annual report

the Berlin Commissioner for Data Protection and

Freedom of Information as of December 31, 2018

The Berlin Commissioner for Data Protection and Freedom of Information has

House of Representatives and the Senate an annual report on the results of their activities

activity (§§ 12 Berlin Data Protection Act, 18 Para. 3 Berlin Information

Freedom of Action Act). This report closes on March 23, 2018

submitted annual report 2017 and covers the period between 1 January

and December 31, 2018 onwards.

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

www.datenschutz-berlin.de

imprint

Publisher:

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

a notice

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

different technical terms. The color highlighting of words in the text (e.g.

Market location principle) indicates that these are printed in the glossary.

8th

List of abbreviations

List of abbreviations

Official Journal of the European Union

General safety and order law

Specialist procedure aid online

building code

OJ EU

ASOG

BAO

BauGB

BDSG (old version) Federal Data Protection Act (old version)

BEEG

Federal Parental Allowance and Parental Leave Act

Civil Code

Civil Code

Federal Court of Justice

BGH

BKA

Federal Criminal Police Office

Federal Criminal Police Office Act

FCAG

BlnBDI

Berlin Commissioner for Data Protection and Freedom of Information

BlnDSG (old version) Berlin Data Protection Act (old version)

BSI

BVerfG

BVerwG

BVG

DAkkS

DB AG

Drs.

DPIA

DSK

GDPR

EDSA

EGBGB

EGovG Bln

EU

ECJ

GG

GPS

GVBl.

AMLA

HIS

Federal Office for Security in Information Technology

Federal Constitutional Court

Federal Administrative Court

Berlin transport company

German Accreditation Body

Deutsche Bahn AG

printed matter

Data Protection Impact Assessment

German Data Protection Conference

European General Data Protection Regulation

European Data Protection Board

Introductory Act to the Civil Code

Berlin e-government law

European Union

European Court of Justice

constitution

Global positioning system

Law and Ordinance Gazette for Berlin

Money Laundering Act

Reference and information system of the insurance industry

List of abbreviations

IBAN

IFG	
IFK	
IMI	
INPOL	
ISBJ	
ISO	
IT	
IWGDPT	
International bank account number (International Bank Account number)	
Berlin Freedom of Information Act	
Conference of Freedom of Information Officers in Germany	
Electronic information system of the European authorities	
Information system of the state police authorities in Germany	
Integrated software Berlin youth welfare	
International Organization for Standardization	
information technology	
International Working Group on Data Protection in Telecommunication (so-called Berlin Group)	
annual report	
JB	
JHA Directive	European Data Protection Directive for Justice and Home Affairs
KJHG	
KTDat	
ArtUrhG	
KV	

KWG

LABO

LOCATIONSo

LAGetSi

Child and Youth Welfare Act

Communications Technology and Privacy Committee

Art Copyright Law

Association of Statutory Health Insurance Physicians

Banking Act

State Agency for Civil and Regulatory Affairs

State Office for Health and Social Affairs

State Office for Occupational Safety, Health Protection and Technical

security

State Civil Service Act

state social court

State Administration Office

Maternity Protection Act

Higher Administrative Court

Administrative Offenses Act

Law regulating participation and integration

State police system for information, communication and

processing

Personnel Structure Statistics Act

social code

Standard Privacy Model

criminal code

Code of Criminal Procedure

LBG

LSG

LVwA

MuSchG

OVG

OWiG

PartIntG

POLICIES

PSSG

SGB

SDM

StGB

StPO

List of abbreviations

TKG

TV L

UIG

UWG

VBB

VDV

WP

ZDRL

Telecommunications Act

Collective agreement of the countries

Environmental Information Act

Unfair Competition Law

Transport association Berlin-Brandenburg

Association of German Transport Companies

working paper

Payment Services Policy

11

12

Introduction Introduction

On May 25, 2018, the motto was "And action, please!".

The General Data Protection Regulation (GDPR)

became effective. And despite all prophecies of doom

in a previously quite overheated

ten public debate that fueled fears

and scandalized alleged pitfalls,

it runs surprisingly smoothly. Of course there are teething problems and

Security in and with the new EU-wide binding data protection law. This

but can in the case of the complete creation of a new legal area on a European

level - and that's what it's all about - still without case law and

practical knowledge shouldn't be any different. Now after almost a

year has passed, everything already appears clearly in a different light.

Despite all the prophecies, the GDPR has learned to walk. This shows

above all due to the enormously high number of complaints that has persisted to this day,

the volume of requests for advice and the number of

ten data breaches.1 Although we were prepared for a considerable amount of extra work,

However, our expectations became clear, especially in the first few weeks after the

entry into force of the GDPR, significantly exceeded. To come in on the tide-

to cope with the calls at least somewhat, we initially set up one

DS-GVO telephone hotline for those seeking advice, through which the most pressing questions

could be answered immediately. And to this day, the

Coping with the significantly increased workload is a challenge

represents my authority only thanks to the extraordinary commitment of my

employees stand the test. There is no relief in sight.

It is unmistakable that the new set of rules places greater emphasis on data protection

focus of those responsible and, above all, the citizens

ger has raised enormous awareness of data protection. I rate this development as

Success, especially since the times are on the threshold of digitalization of our complete

1 See 1 .2 and 1 .3

Introduction Lifeworld are by no means easy for data protection. The hype of the

Subduing gitalization is mainstream, and concerns or references to

Problems and intolerances are only too likely to be handicapped by this

dismissed by modern development.

Algorithms are increasingly deciding which messages to send

reads which partner you meet or even which partners

ei one chooses. And also in the public administration have under assistance

by algorithms and so-called artificial intelligence

automated decisions are being made. All of this has happened so far

Extremely non-transparent. But only who the data basis, the sequence of actions

and the weighting of the decision criteria knows, the legality

review of decisions. For this reason I consider it urgent

required, automated decisions are also comprehensible, controllable

to make it clear and understandable. I therefore very much welcome the fact that a large part

of the members of the Conference of Freedom of Information Officers in Germany

country at the suggestion of the freedom of information officers of Berlin, Bremen and

Schleswig-Holstein has formulated requirements in a position paper for

public authorities even more consistently than before to a transparent and

responsible use of algorithms and artificial intelligence

obligations.2

Digitization is taking democracy and the rule of law to an extreme

test. An occasional critical pause is therefore more important

than ever, given the high pressure to adapt in our rapidly accelerating

But everyday life is also extremely difficult. It is all the more significant, already

Educate children of primary school age about how to handle their own data

to teach them how they themselves can influence what happens with

what happens to their data.3 The most important prerequisite for this is to be critical and

Stay active with regard to all information and messages from the net and

acquire a basic knowledge of the mechanisms of the Internet. my authority

has therefore not only the teaching of media skills, but also

of media maturity written on the flag. It is our goal that more

2 See 13.1

3 See 5.5

Introduction and more children not only use digital media competently, but also use them

also use it reflectively. Incidentally, this also includes

if not usable – for example search engines, the search queries

do not delete and create usage profiles. On our children's website

we developed a wide variety of educational materials for elementary school children and parents

and also teachers. And also using the together with the

Senate Department for Education, Youth and Family in November 2018

given new edition of the brochure “I am looking for you. Who are you?”4 we hope

to be able to contribute to the fact that children are smart and self-confident

Discover the online world.

It turns out that design is the key! Data protection is not a brake for the

Progress, it is rather the necessary corrective to keep technical developments

development in accordance with our fundamental rights. A development

only serves the people if their rights are not carelessly disposed of

tion. Also the new European General Data Protection Regulation

is to be understood in exactly the same way. It was not approved by the European institutions

designed to formalize people's lives and enhance their

limit opportunities. It is exactly the opposite: the basic data protection

order is the European answer to an increasingly rapid and global

developing digitization of all areas of life. It offers citizens

Citizens for the first time enforceable instruments throughout Europe to assert their rights

also to enforce against globally operating companies. Of course is

not easy and many things still have to be specified in detail. but

it is an extremely important step and, in my firm belief, the only one

promising path. My authority and I will therefore continue to work together

get actively involved when it comes to finding solutions to our de-

to preserve democratic and free rights and to exercise these also in the future

to ensure the future.

Berlin, March 28, 2019

Maja Smoltczyk

Berlin Commissioner for Data Protection and Freedom of Information

4

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

competence/2018-BlnBDI-Broschuere_Soziale_Netzwerkde .pdf

15

Introduction 16

Chapter 1 Focus 1 .1 Processing of cross-border cases according to the GDPR

1 focus areas

1.1 Handling Cross-Border Cases

according to the GDPR

Due to the General Data Protection Regulation (GDPR), the work of our

Authority fundamentally changed. This applies in particular to the processing of

Complaints brought to us.1

What is new is that we not only receive complaints against Berlin companies and

hear edit. According to the General Data Protection Regulation, each data subject has

Person has the right to complain, in particular to a supervisory authority in the member

to complain to the European Union (EU) state where your usual

residence or place of work or where the alleged

shock has occurred if it considers that processing of it

relevant personal data violates the GDPR.2 It's coming

no longer on the fact that the processing body is in the area of responsibility

supervisory authority is established. Rather, an affected person should

In principle, you can contact any data protection supervisory authority throughout Europe.

All incoming complaints – but also all cases that we have ex officio

take up - are therefore first checked by us to see whether they are a so-called border

concerning data processing3. This may be the case when the

or the person responsible is established in more than one EU Member State

and the processing takes place in several of these branches. Even if

the person responsible has only one branch in the EU, one

cross-border processing if the processing is significant

affects data subjects in more than one Member State or

may have. It is therefore sufficient if, for example, the service of a German

1 For the general handling of complaints see 1 .2 .

2 type . 77 para. 1 GDPR

3 type . 4 no. 23 GDPR

17

online retailer to citizens in Germany and Austria

tet and potentially significantly interferes with their data protection rights.

If there are indications of cross-border data processing,

all necessary information about the case will be stored in an electronic

on system of all European supervisory authorities (IMI). Check these

whether they are the lead or affected supervisory authority in the case, and

report back accordingly. Cases, in

where we are the lead or an affected supervisory authority. about this

ascertainable is a constant observation of the information system and a

systematic examination of the cases reported there required.

The lead supervisory authority takes over the further investigations

the respective case. The supervisory authority with which the complaint was originally lodged

has been received is in any case an affected supervisory authority. she has the

complainant or the complainant regularly about the status of

processing.4 The electronic information

exchange between supervisory authorities. Necessary translations will be made

performed by the supervisory authorities, so that those affected have no

parts arise.

After completing the investigation, the lead supervisory authority drafts

a final decision in the case of a complaint and communicates this to all

affected supervisory authorities. They have four weeks to submit the draft

review.5 Within this period, you can lodge an objection to the draft.

If no objection is raised, the lead supervisory authority issues the decision

divorce towards the person responsible. This person takes the necessary

measures to prevent processing in all branches in the EU

with the decision of the supervisory authority.6 The supervisory

authority that received the complaint shall notify the

the complainant about the outcome of the proceedings.

4

5

6

kind . 77 para. 2, art. 57 para. 1 letter f GDPR

kind . 60 para. 4 GDPR

kind . 60 para. 10 GDPR

If an affected supervisory authority objects to the draft, it must

they justify this. If no agreement is reached, the lead

competent supervisory authority initiated a dispute settlement procedure before the European

tenschutzausschuss.7 This procedure is intended for the uniform application of the

GDPR across the EU. The European Data Protection Board

then takes a binding decision in the respective matter.8 This

Decision includes all aspects that were the subject of the objection, in particular

the question of whether there has been a violation of the GDPR. The lead

On the basis of the decision, the supervisory authority shall then take

but no later than one month after notification, the decision

tion to the person responsible.9 The supervisory authority at which

the complaint has been filed, must accordingly the complainant

or inform the complainant.

As the lead supervisory authority, we ourselves already have drafts for

Decisions with the supervisory authorities concerned in the described

drive tuned. No objections were raised to the drafts,

so that work level operations could be completed. Our decisions

As a result, we have obligations towards those who operate across borders

those responsible based in Berlin. The complainants were about

informed of the result of their entry.

1.2 Complaints handling under the

GDPR

Handling complaints about privacy violations by public

or private bodies was already one of the legal

common tasks of the supervisory authorities. Even after the European

According to German law, it is one of their duties to deal with complaints from those affected

7

8th

9

kind . 60 para. 4 GDPR

kind . 65 para. 1 letter a GDPR

kind . 65 para. 6 GDPR

to engage persons, to investigate the subject of the complaint and to

inform the data subject of the result of this investigation.10

Due to the sharply increased attention to this with the application of the GDPR

The number of submissions and complaints also increased on the subject of data protection

at the Berlin Commissioner for Data Protection and Freedom of Information by around

fourfold. It can be assumed that the number of entries will

stabilized at a comparably high level in the future, since no significant

there has been a significant drop in submissions. This is due in particular to

that the competence of our authority has expanded considerably. were before

we only for the processing of complaints against Berlin authorities and

company responsible. The so-called market place principle expands the responsibility of our

re authority on all positions that Berlin citizens goods

and offer services or observe their behavior.11

Through the legal framework created with the GDPR at European level

When dealing with complaints, not only the responsible

Distribution of supervisory authorities for data protection within Germany

countries, but all of Europe should be considered. The GDPR would like it to

make it easier for citizens to protect their privacy without unnecessary hurdles

Use data by enabling them to speak in their own native language

che and to submit their complaints to the local supervisory authority. It is

now the task of the supervisory authorities to assign responsibilities to one another

clarify and work together constructively. If it is a cross-border

progressing complaint (e.g. because there are affected persons in several

EU states or a company operates in several states), their

Processing in coordination with the supervisory authorities of the countries concerned.12

For citizens who want to know more about Berlin companies and authorities

complain, our authority remains throughout the entire procedure

the contact person on site and regularly provides information about the respective

Status.13

10 kind . 57 para. 1 letter f GDPR

11 art. 3 para. 2 GDPR

12 See 1.1

13 art. 78 para. 2 GDPR

We receive complaints and submissions primarily by email, often by post

and partly by fax or in person. Many citizens

Fortunately, citizens also use this at www.datenschutz-berlin.de/

complaint.html provided complaint form for your input, what us

processing easier in most cases. Because of the high number of

Submissions from the end of May of this year have meanwhile been delayed by us

acknowledgments of receipt usually sent within two weeks

around some time. The initial backlog could not be proportional to the

Input volume of increased personnel key in the service point citizens

inputs through weekend work and the temporary secondment of employees

be eliminated from other areas for the time being. However, this led to

Work in the other areas affected was left undone, since there was no personnel

compensation was present. Given the significant increase in submissions,

Proper and timely processing of citizens' complaints with the

available human resources are no longer affordable.

In terms of content, the complaints are closely based on those rights that

data subjects from the GDPR (as previously to a similar extent from
Federal Data Protection Act a. F.) are guaranteed, but not limited
to this. Many Berliners are interested in the private ones
Companies and public bodies store data about you and
submit an application for self-disclosure,14 which unfortunately is often incomplete
or is not answered correctly within the prescribed period. Often will
at the same time also requests the deletion of their own data; also this one from the
GDPR guaranteed right15 is unfortunately often violated. Some internet companies
Although men provide for a deletion option with regard to the customer account.
However, in some cases the stored data will continue to be stored
and used. Many people also complain about the general escalation
Collection of your data by authorities, private companies, medical practices or other
other people (such as your landlord or landlady). In numerous cases
these citizens have the right to object to the
processing of one's own data,16 in the enforcement of which we inform the data subject

14 art. 15 GDPR

15 Art. 16, 17 GDPR

16 art. 21 GDPR

stand by as well as in the event of a data processing agency violating the
Obligation to inform data subjects about data processing taking place
ments.17
The right to data, newly created for data subjects with the DS-GVO
portability, according to which responsible bodies can take their own data with them
must enable,18 or the right not only on the basis of an automated
to be subject to a specific decision before processing the data,19

make up only a very small part of the entries so far.

In many cases there is not necessarily a bad will behind a possible

present violation of data protection rights. We are often

Difficulty reported violations of the law eliminated shortly after our intervention.

In the case of less serious or immediately corrected misconduct

we usually leave those responsible with a warning and

refrain from further action.20 For more serious violations, we can

resort to other measures such as fines.21

Last but not least, the complaints we receive also serve as a measuring tool

for what is particularly common for citizens at the moment. Equal-

At the same time, they are an indicator of which business areas or districts

due to a large number of submissions, a negative development

observed and if necessary - with the means given to us - also stopped. we

therefore encourage all Berliners to continue to support us through the

Reporting data breaches to assist in combating them.22

17 art. 12, 13 GDPR

18 art. 20 GDPR

19 art. 22 GDPR

20 kind. 58 para. 2 letters b GDPR

21 See Chapter 11

22 data-protection-berlin.de/complaints.html.

1.3

Obligation to inform in the event of data breaches

The new law23 sees a significant expansion of the information obligations in the

compared to the previous legal situation24 and now applies equally to non-public

public and public bodies of the State of Berlin.25 Previously, in non-public

public area only certain categories of data such as health data

and bank account information covered by the reporting requirement, in public

There was already a reporting requirement for all types of data, in both areas

However, the obligation to report existed only in the case of impending serious impairments

fulfilment of the rights of those affected.26 Now opposite the supervisory authority

both in the public and non-public area, any violation of the

Protection of personal data notifiable. This data breach

is defined as "a breach of security that, whether accidental or unlawful

moderate, to destruction, loss, alteration or unauthorized disclosure

disclosure of or unauthorized access to personal data,

which have been transmitted, stored or otherwise processed".27 After

new legal situation are therefore not only common in earlier usage

"Data leakage" through loss of confidentiality includes, but also the loss

of availability through destruction or loss of integrity through destruction

change of personal data. It is irrelevant whether it is a matter of

Active data is subject to special protection under Art. 9 DS-GVO.

The person responsible is only not required to report to the supervisory

authority if the violation of the protection of personal data pre-

obviously does not pose a risk to the rights and freedoms of individuals

leads.28

23 art. 33, 34 GDPR

24 On Section 42a of the Federal Data Protection Act (BDSG) a . F. see Annual Report 2010, 12.2; to § 18a Berliner

Data Protection Act (BlnDSG) a . F. see Annual Report 2011, 11.2.1

25 The corresponding provisions for the areas of police and justice are §§ 51, 52

BlnDSG in implementation of the so-called. JI Directive (EU) 2016/680; see JB 2017, 3.1

26 § 42a BDSG a . F.; § 18a para. 1 BlnDSG a . F.

27 art. 4 no. 12 GDPR

28 See briefing paper no . 18 of the Conference of Independent Data Protection Authorities of the federal and state governments, "Risk to the rights and freedoms of natural sonen", available at www .datenschutz-berlin .de/infothek-und-service/veroeffent-clearings/short papers/

23

This significant tightening of the legal situation was probably the main reason for the massive increase in data breach reports to us. while in We received 51 reports29 in the entire year 2017, there were reporting period 357 reports, of which 332 reports since May 25, 2018.30 number of reports has leveled off at this high level, a decline is not recognizable. For us it is clear that data protection is also important because This extended reporting obligations has moved more into the focus of those responsible particularly since sanction regulations31 are provided for violations of the reporting obligation are. On the other hand, the information obtained through the notification may not used to identify the data breach underlying the notification to sanction.32 Multiple similar violations, in particular those that can be attributed to structural deficiencies at the controller, but could prompt us to carry out an audit.

The following messages that have reached us are outlined as examples: So shared a youth welfare organization the theft of a USB stick with biographical information data of the inpatient young people, a company doctor sent a a finding to the wrong addressee and two hotels could

attack on a booking platform cannot rule out that credit card da-

ten to unauthorized persons. Numerous other reports related to usage

from open e-mail distribution lists, which means that not only the personal,

ing” e-mail addresses33 were announced reciprocally, but at the same time

sensitive data such as the fact of union membership (as happened

at a union). We also received increasing reports of foreign

installed malware such as crypto-trojans. In this way, the

nical systems encrypted files from unauthorized persons in order for the

29 44 reports in the non-public area, 7 reports in the public area

30,295 reports in the non-public area, 37 reports in the public area

(as of December 31, 2018)

31 According to Art. 83 para. 4 lit. a i . v. m . kind . 33 DS-GVO, the fine is up to 10 million.

euros or, in the case of a company, up to 2% of its total worldwide

th annual turnover of the previous financial year, depending on which of the

amounts is higher.

32 See § 43 para. 4 Federal Data Protection Act. The provision is an expression of the constitutional

Prohibition of forced self-incrimination and "succession regulation" of § 42a sentence 6

Federal Data Protection Act a. F.

33 E-mail addresses are considered "speaking" if they contain first and last names

contain .

Chapter 1 Main points 1 .3 Obligation to provide information in the event of data breaches

Extort money for decryption – for medical data in a doctor’s office

almost a GAU.34 for obvious reasons

1.3.1 Obligations towards the supervisory authority

Legal basis for the obligation of the person responsible to report to us as

The supervisory authority is Art. 33 GDPR. The person responsible then reports the

breach of data protection immediately and if possible within 72 hours after it

became known to him. This period includes weekends and public holidays.35 a

later notification must include a reason for the delay. In the al-

In most cases, the notification was made to us on time, in the case of late

th reports usually with a comprehensible reason for the delay. In

In one case, however, it was unacceptable: the appeal was a public one

Position on vacation, illness, increased workload, unclear responsibilities

and internal consultations, which were repeatedly considered necessary, also in the

Total not suitable to justify the two-month delay in reporting

gen. We have called for organizational improvements that will ensure the smooth

In the future, we will ensure that the responsible body is informed quickly and in a timely manner

Afford.

It should be noted that those responsible are not obliged to keep all information

provide at the same time. Rather, the information can

reasonable further delay will be provided in stages.36

To make the reporting process easier, we have included a form with instructions on how to fill it out

set up on the Internet, which is now predominantly used by those responsible

is used. There is a guideline from the European Data Protection Board (EDPB).

34 Worst Estimated Accident

35 Art. 3 para. 3 Regulation (EEC, Euratom) No . 1182/71 of the Council of 3 June 1971 to

Establishing the rules for deadlines, dates and deadlines, OJ. No . L 124 from 8. June

1971, p. 1f.

36 art. 33 para. 4 GDPR

25

valuable information on the interpretation of the new regulations and additional

games for reportable incidents.37

1.3.2 Obligations towards data subjects

According to Art. 34 DS-GVO, the person responsible must inform the data subject immediately

to notify you of a personal data breach,

if the data breach is likely to pose a high risk to those affected

person leads. While the notification to us as a supervisory authority in the event of a

data breach is the norm, this is the notification of those affected

rather not. Because in the first case there is "only" a risk, but in the second case it is

a high risk to the rights and freedoms of the data subject

puts.

For this it depends on a danger prognosis, which above all the abstract

Risk of misuse (based on the type of data concerned) and the specific

risk of use (on the basis of the concrete potential effects of the data

breach of protection) is taken into account. Such a high risk can when it comes to

the earlier "catalog data" 38 is not from the controller from the outset

be excluded. Rather, a (documented) justification is required,

why with this data there is probably no high risk for those affected

stands. It is not sufficient e.g. B. the common justification that it gives the thief a

high-end laptops was all about the resale device, the data

but would definitely be deleted beforehand. That a person responsible for this but

can not influence is obvious; so he can't take the high risk

exclude. We therefore advise, particularly with sensitive data, to

careful notification of those affected.

37 Form, filling-in aid and guideline (WP 250 rev . 01) can be accessed at www .daten-

schutz-berlin .de/wirtschaft-und-verwaltung/melde-einer-datenpanne/ .

38 These are the data categories in the former Section 42a BDSG, i.e. sensitive data such as e.g. B.

Health data, data subject to professional secrecy, data relating to

criminal acts or administrative offenses or to a related

related, as well as bank account and credit card information.

In the other cases, too, we generally recommend that those responsible

the data subjects – notwithstanding any obligation to notify pursuant to Art.

34 DS-GVO - to be informed about the incident. Our concern with this

what is missing is that the greatest possible

Transparency is created - not only because the idea of transparency is one of the

pillars of the GDPR. Our experiences show that sufferers get it with everything

Recognize displeasure with the data protection violation, if the

Those responsible for their mistakes and they of their own accord and, above all, in a timely manner

informed. The majority of those responsible followed our recommendation.

In certain cases, despite the likely high risk, there is no obligation to

Notification of those affected.39 This is e.g. B. the case when the missing

data medium received was sufficiently encrypted. If the notification

approval would involve a disproportionate effort, has instead

to make a public announcement or a similar measure,

through which those affected are informed in a comparably effective manner. Of this

Several responsible persons have the possibility to use it upon our notice

did. So did an exhibitor at a car show after being sent by post

Applications with account information from those interested in subscribing were lost

corresponding information on its homepage for several weeks.

tion kept ready. A professor of a college has after during the

break, his laptop was stolen from the seminar room

attached in the department, which also indicates the loss of witnesses

technical data was pointed out. An advertisement in a daily newspaper can also be used

effective public notice.

As a result, most of those responsible have

behave cooperatively with us.

39 art. 34 para. 3 GDPR

27

1.4 Data protection certification – The way to

Privacy Seal

s

i

x

a

right

P

right

e

i.e

s

and

A

If companies want to convince their customers and business partners of

that they take data protection seriously and implement it, then offer them data

tenschutz-seal a way for this. These seals can be used by private

certification bodies are issued. We participate in the process

Approve and monitor certification bodies for their activities.

If customers or business partners decide to enter into a business

hung with a company, they often feel the need to get involved

a quick overview of the data protection level of relevant products and

to provide services. Companies operating in a law-compliant

or particularly data protection-friendly operation of their data processing in

have invested want to present this to the outside world. Privacy Certificates and

-Seals meet both needs.

Even before the General Data Protection Regulation (GDPR) came into force

there such certificates. But it often remained unclear what significance they actually

actually own and how thoroughly the issuers of the certificates the certified

actually tested the service or the certified product.

The GDPR creates transparency here: Certification bodies must agree

provide accreditation process. The criteria they use for certification

place, require the approval of the supervisory authorities and, if necessary, the EU

European Data Protection Board and are publicly available. When a

Certification body positively assesses and certifies data processing, then

it must notify the competent supervisory authority of this. Does this see the certi-

If the certification criteria are not met, it may refuse to issue the certificates

prevent or revoke issued certificates. Also the accreditation

Authorization of a certification authority can be revoked.

As a result, everyone benefits: citizens can more easily assess

whether products, processes and services from companies have sufficient

provide a suitable level of data protection. Also companies that process data

such as cloud service providers or document shredders, received through

the certificates ensure security for you and your customers, GDPR-compliant service

to use services, even if the processor is outside the

is based in the EU. Evidence of data protection-compliant data processing is

relieved by.

Companies that are themselves processors or processors can

the certificates show that they offer data protection-compliant services

ten. This simplified proof of compliance with data protection requirements

changes can bring competitive advantages.

1.4.1 Certification and Accreditation

A meaningful certificate comes at the end of a comprehensive certification

development process.

The certificate shows

• which object, i. H. which product, which process or which

service (object of certification) was certified,

• where you can read about the properties of the object of certification

must ensure at least

• in which framework the certificate is valid,

• when it was issued and for how long it is valid as well

• who carried out the certification.

The certificate shows the compatibility of the object of certification with the

requirements of the GDPR. Certifiable according to the current legal

lage40 are products, processes and services in which personal

gene data are processed.

40 kind . 43 para. 1 letter b DS-GVO refers to EN-ISO/IEC 17065/2012, the requirements

Provides bodies that certify products, processes and services.

29

In order to guarantee the necessary quality and thus also trustworthiness

ten, the DS-GVO stipulates that only sufficiently qualified certification bodies

may issue data protection certificates. The qualification of the certification

is ensured through their prior accreditation and regular monitoring

guaranteed.

Accreditation means that a potential certification body has one itself

has passed the exam and is thus permitted to certify. Around

To be accredited, the certification body must first define the criteria

name that they would like to use as a benchmark for their certifications. This crisis

terian submits them to the supervisory authority, which evaluates and approves them if they

sufficient to establish lawful data processing. Main-

The standard here is the GDPR. Further legal regulations must be in place depending on

the type of certification object and the circumstances of its use

are additionally taken into account. This can be the BDSG, the state data protection

be laws and area-specific regulations, e.g. B. from social law or

professional regulations to protect the secrets of patients

patients. Beyond the legal regulations, the certification

criteria also refer to national and international standards, e.g. B. on

the standards of the International Organization for Standardization (ISO) for the

Information technology security.

On the other hand, the certification body must meet requirements relating to an

sufficient professional qualifications of their employees, a suitable organizational

ical structure as well as clearly defined processes and impartiality or

fulfill independence. There is a general international standard for this

EN-ISO/IEC 17065/2012 applicable to the accreditation of certification bodies in

applies to very different subject areas, from organic farming to building materials for the

erection of buildings. It was an important task of the German and other

European supervisory authorities in 2018, this standard with requirements

genes that are to apply specifically to data protection accreditation.

The Berlin supervisory authority was intensively involved in this. was worked out

a provisional amended version of the standard, which is now (as of December 2018)

sent to the European Data Protection Board for an opinion.

