems II" decision of the European Court of Justice; use of

video conferencing systems; Digitization of schools - BER 2.0?; Kickoff for

the certification