1.4.2 Procedure of the accreditation process

In the process of accreditation of certification bodies, the

supervisory authorities and the German Accreditation Body (DAkkS) work closely together.41

The DAkkS controls the entire accreditation process and accepts the applications

against, takes over the formal examination steps. The supervisory authorities examine

and approve the certification criteria, check not only the practical

particular the independence of the applicant and her

expertise and decide together with the DAkkS whether accreditation

is granted or not. After a positive decision, they issue the application

issuers have the authority to act as a certification body.

In detail, the accreditation process is as follows:

program check

1.

Application phase for the

program check

2.

program review and

approval of the criteria

3.

application phase accreditation/

Authorization

accreditation

4.

assessment phase

5.

accreditation phase/

Authorization

6.

monitoring phase

The actual accreditation procedure is preceded by a program

switches. The program examination deals with the certification criteria

teries (what should the company to be certified after presenting the certification

certification body do?) and the planned procedure of the certification body (how

does the certification body want to determine whether the criteria are met?).

41 art. 43 GDPR, § 39 BDSG

31

The criteria and the accompanying processes together form the certification

gram, hence the name of this phase.

The German supervisory authorities are working on creating the requirements

and procedures for evaluating certification criteria and programs

also close together. This is intended to make it possible to compare accreditation

genes of the individual supervisory authorities can be achieved. Furthermore, a system

the necessary quality of the certification

tification programs with their certification criteria are guaranteed.

This also ensures test transparency.

If a European data protection seal is sought, there is also one

Approval of the certification criteria by the European Data Protection Agency

scrap required.42

The actual accreditation process begins with the submission of the accreditation

application to the DAkkS. When reviewing the application, this binds the

competent supervisory authority as authorizing authority in the accreditation

procedure.

The assessment follows the document check. In the course of the appraisal

The responsible supervisory authority checks together with the DAkkS

a team of assessors to ensure that the requirements for the certification body are met

on site. Finally, the assessment team convinces itself of the quality of the

activity of the certification body through its accompaniment during the auditing of a

exemplary customers.

After checking the documents and appraisal, an accreditation

the appraisal results and decides on the granting of the

credit. Two-thirds of this committee consists of members of the

permanent supervisory authority and one third made up of members of the DAkkS. the

DAkkS certifies the successful completion of the accreditation phase

an accreditation notice and the accreditation certificate. the accreditation

42 Art. 42 para. 5 sentence 2, Art. 70 para. 1 letter o GDPR

tion is then included in the directory of accredited bodies of the DAkkS

recorded.

Accreditation is limited to a maximum of five according to Art. 43 Para. 4 GDPR

years and can be extended if the criteria are still met.

Based on the successful accreditation, the competent supervisory authority can

authority grant the certification body the authority to use the certification

fication program without further recognition procedures of other supervisory

hear to be active.

The competence of a body is also recognized in re-

regular intervals by the DAkkS and the competent supervisory authority

supervised. This ensures that the certification authority

respective accreditation requirements permanently met. Are the con-

If deviations are found in the troll assessment, this can lead to a restriction,

suspension or cancellation of accreditation. This can also

affect certificates that have already been issued.

1.4.3 Observation of the certification and further

development of requirements

The certifications issued by the supervisory authorities are also regular

to be checked.43 The accredited certification bodies inform the

competent supervisory authority for the issuance, extension or revocation

requested certifications.44 Are the requirements for certification

not or no longer fulfilled, the competent supervisory authority can issue the certification

instruct the certification body not to grant or revoke a certification.45

Accreditations are also regularly carried out as part of intermediate examinations

checked. This includes document level and on-site checks.

43 art. 57 para. 1 letter o GDPR

44 art. 43 para. 1 sentence 1, para. 5 GDPR

45 Art. 58 para. 2 letters h GDPR

This means that the supervisory authorities will be permanently involved in the processes of accreditation dating and certification involved. The requirements for criteria and pro-programs must be regularly adapted to future developments.

The data protection supervisory authorities have set up a working group for this who participates in the continuous development of the accreditation process in rich privacy works.

Regular working meetings with the DAkkS ensure smooth cooperation work guaranteed. Current developments in the field of accreditation and data protection can be taken into account promptly.

Not only by participating in the certification processes, but also by creating information material and giving lectures, the Berlin Commissioner for Data Protection and Freedom of Information made a contribution to Fulfillment of the legal mandate,46 the introduction of data protection-specific to promote technical certification procedures.

Certificates, data protection seals and test marks will in future be a quality characteristic for the processing of personal data. With that, the citizens an instrument for better orientation in one both dynamic and fundamental rights-relevant area at hand give. Companies can use it to align their processes, products and services to the requirements of the DS-GVO. through the Approval of certification criteria, the accreditation process, the Authorization to act as a certification body, as well as by the regular control of the accredited companies and monitoring of the certifications granted by the supervisory authorities and the DAkkS

the quality of certificates in the area of data protection will be secured in the future.

46 art. 42 para. 1 GDPR

1.5 Advertising under the GDPR

Numerous complaints reach us from citizens who

find adverts addressed to you in your mailbox or advertising

advertising by e-mail, fax, SMS or as a call, although they are the advertiser

have not previously given their consent. Sometimes they didn't even have one

contact with the advertisers and wonder where they get their contact details from

have. Even advertisers who are unsure how the basic data protection

regulation affects planned advertising measures and whether and in which

The extent to which they may use data in the future for advertising measures is addressed

reinforced with requests for advice to us.

A

and

s

i.e

e

right

P

right

a

x

i

s

1.5.1 Definitions

According to the European definition, the concept of advertising includes all measures by companies, self-employed persons, associations and clubs with the aim of To promote the sale of goods or the provision of services.47 So In addition to direct product-related advertising, there is also indirect sales Promotion – for example in the form of image advertising or sponsoring – detected. The advertising term includes classic advertising brochures and catalogues, Christmas and birthday mail, newsletters and customer peace queries.48

The different forms of address and communication channels from personal Addressed advertising by post, e-mail, fax or by telephone are data to be assessed differently in terms of protection.

47 art. 2 letters a of Directive 2006/114/EC of the European Parliament and of the Council of 12 . December 2006 on misleading and comparative advertising (OJ EU L 376 p. 21)

48 See judgment of the Federal Court of Justice (BGH) of 12 . September 2013 – I ZR 208/12 and BGH judgment of 10. July 2018 – VI ZR 225/17, available at http://www .bundes-gerichtshof .de/DE/Entigungen/schlussen_node .html

1.5.2 New regulations

With the entry into force of the GDPR, the previous detailed regulations on Advertising is omitted.49 The GDPR does not contain any special system for the permissiveness of advertising, therefore, in principle, the general applicable provisions for the processing of personal data.

It is still the case that advertising is only permitted if either a legal Legal permission or consent of the person being advertised is available.

The processing of personal data by advertisers can be lawful

be reasonable if this is to protect the legitimate interests of the advertiser

or required by third parties and provided that does not affect the interests or fundamental rights

and fundamental freedoms of the advertising recipients prevail. This applies in particular

Measures even if the data subject is a child.50

The person concerned must not have objected to direct advertising.

The General Data Protection Regulation provides for an explicit right of objection.51

In each specific individual case, the interests of the

be made or the third party as well as the person concerned. direct mail

can in principle be considered as processing serving a legitimate interest

personal data are considered.52 However, for the required

always to ask what is being advertised objectively more reasonable

can or may wisely expect. It is therefore crucial whether the processing

personal data for certain areas of the social sphere typically

wisely accepted or rejected and whether it is reasonable, disadvantages

accept for the right to self-determination.

The advertisers must be able to prove that they have carried out this balancing of interests

actually carried out and that the result is in their favour.

Furthermore, they have to face the interests that are included in the consideration

expressly name the data subject.53 This can be done, for example, within the framework

49 Section 28 para . 3 BDSG a. F.

50 kind . 6 para. 1 letter f GDPR

51 art. 21 GDPR

52 Recital 47 GDPR

53 art. 5 para. 2, art. 13 para. 1 letter d GDPR

of the data protection declaration. Inform the advertiser at the time of the

Data collection transparent and comprehensive via a planned advertising

use of the data, the expectations of the applicants are usually also

indicate that their customer data will be used accordingly. However, through

Transparency is the legal basis for consideration according to Article 6 Paragraph 1 Sentence 1 Letter f

DS-GVO cannot be expanded at will, since the expectations of the objective

standard of reason must be measured.

In this context, the general principles of the DS-

GVO54 to be observed. Data processing must be fair and comprehensible (nominal

tion of the sources of the data).

If it is based on a selection criterion for a division into advertising groups

comes and there is no additional knowledge gain from the grouping,

the balance of interests will usually be in favor of the advertiser.

Interests worthy of protection, on the other hand, should not generally prevail if

following an order to all customers equally

by post an advertising catalog or an advertising letter for the purchase of further products

products of the advertiser is sent.

The creation of advertising profiles or the extraction of data from social network

work for the purposes of direct advertising, however, will only be carried out with prior consent

be allowed. More intervention-intensive measures, such as automated selection

tion process for the creation of detailed profiles, behavioral forecasts or

Analyzes that lead to additional insights also suggest that

that the interest of the applicant in the exclusion of data processing

weighs. In these cases, it is so-called profiling, which involves obtaining a

Requires consent prior to data processing. A reference to a

existing right of objection is not sufficient in these cases.

With regard to the transmission of data for advertising purposes to third parties and use of third-party addresses, it can generally be assumed that the interest sen of the advertised persons is to be given a higher priority than that Interest of advertisers or third parties in the transmission or use of

54 art. 5 para. 1 GDPR

37

External addresses for advertising. The expectations of the people involved is also determined by whether a relevant and appropriate relationship between them and the advertisers, e.g. B. a customer relationship. at a disclosure of personal data to outside of these customer dependent third parties, this is generally not the case. Usually will Customers do not expect their contact details to be shared with companies where they z. B. bought, sold to address dealers for advertising purposes become without being asked.

1.5.3 Consent

Processing for advertising purposes can continue to be based on a voluntary and independent consent of the advertised person.

The consent must be confirmed by a clear affirmative action in be made in written, electronic or oral form.55

Silence, already preset, ticked boxes or even a non-activities of the person concerned are not sufficient for this. Things to note in this However, in particular the new information and documentation duties of the persons responsible.56 The persons concerned are informed information in a transparent, understandable and easily accessible form in one clear and simple language.57 The advertised person must also always be advised of the possibility of revocation.58

A consent can be ineffective in particular if a strong

Imbalance between controllers and data subjects

exists.59 It is also not possible to link a service with a

necessary data processing against the voluntariness of a consent

55 Recital 32 GDPR

56 See also the Working Paper (WP 260) of the Art .29 Group, available at http://

ec.europa.eu/newsroom/article29/news-overview.cfm

57 art. 12 para. 1 GDPR

58 art. 7 para. 3 and Art. 21 para. 3 and 4 GDPR

59 Recital 43 GDPR

chen.60 The validity of the consent is also denied if the

advertised separately according to individual processing operations

possible, although this would be appropriate in the specific case.

It is the responsibility of the advertiser to ensure compliance with the legality

of data processing and the existence of a legally effective consent

proof.61 Although the GDPR, unlike the old federal data

Protection Act no longer requires the written form in this regard. To however this

In order to be able to meet obligations, it is advisable to regularly ask for one

Consent in writing with a handwritten signature or at least in

text form (e.g. e-mail). For the electronic declaration of consent

The so-called double opt-in procedure is required as proof (depending on the con-

specific type of contact: e-mail or SMS), whereby the legal proof of

requirements must be taken into account when logging. are to be held

the content of the consent and the entire opt-in procedure.62

1.5.4 Change of Purpose

Personal data not originally collected for advertising purposes

were, can still be used for advertising purposes, provided that the new

purpose is compatible with the original purpose.63

Responsible a so-called compatibility test, taking into account the in the

GDPR-regulated criteria.64 Otherwise, consent is required

conducive.

60 kind . 7 para. 4 GDPR

61 art. 5 para. 2 and Art. 7 para. 1 GDPR

62 Art. 5 para. 2 DS-GVO and BGH judgment of 10. February 2011, I ZR 164/09, available at

http://www .bundesgerichtshof .de/DE/Entigungen/schlussen_node .html

63 art. 6 para. 4 GDPR

64 Recital 50 GDPR

1.5.5 Unfair Competition Law

and GDPR

Irrespective of data protection law, e-mail advertising and other advertising

e-mail as well as telephone and fax advertising, the

ten of the law against unfair competition (UWG), which also

remain applicable according to the new regulations of the GDPR. These rules

in which cases of unreasonable harassment of the applicant

go and advertising of this kind is inadmissible. If the UWG for certain

forms of advertising and contact channels recognizes an unreasonable nuisance, this is

to be taken into account within the framework of the balancing of interests of the DS-GVO.

E-mail advertising and other advertising with electronic mail and tele

Telephone or fax advertising to consumers is therefore

accordingly only after express separate consent

allowed. The situation may be different in the case of e-mail advertising if the persons concerned

people who have already been customers of the company

similar products are advertised and they are given the opportunity to

is granted.65

1.5.6 Note advertising contradiction

The advertising objection of a data subject can be data protection

may be directed against the data owners and/or the advertisers as those responsible.

Both must take this advertising contradiction into account in the future, e.g. B. through

Inclusion in an ad blocking file. Those responsible have for the effective

enforcement of the data subject's right to object

ken, for example by forwarding the objection. The implementation of

Objection must be made immediately.

65 Art. 7 para. 3 UWG

The sending of personally addressed advertising by post is only

Permitted when either consent or legal permission to do so

present. For e-mail advertising and other advertising with electronic mail

as well as telephone and fax advertising, the requirements of the UWG must also be

respect, think highly of.

1.6 The new Berlin Data Protection Act –

Hopefully not the latest

With the entry into force of the General Data Protection Regulation on May 25, 2018

the reform process of European data protection law was by no means over

de. Rather, this resulted in an enormous need for adjustment by the federal and

State law, which has not yet been fully completed to this day

is.66 The Berlin data protection law is significantly influenced by the Berlin Data

Protection Act (BlnDSG), which was passed on May 31, 2018 by the Berlin

house of orders was decided. It regulates the conditions under which

the public authorities of the State of Berlin generally process personal data

allowed to process.

In addition to adapting the general Berlin data protection law to the DS-

GVO also became the EU data protection directive for police and police forces with this law

Legal authorities, the so-called JI Directive EU 2016/680, into national law.

This also means that the processing of personal data by the police

and judicial authorities newly regulated. As before, however, the BlnDSG will also

further through various area-specific regulations in various

al laws added.67

Our authority was intensively involved in the legislative process. We have

submitted several written statements and informed us several times in the relevant

speaking committee meetings as well as in the plenary session.

66 See 1.8

67 See 1.8

41

Unfortunately, we were not able to assert ourselves with all of our concerns. in the

Unfortunately, the result is that the Berlin Data Protection Act affects some

Places the rights of citizens guaranteed in the GDPR curtailed.68 In the

However, strengthening the rights of those affected is a central concern of the

European data protection reform. Affected rights put people in

the position to exercise data protection in a self-determined manner. Based on information

and information, they should be transparent themselves about the personal

worked data can produce. This is a prerequisite for reporting

Cancellations and deletions enforce the accuracy of the stored data

to be able to It is all the more regrettable that the Berlin legislature in this

area has made restrictions that are no longer required by the GDPR

are covered: For example, according to this, rights to information are not only restricted

if the provision of information leads to the prosecution of criminal offenses or the security

security of the country would be endangered, as stipulated by the European regulations.69

Rather, the refusal to provide information should also apply in the case of comparatively insignificant

be permissible in the fine procedures, such as stopping in a no-parking zone.70

In addition, certain decisions about a refusal to provide information

not even passed by the independent data protection supervisory authority

are testable. According to the new Berlin law, this is always the case if

individual members of the Senate refuse to provide information on the grounds that

there is a potential threat to the federal or state governments.71 An over-

verification of the validity of this reasoning is according to the new legal

The Berlin regulation is just as impossible as checking legality

the specific data processing by the data subjects themselves or on their behalf

tend by our authority.

Other powers of the data protection supervisory authority were also granted by the Berliner

House of Representatives significantly restricted. It is especially in the public domain

questionable whether we can carry out our task effectively. So we got

68 §§ 23 et seq. BlnDSG

69 art. 23 para. 1 GDPR

70 § 24 para . 1 sentence 2 no. 2 BlnDSG

71 § 24 para . 3 BlnDSG

specifically denied the power enshrined in the GDPR to impose fines against

to impose on authorities and other public bodies.72

In the area of the JI Directive, the Berlin legislature has gone even further

and, contrary to the wording of the guideline of our authority,

granted a right of objection.73 If the addressee of a

not comply with the requirement, there is therefore only the possibility of

to appeal to the relevant parliamentary committee, which in turn also

has no legally binding remedy powers. The recording on

the agenda does not have to be short-term, so that a

breach of data protection may persist for a long time without concrete

to be able to intervene. The possibility of bringing about a judicial clarification,

also does not exist. This regulation contradicts the specifications of the JI guidelines

never, which presupposes that the supervisory authority must be able to

to issue legally binding instructions.74 As examples of such effective

Authorizations are given as examples, e.g. B. the power to data processors

instruct processing operations to comply with data protection laws

bring, and the power to impose a temporary or permanent restriction

to impose the processing, including a ban. Contrary to the festival

of the JI Directive,75 according to which the supervisory authority shall apply the

regulations issued under this Directive and their implementing regulations

should monitor and enforce, our authority does not have the

necessary powers to carry out this task effectively.

It remains to be hoped that the BlnDSG will

evaluated in the points we criticized gave way

sert.

72 § 28 BlnDSG

73 Section 13 para. 2 BlnDSG

74 art. 47 para. 2 JI Policy

75 Art. 46 para. 1 letter a JI policy

43

When adapting the BlnDSG to the DS-GVO and the JI directive, it has

the legislature missed a courageous signal in the direction of the protection of fundamental rights

to put. The rights of data subjects contained in the GDPR have been

restricts. The powers of the authority responsible for safeguarding these rights

fen is circumcised.

1.7 Facebook fan pages and the common

Responsibility for data processing

s

i

x

a

right

P

right

e

i.e

s

and

A

In June 201876, the European Court of Justice ruled that fan page

operators on Facebook together with Facebook for the

processing of personal data of visitors to the fan

page are responsible. The decision is based on the before May 25th

2018 Privacy Policy applicable. But the considerations can be summarized in the

GDPR time transferred since the definition of joint controllers themselves

has not changed. In contrast to the old legal situation, the GDPR provides for the

joint controllers, however, additional requirements in Art. 26 DS-

GMO before. According to this, they are obliged to set out transparently in an agreement

increase who fulfills which obligations under the GDPR. Furthermore

the agreement must reflect the respective actual functions and relationships

of the jointly responsible persons towards the data subjects

rend reflect, in addition, the essential content of the agreement must the

data subjects are made available.

1.7.1 Hearing procedure in Berlin

The decision of the ECJ is trend-setting, because it

In terms of data protection responsibility, it is irrelevant whether the person involved in the processing

actors involved in personal data legally or economically "on

act at eye level" or e.g. B. are infrastructural dependent on each other. in the

76 Judgment of the ECJ of 5 . June 2018, case C-210/16 Wirtschaftsakademie Schles-

wig Holstein

As a result, those responsible cannot hide behind large platforms and

Infrastructure providers "hide" their offers

use.77 Even several months after the publication of the judgment of the ECJ

However, we could not see that fan page operators

drivers in Berlin, especially public authorities, consequences of the

would have judged. Nothing official was heard from Facebook either,

in particular, there was still no agreement required under the GDPR

submitted for joint responsibility.78

In September, the Conference of Independent Data Protection Supervisors

federal and state authorities (DSK) in a decision79 that the authority

drove a fan page, as offered by Facebook, without an agreement under Art. 26

GDPR is illegal. In addition, the DSK pointed out that fan page

Operators (regardless of whether they are public or

non-public responsible person) the legality of the jointly

guarantee responsible data processing and be able to prove this

must.80

Shortly thereafter, Facebook published a supplemental agreement that referred to

shared responsibility. However, we have doubts that the

information published by Facebook to date and in connection with the

has provided supplementary agreement, are sufficient to re-

statement of the lawfulness of the processing of visitor data

and visitors to the fan page. So we have a series

from offices of the Berlin state administration, political parties and companies

men and organizations e.g. from the retail, publishing and financial sectors in

written to Berlin. We are currently listening to them on data protection issues

77 The ECJ makes it clear that the fact that organizations and persons who

use the platform set up by Facebook to provide the associated services

gene to claim, this does not depend on the observance of their obligations in the

area of personal data protection, judgment of the ECJ of

5 . June 2018, case C-210/16, paragraph . 40

78 See Art . 26 GDPR

79

"DSK resolution on Facebook fan pages" Düsseldorf, 5. September 2018, available

at https://www .datenschutzkonferenz-online .de/media/dskb/20180905_dskb_face-

book_fanpages.pdf

80 See the in Art. 5 para. 2 DS-GVO specified accountability

to. In particular, we want to know which specific data processing

processing, on which legal basis the data processing takes place

and how the information of the persons concerned is ensured.81

1.7.2 Interpretation and scope of the common

processing of personal data

As part of the fan page procedure, the ECJ pointed out that Facebook

so-called “page insights” for the site operators, i.e

Statistics about the visitors of the site and the type of use

tongue. It played a major role for the court that the fan page operators

and operators by setting certain parameters (e.g. evaluations

by age and gender) according to their target audience in the creation

of the statistics through Facebook.82 It remained unclear whether the common

Responsibility of the site operators for the creation of

cher page insights also to subsequent or further data transactions

work by Facebook should extend. On the other hand speaks that the ECJ

Page insights and parameterization by the site operators

driver in the foreground. However, the ECJ, apparently independent

gig from the parameterization, especially with such visitors

of the fan page who are not registered with Facebook have an increased responsibility

the site operators. In these cases, according to the ECJ, solve that

Merely calling up the fan page automatically processes your personal

data.83 The court thus defined the concept of responsible

processing of personal data.84

81 We have the catalog of questions in the hearing procedure at https://www .daten-

schutz-berlin .de/fileadmin/user_upload/pdf/informationen/2018-BlnBDI-Fragenkata-

log_Fanpages.pdf released.

82 Judgment of the ECJ of 5 . June 2018, case C-210/16, paragraph . 39

83 Judgment of the ECJ of 5 . June 2018, case C-210/16, paragraph . 41

84 Accordingly, the ECJ pointed out in the decision that it is not necessary

it is clear that each or each joint controller has access to those concerned

has personal data, cf. Judgment of the ECJ from 5. June 2018, Case

C-210/16, para. 38

The ECJ confirmed this interpretation in a further decision from the

last year. Shortly after the fan page decision, the court ruled85 that

a religious community together with their proclaimers

members responsible for the processing of personal

ner data is. In this case, the ECJ left it for the data protection

answer sufficient that the religious community the proclamation activity

organizes, coordinates and encourages members to do so.86

Another judicial clarification of the concept of joint responsibility

is not far. In a current procedure, the ECJ has to deal with the question of

Integration of social plugins87 in websites and with responsibility for the

deal with the data processing triggered by this. In December he

Advocate General publishes his Opinion in the proceedings.88 He comes

to the conclusion that the operators of websites with the

Third parties whose plugins they have integrated into their websites as common

responsible persons are to be considered. The Advocate General puts on the survey

and transmission of personal data processed by the plugins

but at the same time suggests shared responsibility

to refer to such phases in an overall chain of data processing operations

limit, in which a participating actor actually contributes to the decision-

information about the means and purposes of data processing. In the case of the social

Plugins is limited to the joint responsibility of the in question-

the website operator according to the proposals of the Advocate General

the phase of collection and transmission. Excluded then remain the white

ter processing by the third parties who provided the plugins. It stays

exciting what the ECJ makes of it.

It can already be stated that the initiation of processing

personal data may be sufficient to establish a data protection law

to establish responsibility. This has consequences for the interaction

85 Judgment of the ECJ of 10 . July 2018, Case C-25/17

86 Judgment of the ECJ of 10 . July 2018, case C-25/17, paragraph . 75

87 Case C-40/17: The case concerns the "Like" button of Face-

book .

88 Opinion of Advocate General Michal Bobek of 19 . December 2018 in the

Case C-40/17

from website operators and third parties, e.g. B. when pixels in the

Websites are integrated or third parties are enabled to place cookies on the

end devices of the users.

1.8 Berlin State Laws − Fit for Europe?

When the GDPR came into effect on May 25, 2018, the state of Berlin

checked whether and to what extent the numerous state laws apply

the European legal regulations have to be adapted. The GDPR contains more than

70 so-called opening clauses for the national legislature, which will continue to exist

allow the processing of personal data in special regulations

to regulate or maintain. For the adjustment of the data protection law

The leading Senate Department for the Interior and Sport has the main administration

called upon to comply with the specialist laws in their area of responsibility

review to see changes in an article law adapting the data protection

right to be included in the GDPR. We were involved in this process

in close contact with some specialist administrations and advised them intensively.

With the Senate Department for Europe and Culture, we were already able to at the end of 2017

the need for change, etc. with regard to the archive law of the state of Berlin

such as the Cultural Data Processing Act, which then send this to the

administration has passed on. We also have the Senate Chancellery regarding

the adjustment of the Berlin Higher Education Act and the student data

advise order.

We have the Senate Department for Health, Care and Equal Opportunities

special to adapt the Health Services Act, the state health

house law, the Chamber of Health Professions Act and the State Equal Opportunities

legal advice.

For the field of public health services have been missing for many years

the necessary regulations for the processing of personal data, in particular

particularly sensitive health data. Despite intensive exchange with the

permanent authorities on the question of the enactment of a corresponding ordinance

still no draft at the end of 2017.89 We could now

achieve towards the health administration that in the course of the necessary

Necessary review and adjustment of the regulations in the health service

law, the opportunity was taken to fill the previously missing processing

executive powers for the public health service directly into law

record. If the Senate Department for the Interior accepts the proposed changes

changes, an essential step has been taken to

processing in the public health service on a legally secure basis

place.

We have also intensively accompanied the current school law reform. The Senate

Administration for Education, Youth and Family took the opportunity in this

In the course of this, the Berlin Schools Act also conformed to the data protection requirements of the GDPR

fit.90

At the present time - almost a year after the GDPR came into effect -

therefore unfortunately only the school law and the health professions chamber law amended

came into force and thus – to a large extent91 in line with the provisions of European law

been adjusted. The parliamentary law stands for all other specialist laws

Legislative process still pending.

We call on the Senate Department for the Interior to complete the legislative process

for the adaptation law to get underway quickly in order to create a European

to establish a legally compliant state in the state of Berlin.

89 JB 2017, 7.1

90 More details on the amendment to the Schools Act under JB 2018, 5.1

91 JB 2018, 5.1

49

2 Digital Management

2.1 Digitization projects in Berlin

s

i

x

a

right

P

right

e

i.e

s

and

A

The Berlin E-Government Act (EGovG Bln) is intended to contribute to

channels, citizens and the economy use digital administrative services

friendly and safe to provide. Implementation is progressing rapidly.

Since March, the Berlin Service Account has offered the option of administrative services

to be able to use it electronically without media discontinuity.92 Currently you can

Although only a few online services are being used,93 it is planned

successively connect all online services to the service account and

visch to offer a large part of all administrative services via it. We have

accompanied the introduction of the service account intensively and the leading

national administration for home affairs and sport with regard to the implementation of data

supports legal protection requirements.

The draft law to improve online access to administrative

services of the Berlin administration (online access law Berlin)94 was

situation of the Senator for the Interior and Sport was taken note of by the Senate and

the mayor should be introduced to parliament after consideration by the council

the. This sets the course for a one-time registration in the

Service account not only electronically in administrative services of the State of Berlin

To be able to claim, but also those of other federal states and the

Federal via its portal network.

According to the Berlin e-government law, the Berlin administration is obligated

plans to keep their files electronically by January 1, 2023 at the latest.95 In doing so

92 JB 2017, 2.1

93 Application for a resident parking permit, a day-care center voucher for citizens

and citizens as well as the use of the point of single contact in Berlin for

take

94 JB 2017, 2.1, p. 46

95 Section 7 para. 1 sentence 1 EGovG Bln, see also JB 2016, 2.1

is through appropriate technical and organizational measures according to the respective

State of the art to ensure that the principles of proper filing

management and the standards applicable to the Berlin administration, in particular

with regard to data protection and data security.

The electronic file enables faster and more efficient transaction processing

development, which not only benefits the citizens, but also
the employees of the Berlin administration. Through them files and other
Documents are transmitted electronically within authorities and among each other
can become. In any case, a safe, up-to-date version of the
to use the appropriate communication infrastructure. Especially
are the transmitted data protected from inspection by unauthorized persons and from
change.96 In the future, it should also protect citizens
be made possible via the Berlin service account to check the status of the process
retrieving the processing itself, which on the one hand enables faster notification
of those affected is guaranteed, but also the employees of the
Authorities are relieved of inquiries.
Since the electronic file naturally also contains particularly sensitive data
are processed, technical and organizational measures must also be taken
which enable the processing of data with high protection requirements. we
have the leading Senate Department for the Interior and Sport in the protection
needs assessment accompanied intensively. In addition, we were preparing
involved in the state-wide tender for the electronic file in an advisory capacity
and were able to ensure in this way that data protection regulations
ments and aspects are already taken into account in the course of the call for tenders. It
it is planned to carry out the tendering process in 2019.
The service account and the electronic file are flanked by the new
sis service "Digital Application", which will in future allow applications to be submitted without media discontinuity
with a uniform appearance and operating concept for all electronic ones
Applications in the Berlin administration should be possible. As with the electronic
Act also applies here that due to the potential processing particularly sensitive
ver data technical and organizational measures must be taken that

96

§ 7 para. 2 EGovG Bln

51

enable the processing of data with high protection requirements. Also here ha-

If we accompany the determination of protection requirements and other data protection

technical hints introduced.

In connection with the introduction of electronic file management and process

The Berlin authorities will continue to process to a not inconsiderable extent

Scope of paper documents accumulate, especially in the area of incoming mail.

In order to include these documents in the electronically supported workflow

paper records are more appropriate while respecting the principles

Transfer records management and storage to an electronic format.97

In any case, the specifications of the technical guideline are to be replaced

scanning of the Federal Office for Security in Information Technology98

ten. In order to find a uniform, safe and economical solution throughout Berlin,

the project "Documentary

Ten-Input-Management (DIM)" initiated. We will also accompany this project.

The introduction of digital administrative services must be for citizens

Citizens are transparent, secure and data protection compliant.

2.2 Aid Online

s

i

x

a

right

P

right

e

i.e

s

and

A

The specialist procedure for online aid application (BAO) is intended to allow beneficiaries

employees and pension recipients of the State of Berlin online

to submit applications for aid via web browser or app, the processing

track status and receive notifications. In addition, it should be possible

to report master data changes. As part of the application,

the functionalities are made available.

We were informed about this four years ago by the state administration

ensures that the prerequisites for applying for the BAO are created

must. In this early phase of the project, we had

97

98

§ 8 EGovG Bln

BSI TR-03138 Substitute Scanning (RESISCAN)

52

Chapter 2 Digital Management 2 .2 Aid Online

shared which documents for a systematic and final assessment

of the procedure are required. These are e.g. B. an IT security concept and

Concepts for organizing access rights, logging

subsequent data access and the deletion of the data.

After the first considerable delays, we received the documents, which, however,

still had to be reworked or completed, or step by step

were submitted after completion. In May 2018 the project resumed

recorded. At a first workshop, the importance of the project

confirmed and the decision was made to continue the project. Since then strides

the project is progressing rapidly with our participation.

The changed from May 25, 2018 with the General Data Protection Regulation (GDPR).

For the project, the legal situation means that a data protection impact assessment

must be carried out because due to the processed with the method

ted medical bills of the beneficiaries an extensive processing

of health data99 and thus particularly sensitive data. a da-

data protection impact assessment is a special tool for describing,

Assessing and mitigating risks to the rights and freedoms of natural

of persons in the processing of personal data.100 A data

protection impact assessment must be carried out by the respective person responsible, in

in this case the state administration office.

In a first phase, the risks of the

Procedure using the Standard Data Protection Model (SDM).101

Risks identified for which appropriate remedial action must be taken

senior As part of the continuation of the data protection impact assessment

it can now be checked whether the planned measures adequately cover the risks

mitigate.

kind . 35 para. 3 lit. b GDPR

99

100 Further information at https://www .datenschutz-berlin .de/wirtschaft-und-verwal-

/data protection impact assessment/

101 SDM: The standard data protection model provides support for data protection

advice and testing as well as for the preparation of a data protection impact assessment

on the basis of uniform protection goals (https://www .datenschutz-berlin .de/

fileadmin/user_upload/pdf/guidance/2018-SDM .pdf) .

53

53

Further developments of the process, such as the development of a user

friendly app for mobile devices are planned. For this must then also

a consideration of the risks within the framework of a data protection impact assessment

take place.

A data protection-compliant planning and design of the future-oriented

ten process online aid application could be accompanied by us on the

be taken away. The subsequent steps and the future

We will continue to follow the plan closely.

54

Chapter 2 Digital administration 3 .1 Threatening letters to the left-wing scene with data from police databases

3

interior

3.1 threatening letters to the left scene with data from

police databases

At the beginning of the year, we learned from press reports that various

Letters have been received from various institutions of the left-wing autonomous scene,

the u. contained names and photos of several specific people. In the

letters, a total of 45 people were named and 21 of these people

Photographs and information were listed, which apparently only

could come from police or judicial authorities. Enter yourself as the sender

"Centre for Political Correctness" and threatened to steal the data of these per-

sons and their family members to the police or right-wing extremist groups

to pass on pen.

A

and

s

i.e

e

right

P

right

a

x

i

s

Immediately after the media reports appeared, we contacted the

lizei and asked for a statement at short notice as to what measures the police

took the time to clarify the facts. As a first investigative measure

we recommended checking the access made to the entries in the

current databases on the persons named in the threatening letter.

The police then informed us that they were investigating against

known for violating the Berlin Data Protection Act (BlnDSG) and

breach of private secrets. According to our

missing, a log data query was prompted to determine

to clarify whether the data of the persons concerned is close in time to the sending of the letter

were retrieved from the police databases and whether the retrieval was necessary for official

was founded. The evaluation of the data queries and further investigations

with the involvement of the Forensic Institute, however, did not result in

knowledge led.

We recommended that the police take further concrete measures, which the investigating

responsible State Criminal Police Office were also partially taken into account. in particular

55

55

We recommended examining an original copy of the

ten letters from the following points of view: Identification of the serial number

of the printer used based on the print image (so-called "Machine Identification

Code"), conclusions about the origin of the letter by analyzing the

ten paper and identification of the author of the letter

fingerprints, if any.

When persons affected in the meantime contacted us confidentially,

we took a quick look at an original letter and found that

that it contained color photos in good resolution. This spoke against that of the

the assumption initially expressed by the police that when the letters were created, photoco-

pien were used.

On March 26, 2018, based on the information available to us

Criminal complaint against unknown persons for violation of the Berlin data protection law

gesetz.102 In the further course of our examination, we unfortunately only received

borders information from the Berlin police. In mid-April we were first informed

that due to an instruction from the public prosecutor's office, further communication

tion should be conducted directly via the competent public prosecutor. We had to do both

the police and the public prosecutor's office repeatedly point out that the

Police President in Berlin as the data processing office for the BlnBDI

is obliged to provide information, even if the public prosecutor's office has

mediation procedure.103

After repeated inquiries, we received the information from the police in August

mation that a police officer from the state of Berlin is investigating as a suspect

was and that the production of the letter was granted. the prosecutor

society finally informed us at the beginning of October that a court had been filed against the accused

Penal order has been issued, which has been legally effective since the end of August. There

however, we still have no knowledge as to where the

personal data contained in the letters sent come from and how

the author of the letters has reached them, our examination continues.

102 § 32 para . 3 BlnDSG a . F. i. v. m . § 32 para. 1 no. 2 old . 1 and no. 1 old . 1 BlnDSG a . F.

103 § 54 BlnDSG

The use of the threatening letters is a particularly serious incident. she

not only constitutes a criminal offence, but also damages the

trust the public in the security organs, their task in particular

is the prevention of crime.

3.2 Processing of Personal Notices in police databases

For several years now, the Berlin police have been creating and using certain political

Licensed evaluations of people, so-called personal information (PHW),

after she had previously rejected them for more than twenty years due to criticism of the

the federal and state data protection officers for their work

had used.104 We tried to reintroduce the notices without success.

said.

A

and

s

i.e

e

right

P

right

a

x

i

s

Regarding the personal information that is used nationwide

den, includes the Mental and Behavioral Disorders (PSYV) indication, which is up to

a corresponding resolution of the conference of interior ministers in 2015

“mentally ill” was called.105 Such personal information should be

the protection of the person concerned or the self-protection of police officers

officials serve.106

Due to inquiries from citizens about the storage of personal

bound information in police databases, we have the Senate Administration

Department for the Interior and Sport has now been written to again on this subject and

noted that we continue to have serious doubts about the legality

the storage of the note "mental and behavioral disorders".

From our point of view, such a note is not necessary for police purposes.

extremely stigmatizing for those affected.

104 JB 2012, 3.8

105 See Drs . 17/2406 of the Berlin House of Representatives

106 See § 16 para. 6 no. 1 Federal Criminal Police Office Act (BKAG)

57

In particular, it is not clear why the inclusion of such a note

This may be necessary for the police to avert danger or to protect themselves

target. As a rule, mentally ill persons do not pose any dangers.

because of her illness, which the police have to fend off. As far as in individual

if such dangers should nevertheless be known, the inclusion of the

also possible personal reference "violent" conceivable and

sufficient.

The personal notice “mental and behavioral disorders” should

in the absence of necessity from the list of references contained in police data

banks are assigned by the Berlin police to fulfill their duties

can be taken out.

3.3 Vulnerability in the police

Database POLIKS?

s

i

x

a

right

P

right

e

i.e

s

and

A

A police officer complained to us that unauthorized access to the political

Licensed database POLIKS due to insufficient security requirements

are possible. You can by entering an incorrect password multiple times

block any access to POLIKS and then by telephone

Hotline unblock this access again without further hurdles and get a new one

give password.

In the examination that was then initiated, it was confirmed to us that access to

POLIKS will be blocked if an incorrect password is entered several times.

To unblock the affected users could then contact

contact the central IT administration. This unblocks an account,

if the report was made by the superior or the supervisor of the

met will be confirmed. After the lock has been removed, the password is

changes; no new one will be given. We have no objection to this procedure

data protection concerns.

If, on the other hand, the user needs an account after an account has been blocked

new password, she or he must, according to the police, contact the respective

contact the local IT administration responsible for identifying the

assign a new password to the person concerned. The specific identification

driving is not uniformly regulated throughout Berlin. The internal police password

According to our findings, the guideline also does not contain any specific

gave, but only the general requirement of proof of identity.

According to the police, this is done either by presenting the service certificate

wise, verification by manager or personal knowledge of the

or the person concerned.

We then demanded that a uniform regulation be created across the authorities

fen and must be enforced that a secure identification of the

guaranteed for each affected person. In particular, it should be specified exactly when

which of the means described for identity verification when changing a password

application and how this is to be done specifically. To later

Checks - especially in the case of suspected abuse - to enable

ally, the allocation of new passwords and the type of identity checks should

must also be documented with the respective local IT administration

the. Furthermore, we have recommended regular random checks of the

local password reassignments.

The police have pledged to revise their password policy.

Unauthorized access to data in POLIKS is subject to a fine and

even constitutes a criminal offense if he intends to cause harm or gain

carried out.107 As the responsible party, the police are obliged to take the necessary

technical and organizational measures with regard to a passport

to make new assignments in order to process personal data

ten in POLIKS to ensure a level of protection appropriate to the risk.108

This also prevents administrative offenses and criminal offenses.

107 §§ 70, 29 BlnDSG

108 § 50 para . 1 BlnDSG

3.4 Control of the accreditation process

at the G20 summit

s

i

x

a

right

P

right

e

i.e

s

and

A

The G20 summit109 took place in Hamburg in July 2017. To access the press

center, journalists needed accreditation from the Federal

despress office. Evidence was required for accreditation

of journalistic activity and a security check. after it im

riots had broken out in the run-up to the G20 summit, security

authorities a new assessment of the situation, as a result of which the

previously granted accreditations have been checked. On the recommendation of the Federal

The Federal Press Office decided the criminal investigation office, a total of 32 journalists

and withdraw accreditation from journalists. Affected complained

in particular that the recommendations of the BKA are based on

Information on criminal investigations were pronounced, which partially

lagged behind for years.

The findings of the BKA were mainly based on data from

the state police authorities in the federal state information system

INPOL had been discontinued. Therefore, we have an examination regarding the

Storage of data in INPOL initiated by the Berlin police.

Prerequisite for the transmission of data to the BKA or for the storage

ing of data into the databases operated by the BKA is, on the one

lying of offenses with transnational, international or significant

Significance.110 A so-called “significance check” must be carried out here. To the

others may collect personal data from suspects and persons

who are suspected of committing a crime only under certain conditions

be served. Based on a so-called "negative prognosis" is to be checked whether because of the

Nature or performance of the act or the personality of the person concerned reason for

It is assumed that criminal proceedings against the accused or

suspects are to be led.111

109 summit of the group of the twenty most important industrialized and emerging countries

110 § 2 para . 1 Federal Criminal Police Office Act (BKAG)

111 Section 8 para . 2 BKA old or . now § 18 para. 1, 2 BKAG

Chapter 3 Interior 3 .4 Control of the accreditation process at the G20 summit

In connection with the documentation and implementation of the materiality

tests and the negative forecasts, we have found structural errors in the

liner police found. It has to be carried out when posting the data

Tests or considerations not documented, but only subsequently for

formulated the answer to our query. In the absence of individual case-related documents

documentation, it was therefore not clear to us whether the BKAG required

such tests have been carried out by the Berlin police before

Data records were fed into INPOL and whether the legally required

conditions existed.

In addition, in some cases the police had no feedback from the

Prosecutor's Office on the outcome of the proceedings, so the legality

further data storage was not checked. In one case this resulted
to the fact that another procedure was stored in INPOL, although the one concerned
Person legally acquitted by a court on factual grounds
had been. Here it must be pointed out very clearly that further processing
processing of data is inadmissible if the data subject has
has been spoken or if the opening of the main proceedings is incontestable
rejected or the proceedings were discontinued not only provisionally, provided that
it follows from the reasons for the decision that the person concerned did not commit the act
or not committed unlawfully.
We have criticized these structural errors in the Berlin police and
demands that in relation to the documentation of the tests to be carried out
procedural changes urgently need to be made. Furthermore, we have
required to take technical and organizational measures so that INPOL does not
unlawful further processing of personal data of data subjects
follows.
The police have now informed us that appropriate organizational
Procedural changes have been made or are currently in the police department
State system for information, communication and processing technically
would be implemented.
61
A storage and further processing of personal data in the
databases maintained by the BKA may only be used within the framework of the statutory
be done. It is necessary to check whether these requirements are met
on the basis of the respective individual case by the reporting office at Berliner
police done. Appropriate technical and organizational measures are required for this
to create suspensions.

3.5 First aid app “Katretter” from the Berliners

fire department

s

i

x

a

right

P

right

e

i.e

s

and

A

We accompany the Berlin fire brigade with the introduction of an app that

Alerting of first-aiders in close proximity to the location of the emergency call

light when – like e.g. B. in a cardiac arrest - particularly fast

Help can also save lives before the ambulance arrives.

The Berlin fire brigade involved us at an early stage of the project.

lit. For this purpose we were given an app "Katretter" as well as those belonging to the procedure

presented software components that are used in data centers and at the control center

are to be operated. The Katretter system is developed in cooperation with the

Fraunhofer Institute for Open Communication Systems (Focus) and the Combi

Risk GmbH is developing and is to be developed in Berlin, but also in other federal states,

operate.

The purpose of the procedure is to alert so-called first-aiders who happen to be

are in the immediate vicinity of a person to be rescued. For this seeks

In the first phase of the project, the fire brigade recruited voluntary first aiders from their own

Rows that install the app and provide assistance in an emergency. Should later too

First responders can be recruited from other medical professions.

Specifically, the procedure should be as follows: If an emergency call is made in which the requested

symptoms point to cardiac arrest, in the emergency

set, the place and more will be entered into the Katretter system at the push of a button

Enter emergency call details. The system now searches in its own database

ken for first-aiders who are in the vicinity, alerted with specification

first responders found one after the other at the scene of the emergency until a first responder

rin or a first aider confirms acceptance of the assignment via app. This person

goes to the scene of the emergency and provides “first aid” until the person arrives

ambulance. After the deployment, the first aider will

Asked to answer some questions about the mission, those of the scientific

accompaniment and possible excessive demands on the first aiders at an early stage

should show.

From a legal point of view, it had to be ensured that participation in the procedure

really voluntary. There must be no pressure whatsoever on employees of the fire brigade

be exercised to participate in the process. Also the questioning at the end

of an assignment must be voluntary and the omission of answering individual

allow questions. In particular, the last point is made scientifically

Often seen with reluctance, as this makes it difficult to evaluate the results. we

have worked to ensure that a corresponding implementation nevertheless takes place.

Another important point is the technical implementation of the project. Around

Identify first-aiders in the vicinity of an emergency location without delay

the locations of those concerned must inevitably be in a database

stored and regularly updated by the apps.

However, it is not necessary that the exact location of

potential first responders because for the few within reach of the

Persons located at the place of use, in the event of an emergency, the exact locations at the

App can be queried. After our consultation will be in the database

the locations of the first responders as circles with a diameter of 500 meters

tern listed. At any point in the circle, the first responder can

with equal probability.

In addition, it is not necessary to enter the entries for previous locations

to keep for first aiders. This would be used to create motion profiles

lead and thus possibly a deep insight into the living habits of the

allow the persons concerned. For IT security purposes and to check the

However, the functionality of the method is the storage of log data for

a period of about four days is required. Therefore, the location data

removed from this log data after just a few hours.

63

Failure to observe the above restrictions would result in the principle of data

thrift violated. In addition, the collection of the data mentioned would

may discourage applicants from registering for the procedure.

Both for the "fuzziness" of the continuously stored locations of the first

helping as well as for the storage period of the logs, which u. location data

included, appropriate values have now been found that both meet the requirements

meet the requirements of data protection as well as the functionality of the system and

enable the verifiability of the correct working method.

The "Katretter" app can save lives. When properly designed

Software and processes are avoided that have precise movement profiles

first aiders arise.

3.6 Location of emergency calls at the Berliner

fire department

s

i

x

a

right

P

right

e

i.e

s

and

A

Smartphones offer the possibility of finding out the current location of the patient in the event of an emergency call

device and via SMS or Internet to the respective rescue coordination center

to transmit. The Berlin fire brigade would like to test this functionality

drive.

Detected by smartphones via satellite tracking112 or other methods

Location data is often much more accurate than that from the mobile network using the

Funkzelle113 determined location data. Rescue workers could

find sons faster by using this system and thus possibly save lives

ten.

We were asked by the Berlin fire brigade for a legal and technical assessment

of the so-called "Advanced Mobile Location" (AML) procedure.

112 Positioning Using Multiple Satellites . There are various systems for this

teme, such as B. the American GPS or the European Galileo.

113 A cell in a cellular network is the local area covered by a

ner antenna of a specific cell tower is served.

The Berlin fire brigade was already in contact with rescue

control centers in other federal states, which will also test the service from 2019

if want to use. In view of the transnational importance

of the issues, we informed the other supervisory authorities for the early on

Federal and state data protection integrated into our examination and with

discussed with them questions about the location determination service for emergency calls.

The preliminary result is that there are currently no suitable legal bases

for the data processing carried out in connection with the procedure

is missing. In particular, there is no specific legal basis for the automatic

ated collection of location data of a person calling via smartphone in an emergency

person through the emergency call center of the Berlin fire brigade. We have the Berliner

Fire brigade recommended in this respect to create a corresponding

writing, e.g. B. in the Berlin Rescue Service Act. On the legal basis

location in the GDPR, which allows data processing if this is for protection

vital interests of the data subject or another natural

114 should be required for reasons of legal certainty

Recital 46 can only be used in individual cases.

Finally, we pointed out to the fire brigade that the proposed

stored data processing by the company Google (location determination

measurement and transmission of the location data to the control center) during the evaluation

of the procedure cannot be ignored. The problem is that

It is currently still unclear which data Google uses for location determination and

whether the data was collected lawfully. For this

should be further clarified in cooperation with the other supervisory authorities

for the data protection of the federal and state governments.

Technical questions also arise. So is used in one of the

Procedure for location determination based on the nearby detected by the smartphone

ten WiFi base stations. There are fundamental

serious concerns, since the locations of private WiFi batteries are regularly

sisstations in databases of companies like Google or Apple

114 art. 6 para. 1 letter d GDPR

without the companies having to obtain the prior consent of the entities concerned

Contact the owners of the WiFi base stations.

In the case of location determinations in the case of emergency calls, there is also the fact that the

may have deliberately switched off the location functions of the smartphone

ben. However, in the event of an emergency call, the smartphones switch on all functions

Determining the location and mobile Internet access to the locations

to transmit to the emergency caller. In addition, this is inevitable

for data transmissions to the operating system manufacturers: In order to

To determine the location via WiFi positioning115, a smartphone has to

database available online shows the locations of the Wi-

Inquire about Fi base stations. Google or Apple will inevitably find out that

any smartphone is in a certain place. To answer

is the question of whether and how the operating system manufacturers use this data and

whether the smartphones or their owners are identified

can become.

Although not all legal and technical issues have been clarified yet

could, the supervisory authorities because of the possible rescue of people

the introduction of a system for locating emergency calls by the

End devices and the transmission to the respective rescue control centers for one

Trial period of three years approved. During this period, the

remaining questions are clarified.

3.7 Post-Effective Video Surveillance

the GDPR

With the entry into force of the GDPR, the legal basis for

changed the operation of video surveillance cameras. Since the GDPR does not

contains a specific regulation on video surveillance, the scale is based on a

data protection-compliant video surveillance according to the general clause in Art. 6 Para. 1

lit. f DS-GVO and according to § 4 BDSG.

115 Determining the location of a smartphone based on those in range

WiFi base stations

According to this, the processing of personal data (and thus the video

surveillance) only permissible if they are necessary for the protection of legitimate interests of surveillance

responsible or third parties and provided that does not violate fundamental rights and

fundamental freedoms of the data subject that protect personal

required data. The DS-GVO requires a consideration in the concrete

individual case both with regard to the interests of those responsible or third parties

also of those affected. This wording is essentially the same as the old one

legal position.

However, they are much more specific and detailed than the old regulation

Requirements for transparency.116 Article 13 GDPR contains a long

talog of mandatory information to be provided. These range from the

Contact details of the person responsible and, if applicable, the data protection officer

commissioned about the interests, the purposes and the legal basis of the data

processing to the storage period and the rights of those affected. Because all these

information is impossible to fit on a conventional warning label

a graded solution is possible here. While the most important information on

belong to the sign itself, the other mandatory information can be found at the location of the

Video surveillance at a location accessible to the data subject (e.g.

at the reception, at the cash desk or at the reception).

Together with the other supervisory authorities of the federal states and the

we have developed corresponding examples, which are used by the operators

Operators of the video cameras can be used.117

In terms of content, citizens showed us video surveillance in particular

gastronomic establishments and in the private living environment. In these cases

however, the old legal position remains essentially the same. In both areas

video surveillance is generally not permitted. In particular, video

generally not beyond the property boundaries for follow-up

cash lots or into public highway land.118

116 art. 12 ff. GDPR

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

video-surveillance-after-the-ds-gvo

118 For exceptions and details see https://www .datenschutz-berlin .de/info-

counter-and-service/topics-a-to-z/video-surveillance-after-the-dsgvo

67

The video surveillance of the guest room of a gastronomic establishment is
according to Art. 6 Para. 1 lit. f GDPR i. V. m. § 4 BDSG usually under data protection law
inadmissible. Here, too, little has changed compared to the old legal situation. Gas-
tronomy areas are customer areas that are used to linger, relax
invite people to talk and communicate and are therefore not monitored with video cameras
may be. The behavior attributable to the leisure area as a guest of a
gastronomic establishment has a particularly high protection requirement
personal rights of those affected. Video surveillance disturbs the
impaired communication and the unobserved stay of the restaurant
visitors and thus reaches particularly intensively into the
privacy rights of the guests. The legitimate interest of the guests prevails
normally the legitimate interest of traders in a transfer
surveillance, which is why their interest is only expressed in exceptional cases
can put.
We are currently working with our colleagues from the
other European data protection authorities intensively a common guideline,
inform those affected about their rights and camera operators
bern is intended to facilitate compliance with legal requirements.
The requirements for the operation of a video surveillance system
are required, particularly in the area of transparency obligations
rose. are operators of video surveillance cameras
therefore requested to check whether their planned or existing monitoring
testing facilities meet the increased requirements.

3.8 Video cameras at the Alexwache

s

i

x

a

right

P

right

e

i.e

s

and

A

At the end of 2017, to fight crime and with the aim of

to make Alexanderplatz visible and accessible, set up the so-called Alexwache

tet. Shortly after the opening, a citizen informed us that he had noticed

that 360-degree cameras are installed at the corners of the Alexwache. At a

A look at the station also shows that the employees working there

Employees pan the cameras as they wish and the images live on large

monitors could observe.

68

Chapter 3 Inside 3 .8 Video cameras at the Alexwache

In the investigation we then initiated, the police stated that the

meras only the building walls and a limited area next to the respective

towards the side of the building. The video surveillance is used for police surveillance

fulfillment of gifts, because the Alexwache is an endangered object

threatened with criminal offenses directed against the police as such. The police

referred to various criminal offenses against police stations and attacks

on police vehicles and police officers in the recent past

Ness. On New Year's Eve, firecrackers were thrown at the office building.

come, moreover, has already urinated several times on the building and there are graphic

fitis been sprayed.

We informed the police that the Alexwache is not an endangered object in the sense

of police law. Rather, this term includes in particular religious

Sites, monuments, cemeteries and buildings and other structures of public

public interest.119 The common feature of these rule examples is that the

Objects themselves are of immediate public interest, with either her

existence as such is of public interest or this is based on

that the property is used by the public.

At a police station, such public interest is in the building

itself not apparent. In this respect, one cannot rely on the

ted state tasks such as security and criminal prosecution, as this

a job description of the police that does not meet the criteria of the

indirectness and the special interest in the protection of the property. other

Otherwise, every building in which government tasks are performed would be an object

in the sense of the police law, which span the scope of protection of the regulation

would.

However, due to the incidents described, the police can turn to the Alexwa

che regarding the exercise of their domiciliary rights with regard to video surveillance

appointed. This is under strict conditions of every public body in Berlin

possible.120 In addition to specific identification and deletion

obligations to be observed, particularly in the context of the proportionality test,

119 § 24a General Security and Order Act (ASOG)

120 § 20 BlnDSG

69

that the detection range of the cameras is about one meter from the building

sade is limited.121

The police have meanwhile taken over our legal position and

necessary measures implemented. i.a. the recording area of the

meras reduced in size and signs attached in an understandable way

clarify the detection range of the cameras.

It is important that before conducting video surveillance, the police

measures whose actual purpose is made clear and possible

legal norms of authorization are strictly separated from one another. The standards have

different conditions and correspondingly different degrees of severity

impact on those affected.

121 See judgment of AG Berlin-Mitte of 18 . December 2003, Az. 16C427/02

70

Chapter 3 Inside 4 .1 fahrCard – With photo and full name?

4 Transport and Tourism

4.1

fahrCard – with a photo and full name?

A petitioner contacted us because his previous company ticket with carrier card

exchanged for the electronic ticket, the fahrCard. he

complained on the one hand that he had to take a photograph in the course of the changeover

had to submit for attachment to the fahrCard, which was the case with the previous carrier

Gerkarte was not required. On the other hand, he complained that

trollers not only his full name when checking tickets, but

who could also see his date of birth.

A

and

s

i.e

e

right

P

right

a

x

i

s

The attachment of the photograph is permitted as it is personal, not

transferable season ticket. The BVG informed us that for a

NEN from the VBB tariff provisions that personal electronic

tickets are to be provided with a photo,122 on the other hand the photo

bild for an efficient control of the authorization to use the ticket

necessary. The photograph is therefore necessary for the fulfillment of a contract between

the respective fahrCard holder and the BVG.123

However, according to our recommendation, the BVG adjusted the storage of personal

son-related data on the fahrCard in such a way that in future only

Year of birth124 and the first letters of the first and last name125

be summarized, so that the complete information for the control staff is not

are more visible.126

The BVG offered the petitioner to exchange his fahrCard free of charge.

122 Annex B to the VBB tariff, number 5 .2 .5, subparagraph 6

123 Art. 6 para. 1 sentence 1 lit. b GDPR

124 As well as day and month always as “01 .01 .”

125 Replacing the remaining letters with "*"

126 This corresponds to the recommended truncation rule in the VDV core application standard,

on which the fahrCard is also based.

Only such information may be stored on electronic tickets

which are used to check the validity and the right of use

are required. The date of birth and full name are in

usually not required.

4.2 Driving school: data transfer to a

interest group

s

i

x

a

right

P

right

e

i.e

s

and

A

A driving school had contacted us because it was just a few days after receiving it

received an advertising letter from an interest group after their operating permit

congratulated on the opening of the driving school and for membership

advertised She expressed the assumption that the state office for civil and regulatory

affairs (LABO) as the responsible supervisory authority

could have passed on to the interest group.

The LABO confirmed this assumption and announced that the granting of a

driving license for driving schools not only because of legal obligations

e.g. B. the trade office and the Federal Motor Transport Authority will be notified, but

at his request also said interest group. The notification to the

band was created on the basis of the Berlin Information Freedom Act (IFG)

been shared.

The notification of the granting of the operating license to the interest group was

allowed. According to the IFG, anyone can obtain information about the content of the

files kept by a public body,127 if none of the

conclusions.128

In the present case, no personal data was already affected, since it was

the driving school is a legal entity.129 But even the

127 § 3 para . 1 IFG

128 § 4 para . 1 IFG

129 Personal data are according to Art. 4 no. 1 DS-GVO only such information that

relate to an identified or identifiable natural person.

ment that a natural person has an operating license for a driving school

granted would have been permissible. Concerns worthy of protection are open to

Disclosure of personal data according to the IFG as a rule, so

far it emerges from a file that the persons concerned are involved in an administrative

drive or are involved in any other procedure, and through this information

with the exception of certain core data130 no other personal data at the same time

Data are disclosed.131 The fact that a natural person is successful

involved in an administrative procedure for the granting of an operating permit

was, can therefore usually be applied for according to the IFG together with the core data

ten how name and address are disclosed.

Other reasons for exclusion were not considered, so that the transfer of the

information was lawful.

The transmission of personal data always requires a legal basis

position. Not only legal obligations to transmit come into play for this

costume, but also provisions according to the IFG.

4.3 Obligation to order data protection

commissioned by taxi companies

We have received several inquiries from taxi companies as to whether they are obliged to do so

be to appoint a company data protection officer.

Those responsible are obliged to appoint a data protection officer or a data

to appoint a protection officer, insofar as they generally have at least ten

sonen constantly with the automated processing of personal data

employ.132 It is irrelevant whether the processing of personal

A

and

s

i.e

e

right

P

right

a

x

i

s

130 names, title, academic degree, date of birth, occupation, industry or business

designation, internal function designation, address and telephone number, § 6

Section . 2 sentence 1 no. 1 IFG

131 § 6 para . 2 sentence 1 no. 1 letter a IFG

132 Section 38 para. 1 BDSG in addition to Art. 37 para. 1 letter b and c GDPR

73

data is carried out as a core activity, rather the regular automatic

tized processing.

One of the taxi companies employed six people in the office

employees who process personal data of passengers, as well as 30

Taxi drivers who carry out taxi journeys. For the question of

It was therefore necessary to check whether there was an obligation to order, whether the taxi drivers

and taxi drivers constantly with the automated processing of personal data

data were entrusted.

If the transfer of driving orders is carried out electronically, e.g. B. by terminal,

via radio device with the appropriate function or via app on the smartphone

the acknowledgment and acceptance of the orders as automated processing

view personal data. Something else can at best with regard to

Such orders apply that are not electronic, but rather by conventional means

radio device or in paper form. Since taxi drivers

but these days, as a rule, we also accept orders electronically

to assume regular automated processing.

Taxi companies are therefore obliged to appoint a data protection officer

to be appointed if they have at least ten employees in total

workers who process personal data either in the office or taxi

carry out trips after electronic order acceptance, employ.

A data protection officer or a data protection officer is always there

to order if at least ten people constantly using the automated

processing of personal data are entrusted. It doesn't have to be

are about a core activity of these people, rather that is already sufficient

regular processing.

4.4

Intelligent video surveillance in the train station

Berlin-Südkreuz

As part of the joint pilot project "Security Station Berlin South

kreuz" from the Federal Ministry of the Interior, the Federal Police, the Federal

minalamt and Deutsche Bahn AG (DB AG) have been systems since August 2017

of the so-called "intelligent" video surveillance. The project is divided into

two sub-projects:

In the first pilot project, the Federal Police tested the use of biometric

visual recognition systems.133 A database with light

created by over 200 people who volunteered to take part in the project. the

Systems should be allocated in specially designated indoor areas of the station

next record the faces of passing passengers, with those previously in the

Compare the image data of the volunteers stored in the database and ultimately de-

Filter out and count faces each time it is detected. That first test

was completed in July 2018. The one in the Federal Police's final report

through a combination of the three tested systems achieved high hit

quote was a very high false detection rate, i.e. a large number

triggered false alarms, opposite. Each one of these systems for itself pointed

even a significantly higher error rate.134 In their final report

the Federal Police goes from three to three for all three systems together

four false hit reports per camera per hour; on certain days

At present, the number of errors can be significantly higher.135 This means that

wrongly recorded about 80,000 to 100,000 people during the project

136 Despite this, the federal police reported that the facial recognition

133 JB 2017, 3.6

134 See the analysis by the Chaos Computer Club of October 13, 2018

135 p. 15 of the report Annex 3 - Analysis of the test data for sub-project 1 "Biometric

Face recognition", available at https://www.bundespolizei.de/Web/DE/04Ak-

tuelles/01Messages/2018/10/181011_final_report_face_recognition_down .

pdf?__blob=publicationFile

136 This number is calculated as follows: 365 days run time of the test x 24 hours per day x

three cameras x three to four false positives .

state-of-the-art systems are a good support tool

ment for the police manhunt could be.

We definitely see this differently. Innocent passers-by in the

According to the available results, Südkreuz station regularly got into trouble

drive to become the object of biometric data processing without it

there would have been a reason for it. In real operation there would therefore be a high

hes risk that a large number of citizens mistakenly

become the subject of police investigations. It would also be very questionable whether

the high error rate would not inevitably lead to a correct

hit would not be recognized as such, because far too many incorrect reports

gene would have to be sorted out by hand. In the last year before the pro-

blematic warned.137 For the final legal assessment of the data processing

However, the processing of this first sub-project by the Federal Police is the

from 2019 the Federal Commissioner for Data Protection and Freedom of Information

responsible.

In a second test scenario, the

Testing of so-called "intelligent" video analysis systems for treatment and

assessment of various risk scenarios. Helpless lying should be

people, large crowds of people and suspicious objects

matized by the data processing systems are recognized and reported.

For this purpose, it is planned to carry out concrete test

recreate scenarios in the station area, e.g. B. leaving a luggage

piece and tracing the person who left that piece of baggage.

Deutsche Bahn comes in handy for running the second test scenario

and responsible under data protection law and thus also we as the responsible data

data protection supervisory authority for Deutsche Bahn. As such, we urgently

advised not to use biometric data processing. Because due to

the fact that a biometric characteristic usually affects the whole life

If not changed throughout, such data processing involves considerable

security risks. A collection of biometric data is not only up to the

face recognition, but also for other data on physical, physical

Siological or behavioral characteristics, such as B. the individual

gait of a person.138 If the data is lost, those affected can lose their lives

become victims of identity theft and related crime for a long time. The assessment

biometric data is therefore always associated with a very deep intervention in the

environment and a considerable risk. Consequently, the

Processing of biometric data by non-public bodies after the

General Data Protection Regulation prohibited and only in narrow exceptions

permitted in all cases.139

Deutsche Bahn has agreed to take part in the test for the biomechanical

tric data. We closely monitor the project to ensure

that this requirement and other data protection regulations are complied with

will.

The processing of biometric data is associated with significant risks.

Therefore, these should be used extremely sparingly and only then by security authorities

be used if it is not too error-prone and after considering all

ler aspects a measurable added value for the security of the citizens

Citizens the restrictions of the right to informational self-determination

tion clearly predominates. The processing of bio-

metric data for the clear identification of persons in principle

prohibited and only permitted in exceptional cases.

4.5 Connected and Automated Driving – What data protection risks arise from the new techniques?

Technical progress is also very evident in the automotive sector. No

The main benefits of electromobility are networked and autonomous driving

important future fields. However, the improvements for road safety and

the increased comfort for the users of the vehicles can lead to data protection

A

and

s

i.e

e

right

P

right

a

x

i

s

138 Art. 4 no. 14 GDPR

139 Art. 9 GDPR

risk, since the technical aids are also increasingly data

detect the driver or the vehicle occupants. Negative effects would be

e.g. B. the creation of movement, behavior or usage profiles.

In the automotive sector, possible data protection

Legal risks increased significantly at the same time as technical progress.

This already starts with car rental companies, who now sell their vehicles to thieves

monitor steel avoidance usually permanently via GPS. This also applies to

assistance systems, which ensure the corresponding driving safety

functions can also call up a large amount of personal data from the vehicle

and evaluate. Another example are modern vehicles that already exist today

are able to exchange data with each other in real time and in the future

should even drive fully automatically.

Many of these modern technologies serve to increase traffic safety,

faster information acquisition for rescue workers and improved comfort

for the users and are therefore generally to be welcomed. Important here-

however, that the processes of data processing are transparent for those affected

rent, so that vehicle owners and drivers

and drivers can actively decide which surveys and processing

gen personal data you agree. Likewise, in the past

means consents given – e.g. B. to collect the vehicle location - also

can be specifically withdrawn. Technical solutions where

one only differentiates between the comprehensive consent to all data processing

or the complete renunciation of intelligent mobility services are

unacceptable. These claims have been valid since May 25, 2018

The GDPR is also anchored in law, because according to the principles formulated in it

cipien "Privacy by Design" and "Privacy by Default" are technical systems and

the default settings of the devices are as privacy-friendly as they are now

the technology.140 Furthermore, suitable technical and organizational

to take organizational measures to ensure a risk-appropriate

to ensure a level of protection for the security of data processing.141

140 kind . 25 GDPR

141 Art. 32 GDPR

This is all the more important as large amounts of data for the functions of the

tized and networked driving. So can in a modern

networked vehicle e.g. B. are not only recorded at what speed

the vehicle is moving and how many people are in the vehicle.

A lot of other information can also be recorded, e.g. B. whether the driver

signs of tiredness already show how his acceleration behavior is changing

represents or which seat and comfort settings the vehicle occupants

because you chose. Or also, which routes have been driven last,

how big the distance to other vehicles is, what condition the tires are in

or whether the vehicle is driving on a dry or slippery road. This

are just a few examples of a large number of generated data, which are

devices or sensors inside and outside the vehicles permanently

recorded, stored and processed. Part of this data is directly after

Collection and evaluation were discarded again, but a lot of data is definitely

also stored for a longer period of time (e.g. last driven routes, personal

positions of the various users of a vehicle, use of navigation

and media services, vehicle diagnostic data, etc.).

In this context, location and positioning

tion data to. These are not only used by various navigation and

further services processed in the vehicle, but u. also through the emergency call system

eCall system, which has been mandatory for all new models in Europe since October 2015

of passenger cars and light commercial vehicles is required. In the event of an accident

the vehicle is automatically localized and the local rescue control center can follow

communicate with the driver via a mobile radio unit. The radio unit is here

each equipped with its own SIM card, which is permanently installed in the car. Of the

eCall emergency call in its basic function is subject to strict regulations on the

tion of data protection, possible additional services by third parties (e.g. vehicle

manufacturer) are not covered by this. There is therefore a risk of

nes unauthorized retrieval of data about the vehicle or the driving behavior of the

Users in particular through private data processors whose services are in modern

Vehicle systems are embedded.

Networked and automated vehicles also use a variety of other

ter sensors to constantly monitor your own position compared to other drivers

testify both to the prevention and avoidance of accidents and to optimal

paint to ensure route planning.

Building on this, the automotive industry is already planning cooperative systems

for cars and trucks, through the vehicles and even the traffic information

be put in a position to independently communicate with each other

standing. This allows z. B. early traffic jam warnings and the calculation

suitable alternative routes through the respective navigation system. onboard systems

warn of possible dangers on the route or, if desired, look for them

next free parking space. Trucks could be automatically networked in co-

can drive in order to get to their destination in a fuel-efficient and environmentally friendly way.

The first test uses of this so-called Car-to-X communication already exist and should be

will certainly be successively expanded over the next few years. enabling

light this will e.g. also by building the next generation of significantly

more powerful mobile networks, the so-called 5G networks142. The significantly faster

Higher data rates in the mobile internet enable vehicles to be networked

and transport infrastructure, but at the same time produce higher risks

through the transmission of personally identifiable information to the mobile device

(e.g. number of SIM card used, IMEI number of mobile device)

or by information about the vehicle (e.g. ID of the connected vehicle,

sign, vehicle identification number). The data obtained can be used, among other things, to

Create movement and usage profiles. Also the frequency of use

nes vehicle and the number of different vehicle drivers can be derived from this

determine if necessary.

Building on the scenarios already described, there have now also been

developed other possible uses in other lines of business, which

have to be looked at closely. For example, the insurance industry offers B. since a

In recent years, optional telematics tariffs143 have been increasing, which are based on a precise

Recording and analysis of all routes and numerous details (e.g.

frequency of trips, average length and duration of trips, time of trips,

selected destinations, driving style, etc.) extensive conclusions about the respective driving

142 5G stands for “5 . generation" of mobile networks.

143 These are often referred to in English as “pay as you drive” tariffs.

allow customers to behave. policyholders who

willingly agree to the necessary data recording, will in return

a discount on their individual insurance premium. Of the

European Association of Insurers has already expressed an interest in

that its member companies may also have access to the eCall data in the future

of their customers should receive in order to still be able to

to adjust more precisely.

Basically, new technologies to increase road safety and

accelerated care for accident victims and to improve the

flow of traffic certainly welcome. Nevertheless, with all the advantages, too
the risks of the new technologies are not ignored. Nearly
every technology also harbors corresponding risks of data misuse. So bends
the permanent location of a vehicle may indicate theft,
However, it also enables the creation of motion profiles. When charging
of electric cars is also regularly charged at least for billing purposes
a personally identifiable ID of the customer by the respective
Provider recorded in order to be able to allocate the charging process during billing.
Telematics offers, on the other hand, usually require a large amount of data from vehicles
collect so that the technology works effectively. This is often accompanied by
automatically a technical surveillance of the drivers. Regarding
of the networked and automated vehicles of the future are the automotive
industry and the branches of industry associated with it (e.g. suppliers and
insurance companies) as well as politics and administration are therefore requested
to sensibly reconcile technical progress and data protection.
In terms of improving traffic safety and for increased
many of the new technologies in the automotive sector have
from welcome. However, here should always be between the expected
Benefits of the technology and possible risks for data protection weighed
become gene. In addition to data security and data protection,
especially the transparency of the providers towards the customers
important to customers so that they are always fully informed about which ones
Data, if any, collected and for what period of time they are stored and
which departments have access to the data. The technologies described

will also be used in Berlin in the future and possibly by Berliners

providers are further developed. We will continue development therefore

observe carefully.

5.1 Adaptation of the Berlin School Act to the GDPR - All's well that ends well?

A

and

s

i.e

e

right

P

right

a

x

i

s

We supported the Senate Department for Education, Youth and Family in adapting

adaptation of the Berlin Schools Act to the GDPR. This process went

not smooth from the start.

Although the GDPR has direct effect in all member states of the EU

European Union, but contains the so-called opening clauses in many places

leeway for national legislators. At the same time they are

Member states required all national regulations that regulate the

processing of personal data, on their processing

to check compatibility with the European legal requirements. A corresponding one

The Berlin school law, which contains the relevant data

processing powers for the schools, school authorities, school inspectorate

etc. contains to undergo.

The draft bill that was presented to us in March 2018 continued the

protection regulations are still very inadequate. In particular contained

the draft does not contain any regulation that is compatible with the requirements of the GDPR

Processing of special categories of personal data. Which includes

e.g. B. Health data of the students or information about their

religious or ideological beliefs. Furthermore, e.g. B.

Work authorizations for parent representatives, who are also involved in everyday school life

processing of personal data are involved.

Unfortunately, the senate administration did not follow us further in the revision

process involved. In summer 2018 we had to send a press release

division that a new draft has already been submitted to the Senate

was. In it, the senate administration had our criticism in essential points

83

who was not picked up. We have our criticisms of the Senate

administration then made it clear again. We were finally able to reach

that some regulations have been adapted to comply with data protection regulations. The School Law

now contains e.g. B. Clear regulations for the processing of special categories of personal

sun-related data.

So all is well that ends well? - Not quite.

Because the law that has now been passed continues to contain one thing in particular

very problematic rule. From now on, the school law justifies e.g. one

Authorization for the school supervisory authority to use the data of pupils

learn under certain conditions even after leaving school

process them e.g. B. to provide vocational training.144 This is already

therefore not acceptable because the persons concerned are regularly involved

those who are no longer going to school and therefore not either

are no longer subject to the regulations of the School Act. Of course school should

is about preparing students for working life

To take care of. But this should be done during school, not after. It

does not belong to the statutory tasks of the school supervisory authority, such

To organize measures for former students, regardless of whether

have this need or not, because they z. B. no longer live in Berlin or

have long since oriented themselves professionally. Such a measure can therefore

are only offered as an additional service for voluntary acceptance.

A storage of personal data of alumni can accordingly

also only take place on a voluntary basis, namely when the persons concerned do so

accept the offer as useful. The legislature should

therefore reconsider the divorce and the next time the

Improve the school law at this point.

With the adaptation of the school law to the DS-GVO, a major

challenge mastered – even if not satisfactorily in every respect.

Now it is also the School Data Ordinance, which is currently being revised

to bring it up to date and to enforce it quickly.

144 Section 64 para. 7 in the version of the 1 The school law that came into force in January 2019

A

A

and

and

s

s

i.e

i.e

e

e

right

right

P

P

right

right

a

a

x

x

i

i

s

s

5 .2 Implementation of the GDPR in child and youth welfare

5.2 Implementation of the GDPR in child and

youth welfare

Since May 25, 2018, youth welfare offices and numerous private

independent organizations of child and youth welfare organized under VAT law

to apply the provisions of the GDPR. In practice there is a high information

required in view of the changed legal situation.

We have received numerous requests for participation in information events

reached. We were not able to handle all requests for lectures due to our

meet limited capacities. We focused on that, if possible

to reach many multipliers. With the social pedagogue

Technical Training Institute Berlin-Brandenburg (SFBB), which is responsible for further training

of the pedagogical specialists in the child and youth welfare of both federal states

who is responsible, we have a specialist event on the GDPR in June 2018

carried out in which more than 100 educational professionals took part.145

The aim was to give the participants an initial overview of the effects

of the new European data protection law on the practice of children and

to give assistance and the relationship to the regulations of the social data protection

to light on the right. Due to the high response to the event,

there will be an in-depth specialist conference in spring 2019, in which we will be active again

involved.

In child and youth welfare, even after the GDPR has come into effect

− as before − the area-specific provisions of the social code books146

apply. While the federal legislature the regulations of the SGB I and

SGB X adjusted before the GDPR came into effect, such a one is available

Adaptation for what is primarily authoritative for child and youth welfare

SGB VIII still pending. For professionals, the challenge is in practice

is to apply the various sets of regulations side by side.

145 The conference documentation can be downloaded from the SFBB website,
https://sfbb.berlin-brandenburg.de/sixcms/detail.php/873533/

146 Social Code - First Book - General Part (SGB I), Social Code - Eighth Book - Child and Youth Welfare (SGB VIII) and Social Code Book - Tenth Book - Social administrative procedures and social data protection (SGB X)

The DS-GVO results in the handling of social data when granting
Child and youth welfare services (e.g. educational assistance, but also
in dealing with child welfare hazards) no serious changes, since
the prerequisites for the admissibility of data processing are within the framework of
Opening clauses for the law of the Member States continue to derive from the social and
data protection regulations.

There are innovations, however, e.g. B. in the case of child and youth welfare
information obligations to be observed or the extended rights of data subjects
according to the DS-GVO.147 We were here on quite understandable practical
Problems drawn attention to: Especially in the case of telephone consultations (e.g. in
crisis situations) or in advising young people in precarious
situations for which the inhibition threshold to accept advice is high anyway
there is a risk that written declarations of information will miss their goal
are absent and act as a deterrent. Here it is important to find practicable solutions
to find songs. These must primarily be in the interests of the persons concerned
be. Because of the transparency and building a relationship of trust in
the contexts are of particular importance anyway, we keep it
from suitable, the information requirements also in the context of explanatory
to comply with discussions with appropriate documentation.

The effects associated with the GDPR for practice is currently in

to dedicate to togetherness. It is important to us that child and youth welfare is here

to support.

147 art. 13 et seq. GDPR

5.3 Uniform specialist procedures in the Berlin Youth welfare - progress report

Also this year new modules of the cross-administrative

Specialist procedure ISBJ-Jugendhilfe (SoPart), which as a central specialist procedure in all

twelve Berlin youth welfare offices are used148, by the Senate administration

tion for education, youth and family has been taken over into real operations.

The cross-administrative major project Integrated Software Berlin Youth

hilfe (ISBJ) has been with us for many years. The currently introduced central IT solution

tion for all district youth welfare offices had to be revised this year

be adjusted by the GDPR. For example, a privacy policy was too

develop in order to comply with the information obligations149 for the data subjects

get. We have the lead for the introduction of the specialized procedure

Senate Department for Education, Youth and Family in preparing a legal

declaration made available centrally for the districts early on May 25, 2018

advise on data protection law. This will certainly be due to the first practical

technical experiences with the GDPR can be evaluated after a certain period of time

have to. In addition to the data protection declaration, some technical processes for

Guarantee of data subject rights (“information at the push of a button”) in the specialist

implement procedures and records of processing activity150

to create. For the new modules to be used, the new instrument had to be

Data Protection Impact Assessment151 are applied.

This year the new module youth job assistance for those in the youth

employment agencies employ specialists from the district youth welfare offices in the real

operation taken over. The access possibilities of the youth job assistance within

of the specialized procedure on the youth welfare data in the other organizational units

ten of the youth welfare office we have with the youth department of the senate administration

148 JB 2016, 5.4; JB 2017, 2.3

149 Art. 13 et seq. GDPR

150 species. 30 GDPR

151 Art. 35 GDPR

for education, youth and family. In the specialist procedure,

ensures that only the necessary data can be accessed.

Finally, with the youth department of the Senate

Administration for Education, Youth and Family a clarifying provision in the

Implementation Act for the Child and Youth Welfare Act (AG KJHG) with the

data protection regulations for data processing, which the

natsverwaltung to the federal government responsible for adapting state law to the GDPR

leading Senate Department for the Interior and Sport.152

Coordination with the youth administration took place again this year

uncomplicated and constructive. The requirements of the GDPR have been

than in most other areas of administration - in time for

Implemented May 25, 2018. It is important to us that the implementation of the

GVO standardized specifications for data protection through technology design

to accompany the ISBJ specialist procedure in an advisory capacity in the future as a positive

Example of the implementation of data protection requirements.

5.4 Data protection in day-care centers - How good are they

Data of our youngest protected?

s

i

x

a

right

P

right

e

i.e

s

and

A

The fact that day care centers with the data of the children entrusted to them

Dealing with data protection issues is particularly important to the parents. But also in

the day-care centers themselves, there is often uncertainty, as with the

data of the children and their families is to be handled.

Especially in connection with the entry into force of the GDPR, the Unsi

security at the facilities for data protection-compliant handling of personal

ment-related data increased again. Dealing with photos,

design of declarations of consent, but also the use of new technologies

such as B. Apps with which the children's drop-off and pick-up times are recorded electronically

or information from day-to-day daycare is made available to parents

152 For the adjustment of state law, see Annual Report 2018, August 1

again and again leads to data protection questions from the parents,

but also in the facilities. Both the requests for advice and the

Difficulties in this area often relate precisely to these topics.

In the context of complaints, it is our concern for the future data protection

achieve fair practices. However, within the scope of our

rer capacities e.g. B. often not possible, declarations of consent abstract

to check whether they are in accordance with the data protection regulations

writings stand. Most frequently we receive questions about how to deal with photo and

Video recordings of children in day-care centres. The “Privacy Policy

for image, video and sound recordings − What is closed in the day-care center

observe?”153, which we submitted at the beginning of the year together with the Senate

tion for education, youth and family154 has in practice

met with a great response, also beyond the state of Berlin. Our concern was

it, the pedagogical specialists with the action guide in practice-oriented

way to give an overview of the complex legal situation. We have im

In the interests of comprehensibility, it is deliberately largely avoided being concrete

Quoting regulations and laws. Since the strict requirements for the effective

validity of declarations of consent even before the GDPR came into effect

were anchored in German data protection law, the text of the

The content of the guide also meets the requirements of the GDPR. However, as we

be asked to explain the extent to which the brochure reflects the legal situation

even after the GDPR has come into effect, we have decided

create an additional information sheet. In this the relevant

specifically named in accordance with the article of the GDPR. With the next edition we will

then integrate the relevant provisions into the text.

The feedback on the action guide shows that it

support for more legal certainty when dealing with data

protection issues in day-to-day daycare. We are planning to extend the range of information for children

to expand the day-care facilities in the future.

153 The guidelines can be accessed at https://www .datenschutz-berlin .de/file-

admin/user_upload/pdf/publikationen/ information materials/2018-BlnBDI_Flyer_

Privacy_Content_Web .pdf .

154 JB 2014, 4.1; Annual Report 2015, April 6th; JB 2017, 6.5

89

5.5 Data protection and media literacy –

Children's website www.data-kids.de online

s

i

x

a

right

P

right

e

i.e

s

and

A

The Berlin Commissioner for Data Protection and Freedom of Information has decided to

Aim set in children as early as possible awareness of the protection of their

data to wake up. That's why we've been working on age-appropriate materials since 2016.

to educate children of primary school age about how they

be able to exercise their right to informational self-determination and

how they should behave, especially online.155

From a developmental psychological point of view, children from around the age of seven are capable, too

assess longer-term consequences. It can be assumed that

Children from the 3rd grade can develop an awareness of data protection issues

to. The sooner we support you, the more media-savvy and therefore

They can participate in social life more diligently and responsibly

exercise their right to informational self-determination

and train skills for the digital world.

We launched our children's website www.data-kids.de in spring 2018

Offer on which children know the most important terms relating to data protection

can learn. A family of robots accompanies them through the data protection

world and explains what the right to informational self-determination is about

himself. In initial materials for teachers, we explain what cookies and the

are entitled to their own image and how children can protect their own data.

So that the children can identify with the robots, we called

a competition in which elementary school children choose names for the robot children

should consider. The then class 3b of the elementary school on won

Tegelschen Ort.156

After we have created the basic structures and most important content of the website

and developed the characters, we presented ours in the second half of the year

155 JB 2017, 6.6

156 See also 14.5

website, also with the help of feedback from elementary schools, on the test

was standing.

In the coming year we will further optimize the children's offer in order to

to reach the target group even better. Specifically, we will use the existing ma-

check materials for child-friendly language and, where necessary, adapt them. the ele-

ments of the website we will be interactive and playful, but in any case gra-

make fish even more appealing.

Our goal is to expand the website to a comprehensive offer,

with which teachers, parents and children exercise their data protection competence effectively

can strengthen.

5.6 Digital Parental Allowance – An Innovative Project?

As early as 2017, the Senate Department for Education, Youth and Family included us in the

Project initiated by the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth

included in the “Elterngeld Digital” project. Applicants should be able to

Applications for payment of parental allowance via a form provided by the Federal Ministry

submitted internet portal digitally.

A

and

s

i.e

e

right

P

right

a

x

i

s

The aim of the “Elterngeld Digital” project is to digitally process the granting

of parental allowance to the beneficiaries. Since the federal parental allowance

is a federal benefit, but it is processed by the parental allowance offices

of the federal states, they are responsible for the decision on the applications.

The Senate Department for Education, Youth and Family has agreed to

participate in the federal pilot project. With regard to the question of legal

We are also committed to the processing of social data by the state of Berlin

involved in the project.

While everything was well prepared on the Berlin side, the project was running on the part of the

Federal rather sluggish. With a one-year delay, the project was

started in autumn 2018 with the so-called application assistant. parents can

Although they fill out their applications online with the help of the assistant, they still have to use it

continue to send them by post to your responsible parental allowance office. a complete

91

Digitalization of the application is currently still failing because a

There is no legal basis in the Federal Parental Allowance and Parental Leave Act (BEEG).157 That

The Federal Ministry for Family Affairs is responsible for data protection

social data and

requires a legal basis for the processing. Since the collection of

data with the application assistant on the part of the federal government, this is also

for authenticating the applicants and obtaining the necessary

responsible for declarations of consent. We therefore had to contact the Senate

ultimately inform you that we will not be able to carry out the planned procedure due to a lack of

unfortunately not able to evaluate data protection law.

The comprehensive introduction of digital offers is definitely desirable

value. However, we consider it necessary to comply with data protection and

technical requirements of the GDPR already during the development and the

Implementation of procedures to consider in order to benefits then also

to be able to offer completely digitally from the outset.

5.7 Please smile! video and audio recording

now in the classroom for research purposes

s

i

x

a

right

P

right

e

i.e

s

and

A

School education is a popular field of research. Usually they will

Pupils and teachers in this context

asked to fill out questionnaires from the researchers. want more

Scientists but also additional audio and video

make deo recordings of individual lessons or units in order to

on the basis of which to gain further insights for educational research

to. This raises data protection issues that are being addressed by those responsible

already considered during the conception of the study and brought to a solution

should.

157 A legal basis in the BEEG is to take effect on 2 Data protection adjustment and

legislation EU − 2 . DSAnpUG-EU – to be created.

The differences to classic forms of survey, such as those using question

arc, are obvious. The surveys carried out with classical means

are regularly pseudonymised. In the case of questionnaires, this means that

these are not provided with the names of the participants, but

each with an identification number or code. When filming the

terichts is to proceed similarly. When recording a lesson

should the researcher e.g. B. are a seating plan that instead of names of

respective students also contains codes. In this way

in combined surveys, e.g. B. also the recordings with the

words are linked in the questionnaire. In this way it can be ensured that

a follow-up survey some time later, the answers from both

assigned to the same person and compared

can, without the researchers for this purpose also the

Need to know the respondent's name.

Of course, these are also personal data

data records provided with identification numbers or codes. Because mostly

a list remains in the school showing which respondents are behind

what numbers hide. This list can still be used to assign

tion of the pseudonyms and thus also of the answers to a specific person

be made. This list must therefore be deleted as soon as the

preservation is no longer required for the conduct of the study.

But even deleting this assignment list is not always enough

under certain circumstances also concrete answer combinations lead to an identity

identifiability of the participating person.

With video and audio recordings, identifiability is always given. So

are naturally the faces and voices of the students on these recordings

to recognize students and teachers, so that this data

always remain personal depending on the assignment via a number.

This results in data protection requirements that apply from the start

are to be taken into account:

The data protection basis for the processing of the data in question

Data is regularly the consent of the persons concerned or their personal

custodians. This goes hand in hand with the fact that these people also

must be clear about what they are actually consenting to. The purposes of the data

processing must be sufficiently clear and presented in an understandable way.

This applies in particular to information aimed at children.158 Im

to speak in connection with video recordings of anonymized data,

is generally prohibited for the reasons given. In addition, the affected

Individuals have the right to revoke their consent at any time with effect for

revoke the future. So those responsible have to find a way

to ensure that in the event of a revocation the recordings are actually for

future uses will be deleted or at least made unrecognizable in a way

be made which excludes the identification of the person concerned.

Likewise, those responsible must address the problem at an early stage, such as with

to deal with the content of the recordings. Because an identification is not

based on voice or face alone. Also the recorded ones

Statements themselves or the interactions in the class association sometimes give

information about the identity of the persons involved. That's how it should be in the

School lessons regularly happen that the students of

be called by the teacher's name or the students

Conversely, address the teacher by their name.

Last but not least, it must be ensured that pupils for whom no

approval is not also included in the recording. you single

Positioning it outside the field of view of the camera is generally sufficient here.

don't run out. Because despite the avoidance of image recordings, this

Procedure nevertheless recorded their voices when those affected are on

participate in lessons.

The use of video and audio recordings for research purposes raises new

Problem areas that have to be taken into account when designing studies

are.

158 art. 12 para. 1 sentence 1 GDPR

6 health and care

6.1 Judgment on the quality assurance process of

Association of Statutory Health Insurance Physicians in Berlin

After we passed the Quality Assurance Agreement eight years ago,

drive of the Association of Statutory Health Insurance Physicians (KV) with regard to the collection of personal

have complained about identifying patient data,159 is now in one

parallel social court proceedings between the complainant

ing doctor and the KV on May 9, 2018 the judgment of the State Social Court (LSG)

Berlin-Brandenburg in Potsdam.160 In the underlying case

did the doctor concerned have the transmission of identifiable

patient data and submitted a corresponding complaint

addressed to us.

A

and

s

i.e

e

right

P

right

a

x

i

s

The LSG Potsdam determined in the second instance that the quality control

ing guideline of the Federal Joint Committee, which requires a pseudonym

mation of the patient data does not expressly provide for this

Time (2011) applicable § 299 paragraph 1 sentence 1 no. 1 and 2, paragraph 2 Social Code

- Fifth Book - Statutory Health Insurance (SGB V) has violated. the

Regulation of the SGB V wrote in the old version the pseudonymization of the pa-

client data for the purpose of quality assurance. With that

our legal opinion represented towards the KV Berlin confirms that

Diglich pseudonymized patient data may be transmitted to the KV.

However, the judgment of the Higher Social Court is not yet final, as

probably the Federal Joint Committee and the KV Berlin against the verdict

have lodged a non-admission complaint with the Federal Social Court. There

with the new regulation of § 299 SGB V a quality assurance regularly

may only take place under pseudonymization of the patient data, the KV has

decided on the basis of the judgment to carry out quality assurance by collecting identical

159 JB 2011, 7.2.8

160 LSG Berlin-Brandenburg, judgment of May 9, 2018 - L 7 KA 52/14

data until the Federal Social Court has clarified

put.

We see the judgment as confirming our legal opinion that

quality assurance by KV Berlin patient data only in pseudonymous

ated form may be collected. The quality assurance by the KV is

also subject to the pseudonymization of patient data

feasible and at a reasonable cost.

6.2 Prostitute Protection Act – Data Protection

compliant implementation in the state of Berlin?

s

i

x

a

right

P

right

e

i.e

s

and

A

With the Prostitute Protection Act, the federal legislature has created a legal framework

introduced legal prostitution conditions. It is regulated under

other things, the obligation to register and to provide health advice for the pro-

established. As early as 2015, we wrote about the draft of the Prosti-

161 The law came into force on July 1, 2017

came into force and had to be implemented in all federal states, including Berlin

will. According to the regulation on determining responsibilities for the implementation

The district office is responsible for implementing the Prostitute Protection Act of December 12, 2017

Tempelhof-Schoeneberg from Berlin for the registration as well as the health

Advice on the Prostitute Protection Act responsible for the state of Berlin.

Both when registering and when providing health advice after the

stitute protection law, personal data of the prostitutes are

in particular data about sex life and health data.

Due to their sensitivity, there are personal

drawn data, an increased need for protection, which is particularly important against

due to the entry into force of the General Data Protection Regulation on May 25, 2018

must be taken into account in the implementation of the procedure.

161 JB 2015, 7.1

That's why we have the Senate Department for Health, Care and Equality

for more information on the registration process and health advice

asked.

The Senate Department for Health, Care and Equal Opportunities has given us, among other things, ge

answers that the Prostitute Protection Act has data protection issues

already consider. European regulations on data protection would also apply

respects, so that the Senate administration does not intend to carry out further content-related

managed to create. One considers the federal regulations in this respect

for sufficient. In addition, the Senate administration informed us that they

only have a coordinating role and therefore no further provisions on

Design of the procedure meeting could. We had to

assume that the Senate administration does not intend to use the statements we have made

Concerns, especially with regard to the implementation of the requirements of the GDPR

with regard to the processing of special categories of personal data

ten to pick up. This is particularly problematic in light of the fact that

the information from the Senate administration that European requirements have been taken into account

been, is not correct. The explanatory memorandum relates to the directive

95/46/EG, but not on the GDPR. In particular, the requirements for

processing of health data, which due to their special need for protection

are expressly regulated in the GDPR are not taken into account. given

However, due to the particular sensitivity of the processed data, we see it as extremely

Extremely important to this, also when introducing the procedural processes for the

Registration and health advice should be respected from the outset.

We will implement the prostitute protection law in the state of Berlin

keep an eye on. We have the district office Tempelhof-Schoeneberg from

Berlin contacted and an offer for advice with regard to the data

protection-compliant implementation.

6.3 Problematic introduction of an electronic

niche health record

s

i

x

a

right

P

right

e

i.e

s

and

A

Due to complaints, we contacted the offer of an electronic

Health record apart, the patients to manage

medical records can be used.

The legislature allows health insurance companies to use electronic health records

support financially. These should serve to ensure that insured persons determine their own documents

to keep them safe and to bring them into the further treatment.

The health and health insurance companies involved want these files

also like to use them to specifically address their insured persons.

The offer of the health record is based on the consent of the users

user. The consent for the various purposes and functions must

alities are each granted separately and expressly. The audited project

has grown dynamically over the course of the year. New functions are constantly

nalities added. However, the users were not

sufficiently informed and the now necessary new consents not

fetched. At our intervention, this defect was subsequently remedied.

The provider of the checked health record operates the health record

a large cloud service provider. The insured receive an app for her

mobile phone and use it to control the file. Would patients like to

medical record a document from a treating doctor

receive the doctor, then they communicate this via the app and the provider contacts them

send an e-mail to the doctor concerned. The doctor

or the doctor is given the opportunity to submit the relevant document

to upload his or her web browser to the file. become in this process

the documents are encrypted.

Before doctors can legitimately do this, they must be satisfied that

the patients really want this transmission. sign for it

the patients enter a declaration of release from confidentiality within the app

the screen of your mobile phone. However, it is difficult for doctors to

whether this document actually comes from the right person. Of the

Provider verifies patients' identity, but not in a way that the

sensitivity of the health data processed later. Consequently

should physicians determine the wishes of patients in other ways, e.g. e.g.

presence of patients in the practice.

Of course, the transfer process of the data must be designed securely

the. An independent research team had in the specific product in

found security gaps during this process, which the provider later fixed.

However, the procedure leads to a new weakness in the practices of the

transmitting physicians: Internet-connected computers from

Doctors can become objects of attack. According to the recommendations supported by us

regulations of the German Medical Association, doctors should use unencrypted medical information

Do not transfer documents to computers that have free access to the Internet.

At present, however, the health record can only be read from such a computer

add from documents.

Even the fact that someone is treated by a certain doctor

treated by the right doctor is to be kept secret, since conclusions can be drawn from this

in the way of a disease. The query of the documents at the

medical service providers at the time of the audit, however,

encrypted. We have asked the provider to change this.

Ultimately, the data processing of the provider of the healthcare

files meet even the highest security requirements. The already mentioned

scherteam had found further gaps in the security of the offer. Also

In the course of our audit, we identified weaknesses. A data protection consequence

In addition, the gene assessment was carried out belatedly and incompletely.

In 2019 we will influence the company so that established standards

standards for the security of such services are consistently complied with and

the same level of security is achieved as required by the law of electronic

cal patient files required.

99

Electronic health records offer patients the opportunity

ability to store and process their health data in a central location

prevail. However, the advantages that can result from this should not be included

be paid for a weaker protection of the data. The data protection law

specific requirements must therefore already be taken into account during the conceptual design

relevant offers are observed and implemented.

6.4 Babylotse Plus: Extension to all Berliners

maternity clinics

s

i

x

a

right

P

right

e

i.e

s

and

A

As part of the "Babylotse" project, expectant mothers are

so-called Babylotsen – available to provide support with difficult

current family situations and the family in dealing with the new

accompany the situation after the birth of the child.

After the “Babylotse” project at the Charité in 2014 as part of

of a research project and accompanied by us in terms of data protection law

has now been decided to carry out this important project in all areas

liner maternity clinics. To implement also in terms of

to accompany data protection regulations, we are in contact with you at an early stage

the competent Senate Department for Health, Nursing and Equal Opportunities

taken. In November 2018, we met the data protection requirements

ments presented to the advisory committee and have agreed to continue the project in the

to continue in 2019.

In order to gain the trust of expectant mothers for the "Babylotse" project,

to win and to be able to carry out successfully, it is next to the concrete

Offers of help important to ensure the necessary confidentiality and

ensure that the data protection requirements in the project are

be set.

100

Chapter 6 Health and Care 6 .5 Charité: New Law – Old Problems

6.5 Charité: New Law – Old Problems

This year, too, we have accompanied the rectification of the deficiencies that we intend to do

three years at the Charité, and to a speedy implementation of the

urgently required measures.162 The

Senate Chancellery, Department of Science and Research, as the responsible specialist

view of the Charité.

A

and

s

i.e

e

right

P

right

a

x

i

s

Before the General Data Protection Regulation (GDPR) comes into effect on May 25th

In 2018, the Charité was obliged to review every procedure for processing patient

or subject data of a prior check based on a risk analysis

and subject to a security concept. This obligation is the Charité

not complied with in the past.

With the GDPR, this requirement now exists in the form of the obligation to

Carrying out a data protection impact assessment for all newly introduced ones

procedures with high risks and for the procedures for which, despite

obligation no regular prior check has been carried out. We have im

October 2018 checked whether the deficits have been processed. The result was

sobering up:

Even five months after the GDPR came into effect, the Charité had no

Completed a data protection impact assessment procedure. only at

Two procedures have been working on conducting an impact assessment

began. The Charité itself estimates that it is responsible for more than one hundred

driving must make such assessments.

We could positively note that the Charité as of October 2018 at least

has created a complete overview of the processes operated. This is first

targeted control of individual projects is possible. The Charité also helps

this directory to control and monitor its own data processing

chen.

162 JB 2015, 8.4.1

Nevertheless, this is only a first and comparatively small step: every procedure
Risks with high risks must be described systematically. The risks have to be there
specifically identified and evaluated. Then it must be determined how
accordingly be reduced.
The Charité already lacks a systematic description of the individual
Procedure. There is a general catalog of risks, but nothing specific
for the respective processing operation. There is also a general
ten and also incomplete catalog of measures to be applied centrally
men. However, specific specifications are needed for both the central
IT operation as well as for processing in decentralized responsibility. your family
These requirements and measures should then be summarized in the statutory
find prescribed data protection concepts. Their absence three years ago
led to complaints from our authorities. As before, lies for
no procedure suggests such a concept.
In the case of some specific technical security measures, on the other hand, certain
Progress can be reported, even if not yet fully implemented.
The information security officer, who was appointed mid-year
res started work at the Charité in 2018. Unfortunately, the Charité is one
Adequate staffing of data protection management to the end
of 2018 failed.
The Charité is still faced with the task of dealing with the risks involved in its procedures
for the persons concerned to assess the necessary technical and organizational
to determine safety measures with a risk analysis, these in
to systematize security and data protection concepts and finally
consistently implement the defined measures.

6.6 Online service provider: Handling of personal related data in the medical sector

As can be observed in many sectors, the offers in the field of Mediation of medical services increasingly on the Internet. Through We are a complaint to a Berlin-based service provider from this area that includes a wide spectrum of medical clinical services from all over the world.

A

and

s

i.e

e

right

P

right

a

x

i

s

Anyone who wants to process health data without providing medical services themselves provide, regularly requires the express consent of the persons concerned Persons. And only those who are aware of the intended processing, its purposes, who is informed of the status and risks can give effective consent. various Providers of online services shy away from the information and collection of Efforts associated with consent. Especially since they run the risk of becoming one

well-informed person might reconsider their offer

gain weight.

The provider we tested acted the same way. He challenged the future

diners and customers, in advance extensive information about

provide their health before providing them with information about the

seen data processing and an input field for the explanation of the

consent confronted. For the first contact, a registration form had to be

be filled, which split into two sides. On the first page should the

future customers describe their respective concerns and if possible

Provide medical records, X-rays or photos. At this time

the provider has not yet explained the processing of the sensitive data,

although the data collected includes the files selected for upload

was already transferred to the company during the transition to the second page

the. Only on this second page was there a reference to a detailed

privacy policy asked for consent.

We contacted the company and complained about the illegal collection

practice of the data. This was initially denied by the company. First

in view of the irrefutable evidence, the company admitted the

ler and agreed to redesign the data processing. A review

is still pending.

When health data is collected online, processing may only

follow after the intended handling of the data has been explained and

the data subject has given their express consent.

6.7 A care service on Cloud International

s

i

x

a

right

P

right

e

i.e

s

and

A

In response to a tip, we audited a care company that had a wholesale

part of the medical information about the person to be cared for that is necessary for the care

People stored at international cloud companies, their employees

are not subject to any statutory duty of confidentiality.

Care providers are subject to the same confidentiality obligations as doctors

Doctors. Those who confide in them should be sure that nothing about their health

means got to the outside. Like other secret carriers, you can use service providers

take advantage of. However, it must then be ensured that this one

subject to a similar duty of confidentiality. For German service providers

the legislature regulated this confidentiality obligation.163 In the case of international

For service providers, this depends on the extent to which the respective country is appropriate

issued secrecy regulations.

We have asked the relevant care provider to ensure

that data is only processed by service providers for whom these prerequisites

tion is fulfilled.

Health professionals need to be careful of them

processed data about their clients also with the

claimed service providers are processed in accordance with data protection regulations.

163 § 203 para . 4 sentence 1 StGB; see also JB 2017, 7.6

104

Chapter 6 Health and Care 6 .8 Clinical Cancer Registry: Long-term retention of registration forms

6.8 Clinical Cancer Registry: Overlong Retention

maintaining reporting forms

Two years after the opening, we officially checked the conformity of the

Data processing of the joint clinical cancer register of the federal states

denburg and Berlin with the legal regulations.

The clinical cancer register collects comprehensive data on all cases of cancer

sick people in the states of Brandenburg and Berlin, including the diag-

noses and details of treatment. The data processed in the register

are therefore highly sensitive. They will be provided by the treating hospitals

and resident doctors reported. They are legal for that

obligated. Patients have a limited right to object

Law.

A

and

s

i.e

e

right

P

right

a

x

i

s

Shortly after opening in 2016, we already had

Burger colleagues run the Potsdam branch of the cancer registry

checked.164 The register subsequently corrected some of the deficiencies identified.

ben. For others this is still pending. This year the test focused

ment to the Berlin branch.

In the cancer registry state agreement between the countries involved is detailed

specified how the cancer registry should deal with the incoming reports

Has. i.a. defines how data is stored long-term and when it is deleted

Need to become.

In the course of the examination, we found that the register next to the

Main database, which is kept in a specially secured database,

maintains a second database of electronic copies of registration forms. there

we found data that lasted two years for those affected from Berlin, from

denburg go back to 2004. The legal regulation provides

compared to that the data from the registration forms within six weeks

are to be recorded electronically. After recording, the registration forms are to be

164 JB 2016, 1.3

nieces. Thus, the data storage transcends both by type – the names

of the patients are separated from

to store the medical data - as well as in terms of time from

limits set by law.

It is also one of the legal requirements for register keeping that

the direct retrieval of data is blocked after a specified period of time and this in

be deleted according to the prescribed cycle. Despite a practice operation from

For two years now, the cancer registry has not had a concept for blocking

and demonstrate the deletion of data.

The highly sensitive and comprehensive storage of data on cancer

diseases in the clinical cancer register must strictly adhere to the legal

oriented guidelines to prevent the interference with the rights of those affected

as low as possible and risks of data leaks or data mis-

need to minimize.

6.9 Individual Cases

6.9.1 Medical certificate for admission to day care centers

s

i

x

a

right

P

right

e

i.e

s

and

A

We received a medical certificate form from a pediatrician,

which had to be filled out for admission to a day-care center. The infection control

law stipulates that before being admitted to a child day-care facility

vaccination advice is given, which is confirmed by the treating pediatrician.

However, protective measures that have already taken place should also be

vaccinations are specified.

However, the indication of previous vaccinations can only be given voluntarily.

genes, since there are no legal obligations for carrying out the vaccinations themselves.

obligation. We were able to get the form adjusted so that everyone

information that goes beyond the mere confirmation of the advice given

in the future exclusively on a voluntary basis with the consent of the parents

be made.

6.9.2 May doctors use patient data

disclose to rating portals?

Patients have the opportunity to

ability to evaluate doctor visits and medical treatments. Unless the

respective doctors with these publicly accessible ratings

If you do not agree, there is the possibility of having them contacted by the portal operator

checked and to submit their own representations of the facts.

A

and

s

i.e

e

right

P

right

a

x

i

s

We received several complaints that were submitted as part of the counter-notice

identifying patient data disclosed to the portal operator

became. This is not permitted and violates medical confidentiality. the

Doctors cannot assume that the respective portal

driver the identity of the patient is known, so that a

gene representation is only permitted without naming identifying data.

107

7 Social and work

7.1

Social assistance data at the Senate administration

for integration, work and social affairs –

Legitimate and safe?

s

i

x

a

right

P

right

e

i.e

s

and

A

The district social welfare offices process the social data of a large number of Berliners

citizens. The Senate Department for Integration, Labor and Social

ales operates an IT procedure for the districts, with which the social data

be served. For its part, the Senate Administration uses the social data to create

tistics for a wide variety of purposes, which are particularly important for the

social planning in the state of Berlin. Since also in the context of statistical production

social secrecy has to be protected, we have been in conflict for some time

talk to the responsible Senate administration. In October 2019 we have parts

of the procedure checked on site.

The district administrations and other institutions in the social field

in the state of Berlin, the IT specialist procedure "BASIS" for the collection of data

Individuals claiming and receiving social benefits. Using the procedure

eligibility requirements are determined, data on the provision of social

All benefits processed and financial benefits paid out.

The Senate Department for Integration, Labor and Social Affairs runs the specialist

drive centrally. Since the processed data are all sensitive

data and also, to a considerable extent, sensitive health data

are subject to special protection is, on the one hand, special

Attention to the data protection-compliant and secure operation of the already since

method that has been in use for many years. On the other hand is closed

take into account that access to the social data by the Senate Administration

for the purpose of compiling statistics while maintaining social secrecy

ses165 and in compliance with the principles for the processing of personal

ner Daten166 must take place.

As part of an on-site inspection at the Senate administration, we

An overview of data processing for the preparation and creation of

provided statistics. We had to realize that there was a need for improvement in the

With regard to compliance with data protection regulations, in particular

the requirements of the GDPR.

The legal basis for the processing could be provided by the Senate Administration

are not always clearly identified. Identifying information of the citizen

and citizens are stored and used in the preparation of statistics

works, although they are not required for this. We found databases

that should have been deleted long ago. Protection against unauthorized or

unlawful processing was insufficient, a number of processing

were not comprehensible in hindsight. There was no data protection and no

comprehensive information security management. A data protection impact

estimation was not carried out.

Since it is in the social service area to facts that go far into the

extend into the personal sphere of life of the persons concerned

Compliance with data protection regulations is of fundamental importance here

tion. It is important to us to work with the Senate Administration if possible

to achieve a fully data protection-compliant state in a timely manner.

165 Section 35 para. 1 Social Code - First Book (SGB I)

166 art. 5 para. 1 GDPR

7.2 Medical information to the State Office for

health and social affairs

s

i

x

a

right

P

right

e

i.e

s

and

A

The State Office for Health and Social Affairs (LAGeSo) takes to determine the

Degree of severe disability Information from the attending physicians

and doctors of the applicants without the respective consent and

Submit a declaration of release from the duty of confidentiality by the persons concerned.

People who live or work in Germany and have a degree of

Disability of at least fifty has been determined are severely disabled im

in the sense of the Social Security Code. The pension office of the LAGeSo provides

determine the severely disabled status of the person concerned. To decide

whether or to what extent there is a severe disability is required

LAGeSo Information from the attending physicians. Get that for this

LAGeSo a declaration of consent and release from confidentiality

to the applicants, submits them to the doctors

but not before. A doctor was unsure whether he could give the requested information

about the LAGeSo is allowed to issue and has asked us to check.

According to the General Data Protection Regulation, doctors must

tion-based data transmissions can prove that their patients

and patients have consented to the transfer of data. From data protection law

From a human point of view, it is therefore preferable if the pension office

and doctors submits the declaration of consent and release from confidentiality.

However, the LAGeSo can refer to the template under certain conditions

refrain from explanations. First of all, it must be taken into account that

LAGeSo is responsible for the accuracy of the information in his request

to the medical profession, i.e. in particular for the legally effective collection of the

Consent. In concrete terms, this means that the pension office must ensure

that the applicants are aware of the consent for a specific case

of the facts as well as voluntarily, and the persons concerned, upon their

right of call for the future. In order to

to comply with the accountability stipulated in the regulation, it is necessary

that the pension office can prove the existence of the declaration at any time

can. It is advisable to obtain written consent for this.

A procedure must also be established to ensure that the

Declarations of consent and release from confidentiality ensures, if

the doctors before the transmission the submission of corresponding declarations

demands. This is necessary in order to provide the doctors with the appropriate

to be able to provide appropriate legal certainty.

In the severely disabled procedure, the LAGeSo must usually

does not create the declarations of consent and release from confidentiality

present to their patients. But if doctors

request the submission of a corresponding declaration, this is theirs

to be made available immediately.

7.3 Improper Sharing of Social Data

between the district office and the health insurance company

A

and

s

i.e

e

right

P

right

a

x

i

s

Through a petition we learned that a district office had social data from a social

beneficiary has exchanged with his health insurance company. background

was that the district office stopped paying the health insurance contributions of the person concerned

had taken over.

The district office has information about changes in the amount of contributions

obtained from the health insurance company in order to adjust the social assistance benefit accordingly

to be able to In addition, it has the health insurance on the assumption of contributions

informed.

This action was inadmissible. The district office must have the amount of the

Be informed about health insurance contributions in order to be able to grant social assistance.

It is also in the legitimate interest of the health insurance company to know which

slowly be taken over by the social welfare office. However, those involved must

Observe the principles of data protection law.

111

Here the district office violated the principle of direct survey, where

according to social data are to be collected directly from the persons concerned and only in legal

queries may also be requested from third parties.167 Such a

There was no exception. The request to the health insurance company was not necessary,

since information about changes in the amount of the contribution can also be sent directly to

beneficiaries could have been asked. Social data may also be shared with third parties

will only be passed on if this is necessary. These conditions

were not fulfilled. Instead of the health insurance company, the district office would have

must inform recipients of the assumption of the contributions. Of the

Benefit recipients would then have their own health insurance via the transfer

acceptance of the contributions by the district office. We have that

Procedure of the district office criticized. As a result, the district office

wisely for a data protection-compliant procedure.

In this specific case, we were able to achieve that the principle of direct

practice will be observed by the service recipients in the future.

7.4 Sensitive data of course participants

an internal online learning platform

s

i

x

a

right

P

right

e

i.e

s

and

A

Through an entry we found out that on the internal online learning platform

a training institution sensitive data of course participants - e.g. B. to

Learning disabilities or for motivation - for participants of a subsequent

courses were available.

The course of action taken by the training institution was inadmissible. The facility

drives an internal online learning platform on which the lecturers' materials for the

Participants of the respective courses are available for download. With new ones

courses, the documents from the previous course were usually copied,

since teachers do not always adapt or create new ones. This worker

relief is of course understandable. However, the documents contained

In this specific case, sensitive personal data from course participants

167 See § 67a para. 2 Book Ten of the Social Code (SGB X)

such as their learning disabilities, which the participants of the following

course were visible. This must not happen under any circumstances. Here it came

likely to lead to another occurrence of this kind even after

the automatic adoption of old scripts after a tip from a lecturer

had been prohibited.

It is already encountering significant privacy concerns, sensitive data

by course participants in a document and for other members

made available to the study group for download. In no case existed

a legal basis that would have allowed the sensitive data for the part

to make it accessible to participants of the following course. on our internet

the training facility has assured that comparable cases will be

rule out the future. At our instigation, those affected were also

informed about the incident in accordance with legal requirements.

Work processes of training institutions are to be designed in such a way that

personal data of course participants are protected.

113

113

8 Employee data protection

8.1 Burdens and blessings of volunteer work

s

i

x

a

right

P

right

e

i.e

s

and

A

Volunteer members of a trade union received from their

trade union and processed a large amount of personal data from trade unions

union members to win back members and to inherit

Provision of services in the wage tax area. The data is

etc. for name, address, age, union membership, level of income,

strike benefits, etc. The honorary members have a data protection

declaration signed and instructed; further agreements were made

not completed.

Trade union data is sensitive data,168 it may

are also passed on to volunteer members, since they do not have any

are outsiders.169 However, for the activity or task of honorary

official, especially with regard to the processing of sensitive trade union

data a clear written description of the rights and obligations of the

responsible and the respective voluntary worker - similar to a

Contractual relationship - required. Just a privacy policy and instruction

of volunteers are by no means sufficient.

Frequently, data from volunteers are not stored on the premises of the

Those responsible, but for example "from home" on private or

external computers that are subject to the direct influence and control of the responsible

literal are removed, processed. This poses a high security risk

this sensitive and particularly sensitive data, which is based on the principles

zen of the GDPR is incompatible.170

168 art. 9 para. 1 GDPR; § 22 BDSG

169 § art. 9 para. 2 letters d GDPR

170 kind . 32 GDPR

Therefore, written regulations are to be agreed with each and every volunteer

languages to be made or the respective order is to be specified and approved in this respect

specify that it is precisely defined which data is how, where and in which

Scope may be processed. It is recommended that similar specifications

as with teleworking from home, in order to give those responsible

ability to give proper control. Likewise in the order but

also to fix the duty of volunteers towards those responsible,

here the union, changes regarding their service provision

Show if relevant to the content and scope of the volunteer

activity are.

In addition, clear definitions of technical and organizational measures,

especially when using private hardware or private end devices,171

meet.172

Irrespective of this, the union should volunteer at least once a year

Ask employees for information as to whether there have been any status changes from their point of view and

whether the degree and scope of the activity are still appropriate for voluntary work.

We have these requirements for employing volunteers

communicated to the trade union concerned and the implementation of our recommendations

Payments or claims promptly requested.

For the activities of voluntary employees of trade unions,

in addition to data protection declarations and instructions, clear work specifications

and set rules of conduct.

8.2 Handling Migration Data

The law regulating participation and integration in Berlin (PartIntG).

with the aim of giving people with a migration background the opportunity to

to give participation in all areas of social life and

171 Bring Your Own Device (BYOD)

172 JB 2012, 2.3

A

and

s

i.e

e

right

P

right

a

x

i

s

at the same time to exclude any disadvantage. The aim is to increase

the proportion of employees with a migration background in the institutions that

fall within the scope of the PartIntG, according to their share in the

people. The Senate is empowered by law to set targets.

In addition, it is determined that in the regular reporting on

the personnel development of the public service and the legal persons

of private law, in which the State of Berlin holds majority interests, the

development of the proportion of people with a migration background reported separately

will sen. In order to be able to report accordingly, the Senate would like statistical

Statements on the migration background of the employees also with others in the

Characteristics recorded under the Personnel Structure Statistics Act (PSSG).

professional career of those affected including e.g. B. Income and Leave

work or other absences173 to ensure professional development

to be able to statistically trace the development of those affected. The Senate Administration

for integration, work and social affairs asked whether a

consent of the persons concerned is necessary.

The regulations of the Berlin Data Protection Act in relation to this question

connection with the Federal Data Protection Act must be observed. Basically allowed

personal data of employees only for purposes of employment

relationship are processed if this is necessary for the decision on the

establishment of an employment relationship or for its implementation or

termination or for the exercise or performance of any law or

rights resulting from a collective agreement, a company or service agreement

and duties of employee representation is required.174 The

Recording the migration background and linking it to others

Characteristics or data of the persons concerned is not necessary for the implementation of the

employment relationship required. In this respect, only the consent of

Data subjects may consider collecting this data as a legal basis without

a corresponding consent is inadmissible.175

173 § 6 PSSG

174 Section 18 para . 1 BlnDSG i . v. m . § 26 para. 1 BDSG

175 Section 18 para. 1 BlnDSG; §§ 26 para. 2 and 3, 22 BDSG

In this context, it should also be noted that in the Berlin Data Protection Act
law a reference to the Federal Data Protection Act, which the processing to
scientific or historical research purposes and for statistical purposes
purposes without the consent of the person concerned is missing.176
The voluntariness can be given in the context of consent to data processing
of the PSSG, because the person concerned has no legal or
economic disadvantages must be feared if they do not give their consent
shares.177 In principle, consent must be in writing, unless due to
another form is appropriate in special circumstances.178 The employer has
the employee about the purpose of the data processing and about their
to clarify the right of call in text form.179
The above Statements also apply to consent to the processing of
their categories of personal data.180 The consent
however, expressly refer to this data. In this context
the special legal requirements are also more suitable for taking action
Protective measures must be observed.181 The data subjects are informed when giving their consent
add the planned links to the characteristics covered by the PSSG
point. If the data subject objects to further data processing
Processing in pseudonymised form would only be processing in anonymous
ized form possible.
The recording of data on the migration background can only be done with the consent
agreement of those affected. These may be subject to the consent
object at any time.

176 § 18 BlnDSG; § 27 BDSG

177 § 26 para . 2 sentence 1 and 2 BDSG

178 Section 26 para . 2 sentence 3 BDSG

179 Section 26 para. 2 sentence 4 BDSG; kind . 7 para. 3 GDPR

180 § 26 para . 3 sentence 2 BDSG

181 Section 22 para . 2 BDSG

s

i

x

a

right

P

right

e

i.e

s

and

A

8.3 Transmission of the medical bill of a

employees to third parties

A police officer had suffered injuries during an operation and doctors

searched. He handed in the medical bills to the police accident insurance service

for reimbursement. His employer now claimed the medical expenses incurred

the polluter.

The medical bills submitted by the person concerned to the occupational accident insurance

were from there unredacted to the judiciary of the police and then to one

external lawyer, who in turn submits the documents to the court

and forwarded to the other side. Both the name and the private residence

writing of the person concerned were legible on these documents.

The address of the employee is a personnel file

tum.182 The admissibility of transmission by the employer to an external

A lawyer is governed by the State Civil Service Act.183 According to this, the

Transmission of personal file data to third parties without the consent of the employee

permitted if this is absolutely necessary for reasons of public interest

is. The public interest also includes the interests of the employer, the granted

to assert service accident insurance against the injuring party in court.

Because the claim for damages to which the person concerned is entitled goes in the case

of replacement by the employer.184 The legal department comes

then the task, the work accident welfare towards the injurer as

to sue for damages.

The transmission of the address must be mandatory for the claim for damages

to be required. This means that there must be no alternative to this

to take into account the interests of the employer. In this sense, the

It is by no means mandatory to provide your private address. Basically have to

Written pleadings before the civil courts to be asserted for the presentation of the

182 Section 84 para. 1 State Civil Service Act (LBG)

183 Section 88 para . 2 set 1 LBG

184 § 79 LBG

contain the evidence required to support the claim. Because the complainant

in the present case as a witness, he had to

lich be named, since it is necessary for the proper naming of a witness

there is no alternative to naming in civil proceedings and the naming

The executor in his position as a victim cannot be replaced as a witness

war.185 As an address, however, the official address was also sufficient.

Irrespective of this, the employer is obliged to anonymize

of the home address. It results from the general duty of care of the

Employer, which in turn as a structural principle from the traditional principles

zen of the professional civil service in the Basic Law (GG) is recognized.186

The transmission of the private address to the lawyer of the police was not permitted.

The specification of the private address was by no means mandatory. Against it

was the transmission of the name for the proper naming of a

witnesses are essential.

8.4 Inspection of assessments of co-

advertisers and competitors

The complainant had applied for the position of secretary at the

national administration for education, youth and family and was rejected.

She therefore asked to see her assessment documents, the reasons for the

to understand rejection. As a result, not only were her

all assessment documents of all applicants

review provided. She complained to us about this since she

feared that her personal data would also be shared with her competitors

Competitors could be viewed in this way.

A

and

s

i.e

e

right

P

right

a

x

i

s

The procedure of the Senate Department for Education, Youth and Family was

unlawful. Application and assessment documents contain sensitive data

185 Section 88 para. 2 set 1 LBG

186 art. 33 para. 5GG

119

ten and are subject to the personnel file law in the public sector

State Civil Service Act or the collective agreement of the states. So they are subject

an increased duty of confidentiality on the part of the employer.187 They are only allowed to

Consent of those affected or, based on a legal basis, third parties

be given notice.188

The right of inspecting the files of unsuccessful applicants arises

from the constitution. According to this, every German according to his or her ability and

professional performance equal access to any public office.189

According to a decision of the Federal Administrative Court in 2012

Is it for effective legal protection of the unsuccessful applicant?

inferior applicant required, but also sufficient insight into the for the

specifically challenged selection decision supporting considerations.

These are usually z. B. summarized in a selection note and do-

documented. Only these reasons can the legality of the selection decisions

support and only these reasons must be given to the person concerned for review

must be presented in an appeals process. Expressly denied

the Federal Administrative Court, on the other hand, has a claim that goes beyond that

to view information and documents that are not part of the selection

are e.g. B. Internal preparatory or explanatory notes.

The Federal Administrative Court thus makes it clear that restrictive handling

Exercise of the application documents in connection with inspection rights of

competitors is required. In the present case, the

Applicants may therefore initially only be presented with the selection note;

in the case of any references in the note to assessments of the competitors

Competitors would be a further right to knowledge of the assessments

or other selection criteria.

In the present case, it was also an employee position in the

Office. A right to inspect personnel files, which is possible in exceptional cases

187 Section 84 para. 4 LBG, § 3 TV-L

188 § 88 LBG, § 3 TV-L

189 Art. 33 para. 2 GG, 19 para. 4GG

data without the consent of the civil servant can be found for employees

te not in the collective agreement of the countries.

The right to inspect the application documents of competitors

There are narrow limits to what is happening to you and your competitors.

121

9 economy

9.1

"Press..." - Recording of customer

talks according to the GDPR

s

i

x

a

right

P

right

e

i.e

s

and

A

Again and again we receive inquiries from consumers,

who inquire whether recordings of telephone conversations are permitted,

if recording can only be prevented if the persons concerned

actively contradict them at the beginning.

An example of this was the case of a large electronics group. At a

Calling the service telephone number, an automatic announcement informed the

Customers at the beginning of the phone call about the recording of the

speak. The customers then had to press a button to

Select your request category. Only as an employee

who took the call, those affected could record it

object to the conversation. If the customers objected,

the conversation already recorded up to this point in time was deleted and

not continue recording.

The procedure of the company was already to be determined according to the old legal

lined up because consent to the recording of customer conversations

start of recording had to be obtained. The possibility of a late

ren objection and an associated deletion are not sufficient. To it

nothing has changed as a result of the GDPR.

On our notice and with regard to the DS-GVO, the company concerned

are reorganizing their service telephone so that customers can

immediately after the greeting, it was pointed out that the conversation was over

Training and quality reasons can be recorded and monitored. There-

After that, customers had the opportunity to comment on the recording

by pressing the "1" button. If they didn't, it would

further conversation recorded.

We also had to object to this approach. After the data

General Protection Regulation, the consent must be confirmed by a clear

ing action take place, with the voluntary, for the specific case, in informed

Wisely and unequivocally stated that the data subject with the

processing of the personal data concerning them.190

A silence or an opportunity to object at the beginning of the conversation

is not sufficient for this.

On our repeated notice, the company has its procedure in the meantime

converted in such a way that customers can actively choose by pressing a button

decide whether you agree to a recording or not. This is

ensures that customers are actively involved in the

consent to the recording of their conversations.

If companies want to record a customer conversation, they have to

Customers before the start of the specific recording by a

clear affirmative action, e.g. B. voluntarily pressing a telephone

button to consent to the recording.

9.2

"Your ID, please!" - Identification at

the assertion of the rights of those affected

Frequently, people asking companies for information or deletion of the

ask about the data stored about them, first asked to contact a personal

identification copy, although there are no doubts as to their identity.

Requesting a copy of an ID represents a hurdle for those affected. A

However, requests for information or deletion should be made as simply as possible

be.191 The additional effort can prevent people from

to exercise their data subject rights. The companies responsible

are therefore only available if there are reasonable doubts about the identity of a person

A

and

s

i.e

e

right

P

right

a

x

i

s

190 kind . 4 no. 2 GDPR

191 Art. 12 para. 1 sentence 1 GDPR

123

Request information.192 If a person requests information about the

data required and the information to those known to the company

address is to be sent, there are usually no doubts about the identity.

The same applies to requests sent from email addresses that

are known to the company because they otherwise come from the same address

ammunition.

If the identity card had to be presented in general, companies would have

grabbed more data than they need. In some cases, those affected

Individuals also asked to send their copy of ID via unencrypted email-

the. Information on how long the ID card data should be stored,

became i. i.e. R. not given.

Of course, information may only be made available to those actually affected.

be provided. Also, an account should only be deleted or created by the authorized

can be blocked. At the same time, however, it should not be more difficult

to assert contractual rights, for example with a company in

to enter into a contractual relationship. Can an account be opened without an ID document?

are placed, it should also be possible to delete them without a document. After all

This raises the question of what is the point of requesting an ID document

if it has not been matched with any information previously stored about the person

can be equalized.

In addition to an identity document, there are other ways of providing proof

the right to know the information stored about an account

and delete the account. So is a portal in which people submit their inquiries

can confirm with the already created access data to their accounts, one

good way to authenticate yourself. At the same time, portals in which

Inquiries are at least partially automated or processed in a well-structured

to facilitate the exercise of data subject rights.

If, in justified individual cases, the request for a copy of an ID

is taken, for example because several of the data of those affected have changed

192 Art. 12 para. 6 GDPR

Companies obligated to point out that for identification no

required data can be blacked out.

A copy of an ID card should be used for the assertion of data subject

rights can only be requested in exceptional cases.

9.3 Long storage period for delivery services

Many delivery services also save the data of their customers

Years after they ordered something. With the entry into force of the

Basic Protection Ordinance have people who have not been involved for many years

had ordered the services concerned, nevertheless data protection declarations from

be sent to this company.

A

and

s

i.e

e

right

P

right

a

x

i

s

By notifying you of updated privacy policies

some former customers of delivery services first noticed that

that their data is still stored with the relevant services. So

turned out to be storing records of orders made up to

up to ten years ago. It turned out that many companies do not have any functional

have on-going extinguishing concepts. There is also a lack of technical implementation

tion to systematically delete inactive customer accounts and the active one at the same time

to obtain database.

In principle, data may only be stored for as long as is necessary for the original

original purpose is required. In the case of a customer account, it ultimately comes down to this

depends on whether it is used regularly. An unlimited storage is

not permitted. The companies have to create concepts, after which time

of inactivity customer accounts are deleted, and these by deletion routines

implement technically and organizationally. It also depends on

which service is involved and in which cycles customers

who typically order again. A storage of customer accounts via

however, a period of two years of inactivity is not regularly required

be lich.

125

Many complaints related to the delivery services are currently-

time in the sanctions process.

Customer data should only be stored for as long as

as long as they regularly use the offer of delivery services

take.

9.4 Report from the start-up consultation hour

s

i

x

a

right

P

right

e

i.e

s

and

A

The consultation hours, which take place twice a month, are successfully entering their third year.

The start-up companies in Berlin take advantage of the specific

very well: Last year, the consultation appointments were usually for

booked three months in advance. Admittedly, the office hours are generally not

time bound. However, due to high demand, it usually was

required to reserve an appointment in advance.

Many start-up companies are also aware of the legal change

the DS-GVO a need for adjustment in their data processing processes or

find that the topic of "data protection" could also become relevant for them.

The GDPR was thus the dominant topic in many consultations,

that we have led. For many start-ups it was important whether they

have to appoint protection officers, how to create procedural directories

are and how the information obligations can be fulfilled. In the counseling

It was often a question of systematically approaching the start-up's data processing

record, identify purposes and legal bases and thus provide assistance

to give how and about what the persons affected by the data processing

are to be informed. We were often able to clarify that no consent

Declarations of agreement are required if the start-ups are about contractual

Process basic data. It turned out that often mistakenly accepted

becomes that the DS-GVO requires consent for all data processing

do badly.

Many discussions also revolved around the design and content of data

declarations on websites. Key themes were the integration

Creation of tools for website analysis and tracking of usage

activities and to integrate social plugins.

In addition, the consultation hour lives - as in previous years -

of specific issues relating to the respective business models.

This shows that the personal exchange is expedient, since different

Possible solutions or the adaptation of processes can be discussed

to. The topic is more and more frequently about the use of automated

decision algorithms and “intelligent” systems. From data protection law

From a human point of view, the aspects of transparency and design are particularly important

of declarations of consent and intervention options as well as the requirements

requirements to carry out data protection impact assessments.

The need for advice among start-up companies remains high.

The experiences from the consultation hours show that the format of a consultation

hour that appeals to start-up companies very well and many are talking

Inquiries can be answered quickly and easily.

9.5 Silent factoring in the age of the GDPR

Small and medium-sized companies in particular have an interest in

to sell outstanding receivables, which are often not yet due, in order to

to have sufficient liquidity. Companies specializing in this, but also

Banks offer themselves as debt buyers. If the debtors

Debtors are not informed about the sale of receivables, one speaks of

silent factoring. This is discreet and prevents customers from

to complain about the sale of receivables that are not due. To us was the

asked whether silent factoring is still possible under the GDPR or which

technical restrictions must be observed.

A

and

s

i.e

e

right

P

right

a

x

i

s

Under civil law, a sale of receivables is possible if there is no prohibition on assignment.

was agreed.193 The Civil Code (BGB) also assumes that

193 § 399 Civil Code (BGB)

127

a sale of receivables without information from the debtor

is possible. Thus § 407 paragraph 1 BGB regulates the liberating effect of the service

previous creditors if the debtor is not aware of

who has assignment.

If the company buying the claim does not receive any debtor data

holds or the debtor is a legal entity, dormant factoring continues

possible without any problems. However, if personal data is passed on to new creditors

biger communicated, the transparency obligations of receivables sellers194 and

buyers of receivables195. Receivables sellers are at least at

conclusion of the contract must be informed in general that a data transfer

mediation may be carried out in connection with the sale of receivables.196 Also

Debt buyers have information obligations. While this is not the case, though

national law regulates the acquisition or disclosure by law,

to which those responsible are subject and the appropriate measures to

provide for the protection of the legitimate interests of data subjects.197 It is

but not to assume that the BGB norms as such legal provisions

you can see. In particular, it should be noted that a buyer of receivables

does not have the right to conduct a credit check on the debtor

carried out, since they did not have to reckon with the conclusion of the contract

that third parties with whom they did not wish to enter into a contract

future agencies would do, which would lead to a deterioration in their scoring value

being able to lead.

Silent factoring should only take place without the transmission of debtor data.

194 Art. 13 GDPR

195 Art. 14 GDPR

196 art. 13 para. 1 letter e GDPR

197 Art. 14 para. 5 lit. c GDPR

9.6 Passing on account data to transfer instruction recipient

Some banks transmit the transfer recipients

the IBAN data of the transferor via account statement. Complained about this

a tenant who had recovered overpaid money from his landlord.

The bank concerned stated that it was legally obliged to transmit the IBAN

to be.

A

and

s

i.e

e

right

P

right

a

x

i

s

The fact that the majority

number of German banks do not transmit the IBAN via bank statement. to

should also be noted that, unlike in the present case, the IBAN can easily

can be used commonly, such as for illegal debits. For

It is also difficult for consumers to trace

Gen and concrete knowledge about who knows their account data and

may have saved.

We have recommended to the bank that in future it should not transmit the IBAN

give up According to the money transfer regulation it mentioned, the bank is not available

Obliged to transmit the IBAN data. This law is aimed at preventing

of money laundering and terrorist financing in the context of money transfers

directs; for this it is sufficient if the bank sends the IBAN data upon receipt of payment

th receives. However, you may not pass the data on to the payee

Submit payee. The national regulations for the provision of

Payment services198 are, in the light of recital 54 of the euro

European Payment Services Directive (ZDRL). Then the or the

Affected parties to the payment transactions all necessary, sufficient and ver-

get real information. However, this is already guaranteed

if not the IBAN data with the incoming transfer to the payment

be transmitted to the recipient, but only

Name, identifier, amount and the specified purpose of the order

Berlin or the client.

198 Art. 248 § 8 EGBGB

Banks should not give credit to payees

communicate the IBAN of the transferring party.

9.7 Illegal registration in the warning

insurance industry database

s

i

x

a

right

P

right

e

i.e

s

and

A

A policyholder complained that her insurance

society them in the reference and information system of the Deutsche Versi-

cherer (HIS) has reported, because their property insurance three claims

reported within 24 months. The system operated by Informa HIS GmbH

bene information system informs insurers about increased risks, there

Registered insured have difficulties in the division concerned

conclude a contract with another insurance company; at least is with

Premium increases to be expected. The complainant was admitted to the HIS

reported, although two of the three reported claims were uninsured.

When registering in the HIS, a balance must be made between

in the interest of the insurance industry to protect itself from increased risks

and insurance fraud, and informational self-determination

right of the data subjects.199 Even if the GDPR when registering

Affected persons in credit bureaus generally assume that individual checks will be carried out

In mass procedures, a list of criteria should always be used

have to accept. In the present case, however, the registration should not have taken place

fen, since three cases of damage were reported in accordance with the criteria, two of these

cases were not insured at all. In particular, insurance companies are after

The GDPR obliges individual cases to be examined in the event of complaints from those affected

to be carried out even if the criteria have been observed.

After our intervention, the insurance company deleted the registration

let her.

199 Art. 6 para. 1 letter f GDPR

The HIS can continue to be operated under the GDPR, but it is one

greater consideration of the individual case required.

9.8 Black Listing of an Online Bank

A

and

s

i.e

e

right

P

right

a

x

i

s

A former customer of an online bank wanted to open an account with it again

to open. The request was rejected. The complainant suspected that the

Online bank account opening for former customers in general

refuses.

The bank has admitted that it will continue to use the data of former customers

save to keep a blacklist, a kind of warning file, so they can use this

does not provide people with a new account. The bank justifies this with

that according to the German Banking Act (KWG)200 it is obliged to

measures to be taken against customers suspected of money laundering

men. Unfortunately, they are currently unable to distinguish between money laundering suspects

and to differentiate those affected who are not suspected of money laundering

they prevent the re-opening of accounts by former customers

prevent further data storage and execution of a data comparison.

The Bank's actions are unlawful. The data of former customers

and customers are to be deleted or, if there is a storage obligation

lock out. In a comparison file to prevent a new bank account

Only those affected may be admitted who are actually subject to money laundering

are suspected or where there are other valid reasons, a new one

Reject bank details.201

The bank has admitted its mistake and wants to change the procedure as soon as possible.

Nevertheless, we have initiated administrative offense proceedings.

A blacklist for former customers, against which none

suspicions exist is illegal.

200 § 25 h KWG

201 See Art . 6 lit. f GDPR

9.9 Video Identification Data Transmission

s

i

x

a

right

P

right

e

i.e

s

and

A

Many new bank customers want to open an account

not going to a bank branch that may be far away; online banks

Some of them no longer even have branches. To those affected after the

Many banks are involved in identifying the provisions of the Money Laundering Act202

service providers specializing in video identification using smartphones

have specialized. One of these companies only carries the identifications

then through if the persons concerned have consented to the fact that the service

ter the data obtained during the identification also for other contracting parties

ner (e.g. when concluding an insurance contract). A bench

considered this to be problematic and asked us for an opinion.

The banks subject to money laundering are responsible for the video identification,

the service provider, on the other hand, is a processor. If this

now wants to use third-party data for its own purposes, finds legal technical

data is transmitted from the bank to the service provider. Since the further

subsequent use of the personal data of the persons concerned (so-called pooling)

which is still required for the bank contract for identification, is the consent

involuntary and therefore illegal.203 In this assessment

nothing changes because data subjects continue to use their data

can already object during the identification process. Also can

those affected are not referred to the post-ident procedure

lead, as this compared to the process desired by those affected

is more cumbersome and time consuming.

The General Data Protection Regulation has the requirements for voluntariness

increased by consents. A video identification must not depend on it

be made that data subjects agree to the further use of their data.

202 § 11 GwG

203 art. 7 para. 4 GDPR

Chapter 9 Economy 10 .1 Data from refugee helpers on the NPD website

10 political parties and

the House of Representatives

from Berlin

10.1 Data of refugee helpers

NPD website

The Berlin state association of the NPD published in February 2018 on its

website204 a map of facilities for asylum seekers created with Google Maps

seekers in Berlin. Title: "An overview of the focal points of foreign infiltration

our city". Each location was given names, telephone and cell phone numbers as well as

like e-mail addresses of people working there. The accompanying text explained

that everyone can now find out "which interesting and

requested guests cavort in your neighborhood, who are responsible for

responsible for whoever is financially involved in the hundreds of thousands of migrant

profit and who to contact if you have a complaint

want to pay directly on the spot". All data came from public sources.

A

and

s

i.e

e

right

P

right

a

x

i

s

The company responsible for the Google Maps map service gave

to have blocked the card due to violations of their own policies

ben.205 However, it was possible to read the source code and thus those in the map

to make stored personal data visible.

The collection, processing and use of personal data is only

negligent, insofar as this is permitted by law or the persons concerned have consented

ben.206 The publication of the personal data was illegal here.

The data subjects have not given their consent. The use was

204 https://www .npd-berlin .de/asylheimkarte-berlin2018/

205 https://www.welt.de/politik/deutschland/article173227076/NPD-veroeffentlicht-auf-

Google-Maps-Karte-mit-Asylumunterkuenften.html

206 § 4 para . 1 BDSG a. F.

also not according to § 28 Abs. 1 Nr. 3 BDSG a. F. allowed. After that was the processing

of generally accessible data lawfully, provided the responsible body

thereby pursued legitimate interests and a weighing of interests resulted,

that no legitimate interests of the persons concerned prevail. By-

However, those who work in the field of refugee aid have a significant

interest that their data is not on a website with xenophobic

Content is published ("uninvited guests", "foreign infiltration of our

Hometown"). The people concerned were targeted for anti-refugee women

and opponents made visible. These legitimate concerns of those affected

Individuals clearly outweigh any interests of the NPD

the publication of this data.

By continuing to make the data visible by looking at the source code

the unlawful state of affairs continues. We have the NPD Berlin

prompted to personal data permanently from the website

delete and submit the process to our sanctions office.

10.2 Election campaign with the help of Deutsche Post

s

i

x

a

right

P

right

e

i.e

s

and

A

In the past federal election campaign, the CDU and the FDP

duct “Voter addresses with party affinity” by Deutsche Post Direkt GmbH

used. The product enables the display of constituency-related so-called clusters

(groups of buildings) whose occupants have a (on a

(adjustable on a scale of 1-10) minimum affinity for the respective party,

so streets that have a high value for the doorstep campaign

can be used. Another function has constituency-related

individual buildings that have a certain minimum affinity for the respective

respective party.

The data made available to the parties when using the product

are not personal. It is true that it is a question of party affinity

on a scale of 1-10 to provide a score that also includes political statements

opinions, i.e. H. on special types of personal data,207 allows.

207 § 3 para . 9 Federal Data Protection Act a. F.

group

However, this score value is not assigned to a specific person in the present case, but other buildings. This assignment is therefore comparable to regular geodata, which are usually also assigned to buildings or properties the. In the case of geodata, we proceed with an aggregation of at least four house assume that the data is so coarse that it is worthy of protection Interests in the processing are not affected.208 In the present case, at least five to six households are grouped together in a cluster pulled. Both the display in the map view and the partial addressing by post is only building-related, so that the data is again coarser will.

The CDU and the FDP have the product "voter speeches with party affinity tät" is used in accordance with data protection regulations.

10.3 “Neutral School” initiative by the AfD parliamentary group

With the “Neutral School Berlin” initiative, the AfD parliamentary group in Berlin headlines. The parliamentary group switched to the online portal on its website "Neutral School in Berlin" and published a registration form there with which reports on suspected violations of the neutrality requirement to the faction can be sent. The AfD parliamentary group describes its initiative as Offer of help and offers to deal with the reported events "while preserving personal personal rights" to the school authorities for review. Similar Initiatives were also taken by other AfD factions in various countries created by desparliaments.

A

and

s

i.e

e

right

P

right

a

x

i

s

Since the initiative was activated, we have received many inquiries from the press, from politicians

politicians, parents, teachers and others

Citizens who have data protection concerns about this initiative

assert ative. Some of these are general information, some

wise people describe that they asked the AfD parliamentary group for information,

208 This corresponds to the "GeoBusiness and data protection" code of conduct issued by the

Approved by data protection authorities in 2015 and approved by the then BInBDI

became .

135

whether they stored personal data from you as part of the initiative

and had received no response.

According to the new Berlin Data Protection Act, parliamentary groups are just as

ordnungshaus and its members outside the scope of the law

subject to the extent that they are required to carry out parliamentary tasks

process personal data.209 This means that our responsibility as supervisory

authority for these areas excluded.

The background to this restriction is that the constitutional

Separation of powers does not readily allow data protection supervisory authorities

as part of the executive power (executive) compliance with data protection

control provisions of the legislative power (legislature). Par-

Laments, including their organs and members of parliament, are therefore subject to

Exercise of parliamentary tasks only if data protection regulations

and the supervision of the supervisory authority if this results from a clear legal

chen regulation results.

The term "performing parliamentary tasks" is also far too

stand. Only administrative activities such as renting offices, that

Hiring employees, purchasing office supplies

etc. are not included and thus remain within the scope of the Berliner

Data Protection Act.210 Any political work by a parliamentary group

against is excluded from this. We were therefore unable to check the online portal

may still take action in cases of specific complaints.

For a long time we have been recommending that the Berlin House of Representatives vote for

to give the parliamentary work itself a data protection regulation and therein

also regulate data protection rights for data subjects. Such data

Protection regulations have existed, for example, with the Hamburg Parliament since

1999. There is u. the right for data subjects is laid down,

to be able to request information about their personal data,

209 See § 2 para. 3 BlnDSG

210 Justification for Section 2 Para. 3 BlnDSG, Drs. 18/1033 of the Berlin House of Representatives, p. 71

ment of the parliamentary work of parliamentary groups in the Hamburg Civic

be stored.211

The Berlin House of Representatives has not yet decided to create a

committed to a data protection regulation. This gap should

close the house immediately, regardless of the “neutral school” initiative,

to prevent legal vacuums.

10.4 Submission of Personal Information

Written Requests

For the Senate, the question repeatedly arises as to whether and to what extent

answering written questions from individual Members of Parliament

related data may be passed on. The prerequisites for

the Berlin Data Protection Act212 explicitly applied in the past. This pre-

schrift has been omitted without replacement in the new version of the law.

A

and

s

i.e

e

right

P

right

a

x

i

s

The right of every Member of Parliament to submit written questions to the Se-

To turn to nat is a valuable asset as a means of parliamentary control

accordingly also anchored in the Berlin constitution213.

As a rule, written inquiries can be answered without

data protection issues are affected. But it is different, e.g. B. off if

MEPs are pursuing the aim of their question to affect individuals

to find out facts or even concrete names214. In the-

In these cases, a decision must be made as to whether the disclosure of information is compatible with the

agree on the informational right of self-determination of the persons concerned

leaves.

211 § 9 of the data protection regulations of the Hamburg Parliament from 19 . October 1999, in

the version of 18 . May 2018; available at https://www .hamburgische-buerger-

schaft .de/recht/

212 § 20 para . 1 BInDSG a . F.

213 art. 45 para. 1 Constitution of Berlin

214 Drs. 18/15244, 18/14847

137

According to the previous regulation in the Berlin Data Protection Act, the transmission

processing of personal data is possible if – to put it simply –

the legitimate interest of the data subject in the transmission is not

object.215 After the amendment of the law in June 2018, the

new law no longer has a corresponding provision.

This does not mean, however, that the Members of Parliament are no longer given any personal

Genetic data may no longer be transmitted. Rather, the constitution grants

MPs even have the right to have direct knowledge of the contents of files

of the administration.216 By its very nature, this right is

even more extensive. Access to files can only be denied if it is public

or private interests in secrecy require this.

Henceforth basing the power of transmission directly on the constitution should

nevertheless only be a temporary solution. Because according to the regulations of the DS-GVO

there must be transparency for natural persons as to how their data is processed

217 This is currently not readily guaranteed. In any case, it is

decisive in the weighing decision to be made in each individual case

lich to take into account that the responses of the Senate to Written Questions

also be published.218 This is a significant difference to the personal

Members of Parliament have access to the files and it is not unusual for them to come to the same conclusion

result in the confidentiality interests of the persons concerned being transferred here

to weigh.

The legislator is required to provide a clear legal basis for the processing

processing of personal data in the context of written inquiries

establish both the constitutional rights of deputies as

also the fundamental right to informational self-determination of those affected

persons into account.

215 See in detail § 20 para. 1 sentence 2 BlnDSG a . F. i. v. m . § 28 para. 1 sentence 1 no. 2,

No . 3 BDSG a. F.

216 art. 45 para. 2 Constitution of Berlin

217 See Art . 5 para. 1 letter b GDPR and recital 42 sentence 2 GDPR

218 § 50 para . 1 Rules of Procedure of the Berlin House of Representatives

11 From the work of

sanction body

11.1 Development of administrative offenses

proceedings

Due to the new data protection regulations, some changes have

genes in the practice of sanctions. In particular, the fine framework

expanded and the number of fines increased.219

In some cases in our sanctions practice, the new fines

written as a basis, although the acts before the entry into force of the new

moods were committed. Although according to the principle of legality

In addition, an act can only be sanctioned if it is punishable

was determined by law before the act was committed.220 An exception to

However, this principle is based on the so-called principle of most-favoured-nation treatment in the

offenses law.221 Does the law change between the end of the crime

and the decision, according to the principle of most favored nation

most law. Although the applicability of the GDPR means, in particular, before

against the background of the extended range of fines, in most cases for

Perpetrators no mitigation, but an intensification of the threat of fines. One

However, there is an exception in the new Berlin Data Protection Act. the

allowed processing of non-obvious personal data was after

old Berlin Data Protection Act a criminal offence. According to the new Berlin data

Protection Act, this behavior is now an administrative offense and therefore

the result is the milder provision. However, such behavior is also punishable

furthermore, if the perpetrator is paid or in damage or

hedging intention.222

219 JB 2016, 1.2.4

220 type . 103 para. 2GG

221 Section 4 para. 3 OWiG

222 § 32 BlnDSG a . F. - § 29 para. 1 and 2 BlnDSG; § 70 BlnDSG

11.2 Unauthorized data collection from the police database POLIKS

Due to the aforementioned new fine provisions in the Berlin data
We now also have administrative offenses against unauthorized persons
To process access to the police database POLIKS.223 In this database
both process data and data from suspects, criminals, crime
suspects, those affected, as well as data from victims and witnesses and
stores; including names, dates of birth, addresses and marital status. the
Database serves the police forces as an information system and should
Quick information on people, things, institutions and processes by
enable targeted inquiries or research.

However, access to POLIKS is also repeatedly misused to
Spy on family, neighbors or third parties and their living conditions. In
This year, in such cases, we created 14 criminal prosecutors under the old legal
sluggish and have already initiated five fine proceedings under the new regulations.
The cases before us related exclusively to unauthorized access to the data
bank from POLIKS by police employees.

From a technical point of view, all police officers can access POLIKS
to grab. From a legal point of view, however, a data query is only permissible if
this relates to a process for which the enquirer is responsible
is. Any query that is not related to work is not permitted. police officers
We are informed at regular intervals about data protection regulations
informed. They are expressly prohibited from using data from POLIKS and others
police information systems for private purposes or from private internet
eat to retrieve.

Unauthorized access to POLIKS is consistently checked with thoroughly recommended

punishable fines.

223 So far, such incidents have been reported to the

delivered to the public prosecutor.

11.3 Police officer warns of police raids

We filed a criminal complaint against a police officer because he

initiation Data from the POLIKS information system about planned

police measures, including raids, retrieved this information

sold to members of the criminal milieu for a fee.

The police informed us about an incident that was caused by the reporting of confidentiality

persons of the State Criminal Police Office had become known. investigations in

Area of drug crime revealed that drug dealers to avoid

law enforcement actions paid sums of money to police officers to

receive information about police measures. In the course of the police

Investigations turned out that the accused police officer had a

a large number of inquiries over a long period of time and without official

genes in the POLIKS database on the personal details of drug dealers

to find out the current status of the investigation. The in this way

The accused police officer then conveyed the knowledge he had gained

for money to the drug dealers. In addition to the suspicion of violating

data protection regulations, there was a suspicion of commercial

bribery, breach of official secrets and participation in

narcotics trafficking.

The unauthorized processing of non-obvious personal data

Any payment is punishable224 and is regularly reported by us to the Berlin State

prosecutors reported.

11.4 Dental employee publishes this

School report of an intern on the internet

We have filed a criminal complaint against an employee of a dental practice

Public prosecutor's office in Berlin because she received the testimony of an intern at

internet had published.

224 Section 29 para. 1, 2 BlnDSG

141

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

In the course of a vocational training measure, the

applied for an internship at a dental practice. under him-

Her application documents also included her school certificate, which she gave to the dental

medical practice sent. Already on the first day of her internship, one expressed herself

Dental practice employee derogatory to the intern about her

school performance. In the period that followed, unknown persons shared

met via Facebook that their school report was photographed, on various

Internet platforms have been set and can be viewed by everyone.

Application documents can contain a large amount of detailed information about

the applicants contain, including sensitive data. One

Publication to third parties - especially on the Internet - without legal

che basis is inadmissible and can be punished with a fine. One

Publication with intent to harm the data subject is above

also punishable.225

The illegal publication of employee data on the Internet can

constitute a crime.

11.5 Criminal complaint against a committee proposal -

seat of the House of Representatives

Berlin

s

i

x

a

right

P

right

e

i.e

s

and

A

Against a member of the Berlin House of Representatives and at the same time

sitting of the technical committee responsible for data protection, we have criminal

applied to 226 for illegal data processing because of these excerpts

a previously illegally published arrest warrant on the short message service

Twitter had spread.

After criminal proceedings for a fatal knife attack in Chem-

nitz an arrest warrant was issued, it was published on the internet a short time later.

225 §§ 43 para . 2, 44 para. 1 BDSG a. F.

226 §§ 42 para . 2 no. 1, 44 BDSG a . F.

public. As it turned out, had an employee of the correctional facility

Dresden photographed the document and put it on the Internet. The so published

The committee chairman spread the public arrest warrant on his Twitter

account. The case was due to the person concerned's position as a Member of Parliament

and as chair of the parliamentary committee responsible for data protection

of particular explosiveness.

The publication of court records, including indictments and detention

commands, is not only subject to data protection law, but also according to the Criminal Code

punishable.227 The personal information published with the dissemination of the

Personal data requires a high degree of protection. Although the twit

ter post with the published arrest warrant removed after a short time. It is

However, not unlikely that the contribution of third parties on Twitter and on

disseminated to other websites. Because of the high number of

Subscribers to the MP's Twitter posts is from

a large group of recipients and thus of a serious injury

of the personal rights of the person concerned.

With the publication of the arrest warrant, in addition to personal rights

of the person concerned also in particular violates his or her basic judicial rights. Included

are fundamental rights that protect individuals in court proceedings

must. Dadu ch is the impartiality of those involved in the proceedings, in particular

of lay judges and witnesses, as well as the protection of

affected person from discrimination. This includes maintenance

until the legally binding conclusion of the proceedings in favor of the

existing presumption of innocence that has not been

of official documents should be endangered. The release is

also suitable for increasing public confidence in criminal justice

to affect care.

The publication of an arrest warrant constitutes a serious

Infringement of rights. By the chairman of the responsible for data protection

technical committee, we would have expected more restraint here.

227 § 353d StGB

143

12 Telecommunications and

media

12.1 Report from the Berlin Group

The international working group on data protection met again in 2018

in telecommunications (IWGDPT or Berlin-Group for short) twice under the

Chair of the Berlin Commissioner for Data Protection and Freedom of Information.

At the Spring Conference in Budapest on April 9th and 10th, the

group with issues of privacy and data protection, among other things

cross-border data requirements for law enforcement purposes, in particular

especially in connection with access to data in a cloud. the border

Exceeding requests for information throw up complicated data protection laws

Questions on. Traditional arrangements for international coordination by the

Law enforcement officials are facing the increasing frequency and

Complexity of cross-border data requests as too cumbersome. alterna

tive mechanisms, such as voluntary agreements between providers and

foreign authorities, may have different and non-transparent

be subject to dars. In the working paper adopted in Budapest

Standards for data protection and privacy protection in cross-border

progressive data requirements for law enforcement purposes outlines the

Berlin Group the current developments in this area and calls for the required

divided actors to use in promoting expeditious processing legitimate

mer cross-border data requests the interests of data protection and

to maintain privacy at all times. The working paper also makes recommendations

binding standards.

Also in Budapest, the Berlin Group adopted the working paper "Ver-
net vehicles". It analyzes the different types of data that
related to networked vehicles, generated, transmitted and
get saved. Vehicles are increasingly connected to the internet
and collect a wide variety of information, e.g. B. to behavior

of the driver or about the persons who are inside or outside
stay outside the vehicle. Such data can come from both the vehicle
gene IT system or by other technical devices that are connected with
connected to the vehicle. Autonomous vehicles require a particularly large amount of data
witness, which is why its further development will also include further data protection
common questions will entail. The working paper shows the risks for the
privacy associated with the different processes. To-
it contains recommendations for all relevant actors, such as these risks
can be counteracted effectively.
On November 29th and 30th, the Berlin Group met in Queenstown, New Zealand
country. The location of the meeting in the southern hemisphere enabled many inter-
Essents and interested parties from the Asia-Pacific region, also once
attend the meeting in person. The date had also been chosen
that the meeting of the Berlin Group immediately before the meeting in Wellington
the 50th APPA Forum228 and the subsequent “International Privacy
Forum” took place, so that the members of the
lin-Group and that of the APPA forum at the other meeting was possible.
This planning turned out to be extremely useful and productive. sex
espe- cially in the field of telecommunications, Asian countries play an important role

Rolle, their integration into the Berlin Group, which has so far been unsatisfactory
was is therefore of importance that should not be underestimated. On the other hand, the
active participation of the Berlin Commissioner for Data Protection and Information
freiheit and other participants of the Berlin Group to the
Lectures and discussions of the APPA Forum and the International Privacy Fo-
rums to extremely positive feedback. The participants there
mer had a lively one due to the international impact of the GDPR
Interest in the first experiences with the new European legal order.
In Queenstown, the Berlin Group adopted a working paper on questions related to the
Data protection in connection with artificial intelligence. The paper de-
defines various terms used in the discussion about the artificial
intelligence always play a role. It describes practical examples
as well as application scenarios for the use of artificial intelligence and there
228 Asia Pacific Privacy Authorities (APPA) Forum

a detailed overview of the challenges for data protection
and privacy. It also contains recommendations with regard to the
maintaining the principles of data protection for relevant stakeholders.
In addition, the Berlin Group passed a working paper on the
gene detection of the locations of people in public space. The location, i. H.
the ability of modern technology to track the movements of individuals and
Recording is an area where the real and virtual life of the
meet people On the one hand, the paper shows the potential of the technologies
for the benefit of people, such as when the efficiency of road use
improved and thus the CO2 emissions can be reduced or if
“Smart City” services e.g. B. the effectiveness and cost-effectiveness of public services,

such as in local public transport. It settles on the other hand

but deal with the risks for data protection and privacy, there

knowledge of people's locations not only opens up the possibility

recognizing typical movements, but also influencing people

senior It contains both recommendations aimed at the actors who

che mechanisms for location tracking or the possibilities of

integrate location tracking into their devices (such as smartphone manufacturers),

as well as recommendations addressed to the supervisory authorities.

Both working papers from the November meeting are still subject to reservation

the final acceptance and, as is usual in the Berlin Group, will become so

given in a written circulation procedure. The papers are expected

Published on our website in early 2019. The papers from the spring

session in Budapest are already available there.

12.2 ePrivacy Regulation: No agreement in European Council!

A

and

s

i.e

e

right

P

right

a

x

i

s

As early as January 2017, the EU Commission submitted a proposal for a

regulation on privacy and electronic communication, the so-called ePri-

vacy ordinance, published.229 The ordinance is intended to provide guidelines for the protection of

Fundamental rights and freedoms of natural and legal persons in the

Provision and use of electronic communication services with direct

direct validity in the European Member States and, in particular,

special the rights to respect for privacy and communication as well as

regulate data protection in this area in Europe and further harmonize

The European Parliament then had a negotiation in October 2017

position on the draft and the inclusion of interinstitutional

negotiations decided. Now all that was missing was the positioning of the euro

European Council to start the so-called trilogue, i. H. about the draft regulation

to be negotiated at European level between the Commission, Parliament and the Council

and finally to say goodbye. To date, however, no agreement has been reached in the Council

be achieved among Member States, so that the legislative process

has not progressed.

In the European Council, the text of the draft regulation in the competent

Council Working Group on Telecommunications and Information Society

del. As from the current progress report of the chair of the working group

shows,230 there is still a need for discussion on the legal

requirements for the processing of electronic communications data, for protection

of information stored on the end devices of the users

ons, the default settings for privacy and the question of who

should lead protective supervision. Apparently, a number of Member States are of the opinion that the regulations must be more closely aligned with the GDPR, by granting the processing powers for balancing and for processing be opened for other purposes. In this context, it is required for held, a more far-reaching processing of communication meta-

229 For details on the draft, see JB 2017, 1.4

230 Council document 14491/18 of 23 . Nov 2018

to allow data. This is questionable, as the EU Commission's proposal for ePrivacy Regulation was designed to use the GDPR for certain data processing work in the field of electronic communication to supplement, to and to create specific and prioritized special regulations. This pre- having is the opposite, if now unspecific permission facts as well as possibilities for extensive purpose-changing data processing will create.

In addition, the member states argue about the regulations for the use of online services and the question of whether the providers of these services should have the ability to visit their advertising-financed websites for the benefit to subject users to the condition that they use web tracking allow. This is one of the core issues of processing Usage data on the Internet, because users could access them way be forced to relinquish control of their data in order to log in to move the Internet. If access to websites from the possibility is made dependent on the activities of the users on the Website and cross-site tracking in detail and the collected Passing information on to third parties leaves few or none at all

Opportunities to still freely decide online how personal

data is used or how this data should be effectively protected.

– The hope remains that the Council will arrive at a balanced, interests

position that takes sufficient account of the users

becomes.

The delays in the Council mean that entry into the trilogue negotiations

ments and an adoption of the ePrivacy Regulation before the European elections

len 2019 is more than questionable. This situation is not only for the users

and users of electronic communications extremely unsatisfactory, but

also for the companies and organizations for which the hanging

legislative procedure brings with it considerable legal uncertainties.

12.3 Position determination of the Germans

Data Protection Conference: Telemedia Act

and usage data processing at times

the GDPR

In April, the German Data Protection Conference (DSK) determined its position

on the applicability of Section 4 of the Telemedia Act for non-public

published positions.231 This determination of position was triggered by the announcement

The Federal Government's notification that the Telemedia Act will not be amended

was planned. The DSK therefore considered it necessary to respond to the resulting legal

to react to security and to the application priority of the DS-GVO

to position the Telemedia Act.

A

and

s

i.e

e

right

P

right

a

x

i

s

Contrary to what is intended by the EU Commission, the ePrivacy Regulation is

not finished in time.232 This means that the previous data protection

line for electronic communications,233 which are required by the ePrivacy Regulation

should be put into effect first. In relation to the GDPR, therefore

Regulations that the previously applicable data protection directive for electronic com-

communication through national law,234 still have priority

be turn. This is what the GDPR determines in the context of a so-called collision rule.235

This comes into consideration for large parts of the Telecommunications Act,

which provisions of the ePrivacy Directive

implemented in German law.

231

"On the applicability of the Telemedia Act for non-public bodies from

25 . May 2018", position determination of the conference of independent data protection

Federal and state authorities – Düsseldorf, 26 . April 2018, available at

ter https://www .datenschutz-berlin .de/fileadmin/user_upload/pdf/publikationen/

DSK/2018/2018-DSK-position determination_TMG .pdf

232 For the status of the legislative process, see 12.1

233 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 communications (Privacy Policy for Electronic Communications
nication)

234 Unlike a European regulation, a European directive does not apply
immediate and must be implemented by national law.

235 See Art . 95 GDPR

The Telemedia Act, on the other hand, is different. Here the supervisors had
pointed out for a long time that in particular the provision on
Setting Cookies236 in the Privacy Policy for Electronic Communications-
tion was not or not fully transposed into German law. dementia
speaking, the collision rule in the GDPR for the Telemedia Act
not to wear. National regulations can indeed also then
be preserved in addition to the GDPR if an opening clause of the GDPR so
permitted. However, such is not the case for the provisions of the Telemedia Act
evident. Against this background, the provisions of Section 4 apply
of the Telemedia Act for non-public bodies the priority of application
GDPR.

In practice, this means that for the processing of user data
and users of a website the GDPR applies. data processing,
those for the provision and presentation of the website and to ensure its integrity
of the website are required, as well as certain methods of web analysis or
Range measurements are carried out regularly as part of a balancing of interests
be allowed. If, however, the surfing behavior of the users

across websites, including with the involvement of third parties, in detail

The consent of the data subject is required.237

Already together with the position determination, the DSK had decided in the

Following the publication of the position, a consultation with the

to carry out. As part of a consultation process, we

position towards the economy and will this be further con-

substantiate.

Many websites do not (yet) meet the requirements of the GDPR. This

concerns e.g. B. the cookie banners that are still used, which due to a lack of choice

possibility no consent i. s.d. represent GDPR. Here there is

towards the need for adjustment.

236 See Art . 5 para. 3 of Directive 2002/58/EC

237 We have notes on the processing of usage data for further explanation

published by websites and blogs on our website, available at

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

for-processing-of-usage-data-through-blogs-or-websites/

12.4 Photos at risk? Art Copyright Law and GDPR

The introduction of the GDPR was discussed intensively in public, and

under which conditions the publication of photos is legal. There-

The background is that the right to one's own image, i. H. the power to disseminate

is designed as a simple law by the so-called Art Copyright Act238. Since the

Distribution of photos regularly, but also processing of personal

ner data, comes at least outside of the personal familial

The GDPR can also be considered as applicable law.

A

and

s

i.e

e

right

P

right

a

x

i

s

In the public debate, the fears of photographers and

tographers and journalists play a particularly important role because

these through the DS-GVO restrictions on their artistic freedom or free

feared reporting. For these areas, however, the GDPR is

parts not applicable. If personal data, including photos,

within the framework of freedom of expression on journalistic, literary or artistic

processed for commercial purposes, § 19 BlnDSG applies in Berlin, which

continuously suppressed and referred to the KunstUrhG.

If the GDPR is to be applied outside of these areas, the publication must

The publication of photos is based on a legal basis under Art. 6 DS-GVO

the. If the persons depicted do not give their consent, it must be checked whether

whether another legal fact can justify the publication.

In this context, the regulation on the balancing of interests

tion,239 which involves weighing up the legitimate interests of the

Those responsible (i.e. the person who wants to use the photos) and the

interests of the persons concerned (i.e. those depicted) worthy of protection

sees. Similar considerations play a role in this consideration

also be taken into account within the framework of the KunstUrhG. Specifically, this means

that the legitimate interests of the person wishing to use the photos

238 Act on Copyright in Works of Fine Art and Photography

graphy – KunstUrhG

239 See Art . 6 para. 1 letter f GDPR

subject to special circumstances in individual cases, e.g. B. could then predominate

when it comes to images from the field of contemporary history, images of people

sonen as "accessories" next to a landscape or other location or around

pictures of meetings, processions and similar events. If it

However, if the photos are of children, it must be taken into account that re-

The consent of the children or the parents is required, as children

according to the DS-GVO as particularly in need of protection.

For journalistic, literary or artistic activities that are

move about freedom of opinion and information, has

under the GDPR has not changed much. Essential parts of the GDPR are

excluded from the application in these areas. This also applies to the

publication of photos.

12.5 A Scoring for Judges

s

i

x

a

right

P

right

e

i.e

s

and

A

We took a submission as an opportunity to launch the internet platform www.rich-

terscore.de to undergo an on-site inspection. The platform wants legal

lawyers an exchange about judges,

enable judiciary and courts.

The platform operators collect and store personal data about

the judges working in the courts covered. At the speech

The data is information on the affiliation to the jury (Ti-

tel, name, court and tribunal) resulting from the business allocation plans

of the courts and thus from publicly accessible sources. Besides that

are assessments by the judges and com-

mentare in free text fields. The evaluations of the judges can

based on a scale of up to five stars in the categories of speed,

preparation, willingness to provide information, objectivity and legal knowledge

will.

In response to our intervention, it is no longer just the submission of an assessment, but

where even the mere inspection of the collected data excludes

lich the lawyers registered on the platform

possible. This prevents the content from being shared with an unlimited public

ability to be used for any purpose. At the same time, our

Demand that judges also have access to the above

to provide them with stored ratings by setting up a special

targeted access to judges. In addition, we were able to achieve

always also the specific number of ratings in the individual categories

is displayed so that it can be assessed whether the rating given

is representative. Finally due to our recommendation meanwhile

Word filters used for the comments in the free text fields in order to

to check possible violations of the law.

By listing personal data, the judges

affected in their right to informational self-determination. The one on www.rich-

terscore.de possible ratings affect the social sphere, i.e. the

Area in which the human being privately or professionally in exchange with others

people. In principle, statements in the social sphere can only

be restricted if they have serious effects on the person

privacy rights are to be feared. This is e.g. B. the case when the outer

cause stigmatization, social exclusion or a pillory effect

can,240 but not with the possible ratings on www.richterscore.de.

The evaluation criteria specified on this platform are primarily

objective nature; the evaluation carried out indicates the respective subjective assessment

statement of the lawyer. Consequently, they ask

comments i. s.d. Art. 5 para. 1 sentence 1 Basic Law (GG). Due to the

Design of the evaluation criteria is an unobjective abusive criticism

unlikely. Only in the comments would such a theoretically possible

lich; but this is counteracted with the help of the word filter that has now been set up

works.

Even the fact that the ratings are given anonymously cannot

Inadmissibility of data collection on www.richterscore.de and

- justify storage. Anonymous use is inherent to the Internet.

Limiting freedom of expression to statements that

240 BGH, judgment of 23. June 2009 - VI ZR 196/08, Rn. 41 (so-called cheat-me verdict)

153

153

can be assigned to a specific individual is according to case law

of the BGH with article 5 paragraph 1 sentence 1 GG incompatible.241

After implementing our demands, the platform www.richter-

score.de now data protection compliant.

241 BGH, judgment of 23 . June 2009 - VI ZR 196/08, Rn. 38

154

Chapter 12 Telecommunications and media 13 .1 Freedom of information in Germany

13 Freedom of Information

13.1

Freedom of information in Germany

After years of unsuccessful initiatives, the general

Access to information standardized by law. Both areas of law, data protection

and freedom of information were regulated in one and the same law,242 a

German novelty. After the newcomer from Hesse there are still three

desländer, namely Bavaria, Lower Saxony and Saxony, without information disclosure

health laws.

The Conference of Freedom of Information Officers in Germany (IFK)

retired on the initiative of the Freedom of Information Officers of Berlin, Bre-

men and Schleswig-Holstein issued a position paper on the issue with a large majority

the transparency of the administration when using algorithms.243 The public

Public administrations are increasingly making automated decisions

Using algorithms and artificial intelligence (AI). resulting from this

also from the point of view of freedom of information problems because of these

Procedures work largely intransparently and it is therefore questionable to what extent

these can be used in accordance with fundamental rights. The public administration

is obliged to act in accordance with the law, its decisions must be prior-

be visible and understandable. This can only be achieved if it is guaranteed

can be that the procedures through sufficient transparency and through the

technical and organizational design can be checked and controlled. the

Transparency requirements must already be taken into account during programming

(“Transparency by Design”). The position paper specifically describes the

Obligations of the public authorities, even before the decision on deployment

of these procedures to check whether this is possible in accordance with fundamental rights, because

242 Hessian Data Protection and Freedom of Information Act (HDSIG), GVBI. S. 82 ff.

243 position paper from 16 . October 2018: "Transparency of administration when using

Algorithms are indispensable for the protection of fundamental rights in practice”, available in German

and English version at www .datenschutz-berlin .de/infothek-und-service/ver-

publications/decisions-ifk/

not every data processing is allowed. The task of public

public administrations to ensure sufficient transparency.

In addition, the IFK passed a resolution with which the social

carriers are asked to submit administrative regulations independently of the application, in a timely manner and publish in a user-friendly way.244

13.2 Freedom of Information in Berlin

13.2.1 General Developments

The Berlin Information Freedom Act (IFG) had to - unlike the Berlin Data Protection Act (BlnDSG)245 – not in line with the new European legal framework be adjusted, as the new data protection law has no effect on the material ell-legal provisions of the IFG on the disclosure of personal data ten hat.246 Because the General Data Protection Regulation (GDPR) expressly allows the disclosure of personal data in official documents relating to Fulfillment of a task in the public interest in the possession of a authority or a public or private body.247 Also have the EU Member States expressly have the power to issue special regulations regulations for the processing of personal data for tasks that are carried out in public interest.248 Legally standardized access to official information tion according to the IFG is a task in the public interest. The processing (Disclosure by transmission)249 of personal data is also

244 Resolution of 16 . October 2018: "Social participation needs consistent publication publication of administrative regulations!", available at www .datenschutz-berlin . de/infothek-und-service/publications/decisions-ifk/

245 See 1.7

246 § 6 IFG

247 Art. 86 GDPR, recital 154

248 Art. 6 para. 1 letter e, para. 2 and 3 GDPR

249 Art. 4 no. 4 GDPR

half permissible,250 because it is necessary to fulfill a legal obligation

to which the person responsible is subject.251

However, the GDPR has indirectly influenced freedom of information in Berlin.

So far, the tasks and powers of the Berlin Commissioner for Information

freedom of information in the IFG by referring to the regulations in the "old" BlnDSG nor-

mated. Since these regulations no longer exist, the reference now goes to

Empty. We have therefore approached the leading Senate Department for

Interior and Sport put forward the required amendment to the IFG and with one

specific proposal suggested that the applicable regulations from the "al-

ten" BlnDSG directly into the IFG. These include in particular

more the right to complain252 and the obligation to support public

places.253

The divestment of the powers of the Freedom of Information Commissioners

the BlnDSG is not only for reasons of practicability, but also because

appropriate to the independent importance of freedom of information. For this

also says that the freedom of information officers - unlike the data

protection officers – primarily as arbitration boards and in an advisory capacity

persons submitting the application and the bodies responsible for providing information,

so that the new tasks and powers as data protection officer according to the

DS-GVO not easily transferred to the freedom of information officer

can become.

It remains to be hoped that the corresponding change in the IFG will, if not at short notice,

tig, but then at the latest within the framework of a transparency law

becomes. Because according to the coalition agreement, the IFG should move in the direction of transparency

set to be further developed; a draft - according to the planning of the Senate

Department for Home Affairs and Sport – should be in the House of Representatives in the course of 2019

be introduced. For this purpose and to exchange previous experiences with

250 species. 6 para. 1 letter c GDPR

251 §§ 2, 6 IFG

252 § 26 BlnDSG a . F.

253 § 28 BlnDSG a . F.

she set up a working group at the IFG. We have the working group

offered our cooperation.

13.2.2 Individual Cases

Release of judge data by the administration of justice?

s

i

x

a

right

P

right

e

i.e

s

and

A

The Senate Department for Justice, Consumer Protection and Anti-Discrimination

asked us for an assessment of how the objection to the back

assigned request for information from the operator of the rating portal at www.

richterscore.de should be avoided. The platform wants lawyers

Lawyers an exchange about judges, jury bodies

and enable courts. Among the coveted data was the name, which

respective function as well as the respective share of activity at the court. We have the

Senate administration recommended remedying the contradiction.254

This result was based on the following assessments: If no consent

ment of the judges concerned is the legal basis for

the transmission of the requested data § 3 paragraph 1 sentence 1 IFG. The claim is not

excluded or restricted according to § 6 paragraph 1 IFG. Because of revelation

of the personal data are legitimate interests of the persons concerned

not against. This applied not only to those data for which, according to the rule

Examples of § 6 Paragraph 2 Sentence 1 No. 1 lit. a and No. 2 IFG interests worthy of protection

Those affected usually do not oppose, but also for further

data such as B. the information as to which proportion of those affected in which

are properly active. The legal concept of the aforementioned regulations should be

At least include the decision on the objection.

The applicants' interest in information was understandable and as such

– in view of the now common and comparable offers for doctors –

not to be denied per se. The interest in information was also not opposed to

that the applicants are also pursuing economic interests. Because that

IFG does not offer any indication of such a restriction; rather it lets

254 See also 12.5 (data protection assessment of the platform)

just the free further use of the information obtained, how not

most recently resulting from the repeal of Section 13 (7) and Section 22 IFG in 2015

against the background of the European Directive on the re-use of

public sector formation. The repealed provisions

genes had the use of the information obtained for commercial purposes as

prohibition subject to fines.

The judges concerned had interests in secrecy

Senate Administration not listed and were not visible to us. the

According to § 6 Para. 1 IFG to be carried out, but so far omitted balancing of interests

ment could therefore not be at the expense of the applicants.

The Senate administration has nevertheless rejected the objection and

Access to information, finally, citing the “disproportionate

Administrative effort" rejected, which with the necessary evaluation of approx.

1600 personnel processes would go hand in hand. Electronic are the coveted data

unavailable.

We have encouraged the operators of the platform to resolve the matter

to be clarified by administrative courts.

Electronic application and prepayment of fees at AG Wedding

A petitioner asked us for support because he was on his two electronic

IFG applications at AG Wedding have not received satisfactory information.

He had a list of all the works of art in the district court with

Company and work names, year of purchase and value requested. Another request

concerned copies of all written documents submitted to the district court in 2018

chen complaints and supervisory complaints. AG Wedding has both

Applications rejected, pointing out that no cost statement could be sent by e-mail

resolving application can be made. The district court also stated

that it intends to cover the costs incurred for the provision of information "in advance

to raise bullet paths".

A

and

s

i.e

e

right

P

right

a

x

i

s

In both cases, requests for information were permitted under the IFG.

Because the scope of the law also extends to the courts,

159

however, only to the extent that they perform administrative tasks.255 That was undisputed here

the case. However, the opinion was that an IFG application could not be sent by email

can be made is not correct. Because with the last change of the IFG

expressly standardizes the possibility of submitting an application not only verbally or

in writing, but also electronically.256 On the other hand, the petitioner had the

Statement that the costs may be charged in advance as an inadmissible advance payment

missunderstood. Because this request from AG Wedding was only made just in case

that the petitioner does not have a postal address for the delivery of the fee

wanted to specify.

The cases were nevertheless an occasion for us to refer to the case law of the Oberver-

verwaltungsgericht Berlin-Brandenburg for advance payment of a fee for the

access to information.257 The OVG had made it clear that in

range of access to information, an official act subject to a fee is only sufficient

depending on the prior payment of the administration fee

may be done. The prerequisite is that there are indications of this

are that without the advance payment, the interests of the budget would be jeopardized. Such

Indications would not already exist if the administrative burden for the

access to information is high and possibly after the

exceed the maximum fee provided for in the relevant fee framework. a Kos-

advance payment decision is unlawful if there is a risk to the interests of the household

resses objectively not recognizable and the assessment of the fee solely on the with

administrative effort associated with providing information.

With the now express option of submitting applications electronically

in the IFG a small, actually self-evident step in the direction of digital

done. IFG notifications, which are general and without examining the individual case

demand an advance on costs are unlawful.

255 § 2 para . 1 sentence 2 IFG

256 Section 13 para. 1 sentence 1 IFG, amended by law from 2. February 2018, GVBl. S. 160

257 OVG 12 B 22.12, decision of 26. May 2014

Victory in stages in the district office of Neukölln

A petitioner complained to us that she was in the monument protection

authority of the Neukölln district office did not receive any access to the files. She wanted them

Remodeling, especially of the inner courtyards of those listed as historical monuments

Understand the "IDEAL passage". Inspection of the documents of the

closed procedure is dependent on the submission of a power of attorney from the

senschaft (owner) has been made dependent on what she as a tenant of

listed building could not understand. Later became for the

File inspection on site a fee of 40 euros plus the costs for

copies collected. Also was informed that at the request of the building cooperative

all personal data, company and price information on the occasion of the filing

insight would be blackened. After our first intervention, the monument

copies of documents submitted to the petitioner's protection authority with redactions,

without requiring a power of attorney from the cooperative.

A

and

s

i.e

e

right

P

right

a

x

i

s

After this first inspection of the files, the petitioner asked us again for support

asked because she felt that her information access rights were protected by the Office

were not fully taken into account. We therefore held a sighting of the speech

standing files on site for appropriate. In principle, on-site inspections

against the background of the IFG, it was initially important to understand

what the original process consists of in detail and what information

out for what legal reason the applicant was withheld

will. Therefore we asked for submission of both the original files and those of the

Copies submitted by the petitioner at the file inspection meeting. In addition, we asked

the redactions made in the copies become legal in good time for the on-site visit

to justify. Because according to the IFG, all are contained in files

Disclosing information unless there is a restrictive circumstance

according to the IFG.258 Blackening was only allowed in this case

and could the expenses for this be charged to the petitioner. Whether all

Redactions were legally required was doubtful.

When comparing the original process with the blackened copies, we

states that legal reasons for not disclosing the retained property

258 Sections 4 et seq. IFG

information could not be given. Already the extensive participation

the Department of Environment and Nature of the district office spoke for the fact that it is at

the transaction in question was, as a whole, "environmental information".

According to the case law of the Federal Administrative Court, this term is broad

to interpret; a direct connection between the individual data and the

Environment is not required.259 The district office has checked our recommendations and

the petitioner finally after four months the entire process - moreover

made available free of charge –260 for file inspection.

Through an on-site inspection, we were able to provide the petitioner with a comprehensive

and to provide free access to files.

259 BVerwG, judgment of 23 . February 2017 – 7 C 31 .15

260 According to § 18a para. 4 sentence 3 no. 1 IFG, access to environmental information is available

Location free of charge.

14 From the office

14.1 Developments

The first experiences after the GDPR came into effect on May 25, 2018
confirm that this date is indeed a turning point for data protection
overall and for the supervisory activities of the Berlin commissioners
for data protection and freedom of information (BlnBDI) is to be considered in particular.
The public debate about the new set of rules has both citizens and
Citizens as well as authorities, companies and other institutions for the
Sensitized to the topic of data protection. The handling of personal data
has since become more conscious in many parts of society. The data
processing data subjects are increasingly demanding their data protection rights
the responsible authorities are increasingly realizing that
data protection when introducing new processes or products
must be taken into account from the outset in order to avoid a later technical,
to avoid additional financial and bureaucratic work.
Of course, this development has a significant impact on supervisory
official practice. Due to the immensely increased number of submissions, complaints
and requests for advice that have been sent to the
BlnBDI are addressed, the workload in the entire authority is not
more to deal with. It is far from possible to deal with all inquiries properly
are answered, required tests are hardly feasible.
The situation is particularly problematic when it comes to processing citizen petitions
ben. The number of complaints has increased compared to 2017
nearly quadrupled. Simply because of the large number of (new) incoming complaints

their timely processing is fundamentally at risk. This is critical insofar as

than the clarification, examination and evaluation of complaints

rarely leads to further regulatory action. A timely processing

processing of these processes is therefore important for the supervisory activities of the Bln-

BDI of central and overriding importance.

163

The increase in complaints is mainly due to the fact that

the area of responsibility of the BlnBDI has expanded considerably. Was the

previously only heard for the processing of complaints against Berlin authorities

and companies responsible, the DS-GVO with the so-called market location principle has the

extended to all (national and European) bodies that

offer goods and services to the citizens of Liner or

keep watching. The introduction of the one-stop-shop principle261 requires that

In the case of all incoming complaints, it must first be checked whether a cross-border

continuous reference exists. If this is the case, the BlnBDI, as the lead

authority to inform all supervisory authorities in the EU about the complaint and

to involve all supervisory authorities concerned in the process. Go to one

of the other European supervisory authorities a complaint with cross-border

progressive reference and are thereby the rights of Berlin citizens

and citizens affected, the BlnBDI acts as part of the (European) test procedure

"affected authority".

This leads to complicated, labor-intensive and time-consuming coordination

procedures with the other supervisory authorities, which are also in English

and must be managed under strict deadlines. In order to

to be able to cope, the service center for European affairs was created

fen. Cross-border issues are coordinated via the

electronic internal information system (IMI). The number of

tenuous cases exceeded all expectations. Since the effective date of

In 2018, around 500 cases were entered into IMI under the GDPR. All cases

were checked in the Service Center for European Affairs for a possible

checked by the BlnBDI. In over 150 cases, concern was found

so that the authorities deal with the content of the respective facts

had to.

According to the DS-GVO, responsible bodies can use their products and services (free

willingly) have it certified under data protection law.262 The certification can be carried out by

accredited certification bodies or by the competent supervisory

authorities take place. The accreditation of the bodies is carried out by the Deutsche Ak-

261 Art. 56 GDPR

262 Art. 42 GDPR

kreditierungsstelle GmbH (DAkkS) together with the supervisory authorities

taken. It's a completely new one for regulators

area of responsibility. The activity as an assessor in the accreditation

procedure requires extensive legal and technical special

to know. Appropriate knowledge and skills were at the supervisory

hear not yet available. In order to acquire them, individual workers have

the BlnBDI in training courses of the DAkkS on the requirements for certification

places participated. According to the DAkkS, by mid-October for

Berlin has already received nine expressions of interest in the accreditation of certification

agencies. At that time there were only more in North Rhine-Westphalia

Expressions of interest (12).

In the first five months, the BInBDI received around 5,000 general inquiries
Gen of citizens, companies, authorities, freelancers
Persons, clubs, associations etc. in connection with the implementation of the
GDPR a. A large proportion of the requests for advice were made by telephone. To the
To deal with inquiries, a tele-
fon hotline specifically for questions about the GDPR. You can use this hotline
the citizens, companies, associations and freelancers
People can answer their questions about the GDPR daily from 10:00 a.m. to 1:00 p.m.
2,164 people answered the hotline in the three months it was active
calls in.
Since 2017, the Berlin Commissioner for Data Protection and Information
freedom of movement, start-up companies offer special consultation hours to
to support the development of start-up companies in Berlin. All in all
55 consultations were held with interested companies in the reporting period
carried out. The consultation hours are always fully booked well in advance. If
advice for start-up companies will continue to be offered in 2019
can, in view of the heavy workload on the employees
currently uncertain due to other (mandatory) tasks.
In order to gain multipliers in the implementation of the GDPR, the
Officials of the BInBDI in chambers, associations, authorities and other
directions by the end of December 2018 in a total of 54 specialist lectures on the
application of the GDPR. Not all lecture requests could be accommodated

of official task management are taken into account. Therefore have
many employees of the authority further lectures outside
of service as part of a secondary activity in their free time.

Of the 15 positions requested for the 2018/2019 budget, the BlnBDI
five posts in the higher service, four posts in the senior service and the
Position of a (foreign language) secretary approved. The approved positions
except for one A 15 position in Department III (IT), all filled
will. This position was filled in view of the general
Lack of skilled workers in this area is problematic, so this position is over
was advertised again in 2018. The four other posts in the higher service
tes were recruited with legal specialists to strengthen the service
make citizen submissions, the service centers for European affairs and sanctions
tion as well as the working areas of fundamental questions of the DS-GVO, economy and
Certification/Accreditation occupied. The posts of the higher service were
with officials for clerical processing in the service points for citizens
ben, European affairs, sanctions, in general administration and with
occupied by a media educator.
The experiences from the first months after the GDPR came into effect
clearly show that the positions approved with the 2018/2019 budget
Additional personnel requirements caused by the implementation of the GDPR at the BlnBDI
has arisen, do not nearly cover it. The BlnBDI can fulfill its tasks as
supervisory authority for data protection in the future only properly and promptly
comply if the authority is granted further human resources.

14.2 Cooperation with the Chamber of Deputies from Berlin

The Committee for Communication Technology and Data Protection (KTDat) met
in eleven meetings in which the Berlin Commissioner for Data Protection and Information
give recommendations and suggestions on various topics
could. A particular focus was on adapting the Berlin Data Protection Act

to the new European data protection law.263 In addition, the

electronic class register,264 the law amending the school law265 as well

such as IT security and data protection at Charité266

the referral in the committee.

14.3 Cooperation with other entities

The conference of independent federal and state data protection authorities

the (DSK) met on 25./26. April in Düsseldorf and on 7./8. November in Munster

and passed numerous resolutions on current data protection issues.267

Due to the extremely high need for coordination in connection with the

General Data Protection Regulation also found a total of three special

of the DSK: on January 30th in Berlin as well as on July 11th and September 5th

About in Düsseldorf. The rules of procedure of the DSK also had to be based on

the new requirements of the DS-GVO completely revised and "Euro-

be made suitable for paternity. This was a difficult timely process

was successfully completed before the GDPR came into effect. the

In particular, the challenge consisted in assigning procedures to cooperation

define the voting binding common positions within

allow for the tight timeframes of the GDPR. To achieve this,

the majority principle extended to almost all areas of content, moreover

the representatives in the various European committees

both at managerial and work level with greater autonomy

ness and the distribution of responsibilities between the Germans

Supervisory authorities have been defined more stringently.

263 Word protocol KTDat 18/11 from 14 . May 2018, p. 14 ff.; Word protocol KTDat 18/12 from

28 . May 2018, p. 10f.

Content protocol KTDat 18/15 from 15. October 2018, p. 7

264

265 Minutes of decision KTDat 18/16 of 12 . November 2018, p. 4

266 Word protocol KTDat 18/7 from 22 . January 2018, p. 6 ff.; Word protocol KTDat 18/8 from

19 . February 2018, p. 7 ff.

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

decisions/

167

In the course of the revision of the rules of procedure of the DSK and the review

All responsibilities were assigned to the Düsseldorf group, in which the supervisory

authorities for data protection in the non-public area have so far

had worked after its last meeting on February 28th/February 1st. March in Düsseldorf

village dissolved. With the GDPR, this structure could no longer be represented. the

content coordination for this area is now taking place in the working group

Society of the DSK, which works for the DSK and for the first time on 19./20. September

also met in Düsseldorf.

The Conference of the Freedom of Information Officers in Germany (IFK) met

on March 20 in Stuttgart and on October 16 in Ulm. She made a decision

on the publication of administrative regulations and decided on a basic

typographical paper with suggestions for promoting a cultural change in the public

administration and a position paper on the transparency of administration when entering

set of algorithms.268

The International Conference of Data Protection Commissioners

Protection of Privacy (ICDPPC) took place in Brussels from 21 to 25 October

and passed resolutions on e-learning platforms, on issues of ethics and

Data protection in the development and use of artificial intelligence, to

cooperation between data protection and consumer protection authorities as well as

Rules, Procedures and the Future of ICDPPC.269

The Berlin Group (IWGDPT) met under our chairmanship on 9./10. April in Buda

plague and on 29./30. November in Queensland.270

The Global Privacy Enforcement Network (GPEN) deals with practical

Privacy Enforcement Issues. Also in the realm of practicality

The international exchange helps enormously with the implementation of data protection, because

optimized through local procedures and harmonized across borders

268 More on this in Chapter 13. The papers are available at https://www .datenschutz-

berlin .de/infothek-und-service/veroeffentlichungen/beschluesse-ifk/

269 https://icdppc.org/document-archive/adopted-resolutions

270 For the results, see 12.1

can become. The meeting took place on 13./14. June chaired by the Israeli

schen data protection supervisory authority in Tel Aviv.

14.4 Public Relations

Already in 2017, our authority restructured its press work in order to

to achieve a higher public awareness of the topic of data protection

and to make clear its importance for each and every individual.

This year we answered a total of 202 press inquiries and were able to

nearly double our work in this area. A main topic

was of course the implementation of the GDPR. journalists

In this context, they were particularly interested in how the complaint

de revenue has developed numerically as a result of the legal reform, due to which

Which topics citizens have complained to us about and about which
areas had particular implementation problems. More topics that
were of great interest to the media public was the pilot project
"Sicherheitsbahnhof Berlin-Südkreuz", the referendum for more video surveillance
surveillance and known security deficiencies when accessing the police
national information system POLIKS. Our press team was made up of journalists
Journalists on these and various other topics are available so that the
sometimes difficult data protection and data protection issues
media reporting could be presented correctly and in an understandable way.
With a total of 19 press releases, the Berlin representative for
Data protection and freedom of information with their own topics to the public.
So we could in social discourses, such. B. in the wake of the scandal
around Cambridge Analytica and the data trade of Deutsche Post or at the
Debate about a possible ban on names on doorbells in apartment buildings
sern, do important educational work.
We published the following press releases this year:

• Data protection for children: New children's website www.data-kids.de online
(January 8, 2018)

• Recommendations for data protection in the WHOIS directory at ICANN
(March 9, 2018)
• Working paper "Updating the firmware of embedded systems in the
net of things” (March 12, 2018)
• Invitation to the press conference: Annual Report 2017 (March 16, 2018)
• Annual Report 2017 (March 23, 2018)
• Data trading by Deutsche Post – How those affected can defend themselves

(6 April 2018)

• Open Day and Netzfest: Berlin Commissioner for Data Protection and

Freedom of Information on the Road (May 2, 2018)

• A turning point in data protection. New data protection law: be careful, but not

Panic! (May 25, 2018)

• The new Berlin Data Protection Act – a missed opportunity (May 31, 2018)

• Press release – datenschutzkonferenz-online.de – Homepage of the data

protection conference goes online (July 19, 2018)

• Data protection for cross-border data queries on law enforcement

purposes – Berlin Group calls for standards (14 August 2018)

• 100 days of the General Data Protection Regulation – time for an initial assessment

(30 Aug 2018)

• Warning of subscription trap of the so-called data protection information center!

(October 2, 2018)

• Berlin Group publishes working paper on networked vehicles

(October 4, 2018)

• Position paper “Transparency of administration when using algorithms

indispensable for the protection of fundamental rights” (17 October 2018)

• Doorbells are not a privacy issue (October 19, 2018)

• Berlin data protection officer opens comprehensive audit of operations

from Facebook fan pages (November 16, 2018)

• New privacy tips for teenagers (November 26, 2018)

• Examination of an electronic health card (December 13, 2018)

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 distribution list possible.

14.5 Public Relations

14.5.1 Events

On January 29, at the invitation of the conference of independent data protection

authorities of the federal and state governments held a central event on the occasion

of the 12th European Data Protection Day in the Representation of the State of

Saxony at the federal government in Berlin. The topic was "Sovereignty in the digital

world – an illusion?”.

On May 5th we took part in the joint "Open Day" of the MP

Tenhauses of Berlin and the Bundesrat. The event in the MP

tenhaus of Berlin was connected to the 25th anniversary of the entry of the

Berlin state parliament in the building of the former Prussian state

daytime There we presented a stand with information material on various

those privacy issues. In addition, our subject specialists answered

and speakers for questions about data protection. The following focal points

the offered: data protection rights, what to do against unwanted

Advertising? Register of residents – who has access to your data and why? The European

General Data Protection Regulation is coming! What's new? Privacy and School –

What is allowed, what is not? Both the information stand and the advisory service

met with great interest.

On May 5th, my authority was also present for the first time with a broad information

offer at the Netzfest of the internet conference re:publica. Next to one

own information stand were a lecture and a workshop with topics

about the changes caused by the new European General Data Protection Regulation

regulation (DS-GVO). The offer aroused lively interest among the public,

who also used the opportunity to clarify their own data protection issues.

With well over 2000 visitors during the day, that was it

171

Information provided by the Berlin Commissioner for Data Protection and Information

onsfreiheit at the re:publica Netzfest a complete success.

For the launch of our children's website www.data-kids.de, the Berliners

elementary schools were asked to enter a competition to name the children

that of the robot family.271 The winner – class 3b of the basic

schule am Tegelschen Ort – was held on June 25th in the auditorium of the elementary school in im

As part of a solemn ceremony with the active participation of the children, the

sponsorship awarded.

14.5.2 Publications

Due to the changed legal situation after the DS-GVO came into force on May 25th

it is necessary to check that all information material is up-to-date and

to revise if necessary. We started this in May and already have a series

of brochures published in updated or revised editions. follow

The following brochures are now available to all interested parties:

Current legal texts:

• General Data Protection Regulation: Last corrected text on May 23, 2018

Regulation (EU) 2016/679 of the European Parliament and of the Council of

27 April 2016 (General Data Protection Regulation) with recitals

• Federal Data Protection Act: On April 27, 2017 with effect from May 25, 2018

adopted new version of the Federal Data Protection Act according to the requirements

changes of the GDPR

• Berlin Data Protection Act: New version of the Berlin Data Protection Act

zes (BlnDSG) for the public sector in Berlin with effect from

June 13, 2018

271 For more details on the children's website, see 5 .5

Brochures:

• Freedom of information in Berlin: The rights to information vis-à-vis the authorities

The Berlin governs the and other public bodies of the State of Berlin

Freedom of Information Act (IFG). The updated flyer explains the information

mation and other rights of inspection of every human being and every legal entity

person and describes the procedure and restrictions on the

Currency of the right to file inspection and information.

• I search for you. Who are you? The guide, which has already been published in its 12th edition,

Information on social networks & data protection has been updated

brought. Within the framework of the Berlin state program "jugendnetz-berlin"

published by us and the Senate Department for Education, Youth and Family

This brochure gives ten important tips on how young people can

Protect data on WhatsApp, Instagram and Co.

• My private sphere as a tenant: The guide informs u. about, wel-

che data may be queried in the rental application process, who one

on what occasions during the rental period must be allowed into the apartment, under

what conditions the landlords are allowed to use video cameras

and when data transfers to third parties are permitted.

14.5.3 Lectures

For years, the employees of the Berlin Commissioner for Data

protection and freedom of information an extensive lecturing activity within the framework

of congresses, workshops and training courses. This year the need was for

Specialist lectures are particularly large. We received numerous inquiries, which

Due to the limited capacity, unfortunately only part of the offer could be met.

In the areas of health and youth and family alone, 15

Lecture requests will be rejected.

In order to compensate for the limited individual advice, we have

tries to get as many multipliers as possible through the specialist lectures

tors (e.g. at events organized by industry associations, chambers, specialist publishers

or interest groups). So did the Berlin commissioners

for data protection and freedom of information and the speakers

their authority this year a total of 54 specialist lectures, some of them over a hundred

held by the participants. After the lectures

Questions from the participants were regularly discussed and

answered. Topics that were particularly in demand were:

• Changes due to the GDPR

• New sanction rules

• The testing and supervisory practice of the BlnBDI

• Data protection and media literacy

• Data protection in associations

• The data protection impact assessment

• Anonymization/pseudonymization

• Effects of the GDPR on child and youth welfare

We also regularly offer lectures at the Children's University in Lichtenberg (KUL). In

this year there was an event on November 17th for parents on the subject

"WhatsApp, Instagram & Co. - Of risks and side effects".272 The lecture

met with great interest, the lecture hall was filled to the last seat.

Afterwards, questions from the audience were answered for about an hour

tet. We will also present the lectures on data protection in social networks in

continue to offer for years to come. Interested schools, universities and

other educational institutions can, if necessary, take part in lectures on this

topic please contact us.

Overall, only part of the requested lectures could be given. the actual

material demand was and is significantly higher.

272 See https://kinderuni-lichtenberg .de/vorlesungen/noch-planung-6

Chapter 14 From the Annex service

Speech by the Berlin Commissioner for Data Protection

and Freedom of Information on September 13, 2018 at

Berlin House of Representatives on the annual report

2017

Dear Mr President,

Ladies and gentlemen,

on the agenda today is the statement by the Senate on my

res report 2017. Our testing activities again included a wide range of

practice areas.

The field of video technology and video surveillance was again very important.

We have the use of body cams for the security personnel of the Germans

railway and the expansion of video surveillance in local public transport

table accompanied. On the subject of video recordings in Berlin kindergartens we have

together with the Senate Department for Education, Youth and Family

Guidelines for pedagogical professionals developed. We checked one

system for outdoor advertising that analyzes biometric characteristics of passers-by,

as well as the draft law of the initiative for a referendum for more

deo surveillance, before which we after careful analysis of constitutional

for some reasons.

There were also many exams in the field of housing, what before

not surprised given the tight Berlin housing market. we

have worked to ensure that the district offices meet the requirements of the misappropriation

Comply with the prohibition of information and do not impermissibly disclose intimate information

collect information about the private lives of homeowners.

As part of a large-scale inspection of the real estate industry, we have

forms used there for self-assessment in rental applications

and masses of illegal forms have been taken out of circulation.

175175

Appendix Above all, however, 2017 was characterized by the intensive preparations for

the General Data Protection Regulation, effective May 25 this year

is.

We have advised companies and authorities on the transition to the

Regulation accompanied. But our own work has also undergone profound changes

experience changes. New methods of cooperation between the European and

German regulators had to be developed in order for the day of

Be prepared for the General Data Protection Regulation to take effect. Inside

our authority had to restructure and organize the work processes

be ted. In addition, the preparation of the content for the new

legal regulations are made, also in close cooperation with the others

regulators.

As we now see, the effort was worth it; our preparations have us

helped to master the transition to the new legal system. Although we are on

had hired a considerable amount of extra work, the increase in the

questions, however, once again clearly exceeded our expectations. In the

In the last four months I have received around 1,800 complaints from citizens

citizens, four times as many as in the same period of the previous year. Also the

There is a large number of requests for advice from companies and authorities

an unchanged high level. In addition, I am currently

around ten times as many reports of data breaches as in the previous year. and

there are no signs of an easing of this situation so far. my

hörde works at the limit of its resilience and can only do its job

partially fulfill. I am very happy that I have highly motivated employees

and employees who carry out their work with enormous commitment –

otherwise we could not meet these challenges and would like to do so

I would like to take this opportunity to thank you very much!

Above all, I see these numbers as a success. They show that the new

gelwerk the companies, the authorities, but also the citizens

raised awareness of data protection. This was an important concern of the European

European legislature. The figures show us that the mammoth data

General Protection Regulation takes effect – despite all the teething problems that it

remains to be healed in the coming years.

176176

Appendix It seems important to me at this point to point out again that

the General Data Protection Regulation was a necessary step to civil rights

in a time of advancing global digitization.

The current technical developments are nothing less than a

change for our society. Digitization has now found its way into almost

maintained all areas of life. Some of it has the potential to transform our lives

facilitate and improve. At the same time, however, these developments

also dangers for our free, democratic society.

The quasi-monopoly positions of large data companies mean that this is not the case

only citizens, but also companies and state institutions

tion more and more dependent on them and fair competition

is hindered. In addition, algorithms are increasingly preparing decisions

statements about us humans or even make them yourself. These algorithms are

mostly completely non-transparent, although they have a significant impact on the

life from all of us can have. The rising one is also to be taken very seriously

Danger of manipulated opinion-forming processes or political elections.

The General Data Protection Regulation is an important first step towards

contribute to the protection of our freedom rights worldwide. It may

However, in view of the challenges mentioned, this does not remain the case. So that all

People benefit from the advantages of digitization and they do it carefree

can enjoy, we must counteract undesirable developments. This is for

one the task of the supervisory authorities, which urgently need better

equipment in order to be able to fulfill these tasks. On the other hand

but also politicians more than ever in demand, courageous answers to the big questions

found in our time; there is a considerable need for regulation.

Ladies and gentlemen, I would therefore like to take this opportunity to warmly welcome you

You appeal to your opportunities as elected parliamentarians

mentarians and to work to ensure that necessary regulatory

steps are taken.

The fact that today a Federal Council initiative to combat identity

crime is on the agenda is a good step in that direction.

177177

Appendix But there are many more points where something needs to be done. That's the way it is

urgently required that the European e-privacy regulation finally be

who will also protect people on digital messenger services

should expand. Changes in competition law need to be discussed

and the taxation of digital companies. And urgently need solutions

can be found for the transparency of algorithms. – By the way, this is not

only an issue of data protection, but also of freedom of information. Only in-

informed citizens can make sovereign decisions. and

sufficient information is also a basic requirement for that

such a fundamentally important trust that citizens have in the state.

In an increasingly complex digitized world, in a time of

uncertainty also ensure that alternatives to the offers

ten offered by global digital companies. That creates trust

that creates independence and that creates freedom for the development of the

local economy.

We should all see data protection and freedom of information as an opportunity

to bring our democratic and liberal values safely into the future

gen. Let's work together with civil society and businesses

work actively and constructively on new solutions!

Thanks very much!

178178

Appendix Glossary

2 factor

authentication

Anonymous/Pseudonymous

Art. 29 group

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 (e.g. a password),

that only she knows

3. Biometric characteristics of the person like theirs

Fingerprint.

Anonymous data can no longer be assigned to a person

be assigned. In the case of pseudonymous data, this is one

certain third party possible under pre-determined

laid down conditions.

Group according to Art. 29 European Data Protection Directive

line, made up of representatives of all

European data protection authorities.

It has an advisory function; primarily opposite

the European Commission, but also towards

other data processors within the European

sian union.

Car to X

communication

Generic term for networking from vehicle to vehicle

or from a vehicle with the infrastructure.

Chief Information

Security Officer (CISO)

clusters

Responsible for the development of security

security guidelines, for alignment, planning and co-

ordination of measures to ensure the

Security of data processed by an organization

information and for evaluating the implementation

of these measures and the remaining risks.

Derives from English "cluster" = "cluster", "amount"

and stands for dense accumulation of houses,

Development in groups, clusters of high-rise buildings.

179

Glossary Cookie

Cookie Banner

CRO

double opt-in

procedure

GDPR

A cookie is a text file that is used to communicate with a

website related information on the computer

ter of the users to be saved locally

and the website server on request back to over-

average This allows users to

recognized and visited websites as well as time

points of the visit are assigned.

Banners are graphic or animation files that are included in the

Website are embedded and either at the edge

appear or overlay the website. In the

usually contain these advertisements. cookie banner

usually contain information on the use of cookies

and are usually connected to a simple "OK" button

see.

CRO stands for Clinical Research Organization

tragsforschungsinstitut). This is a

Service companies for the medicines and

Medical device manufacturing industry, which the

Research and development of drugs

medical products in the course of planning and implementation

development of clinical studies.

Double opt-in procedure refers to a process in which

the user after entering their contact details

in a distributor this in a separate second

step must be confirmed again. Mostly this becomes

an email message asking for confirmation

sent the given contact details. There-

In addition, a confirmation can also be sent by SMS or

be done by phone.

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 across the EU

become sane. On the one hand, this is intended to protect

personal data within the European

Union ensured, on the other hand the free data transfer

end-to-end

encryption

fan page

traffic within the European single market

be achieved. The regulation he replaces the from the

1995 Directive 95/46/EC on protection

natural persons in the processing of personal

related data and free data traffic. she is

already came into force on May 24, 2016, but was

due to a two-year transition period only on

Effective May 25, 2018. Since then she has been in all member

States of the European Union directly applicable

bar.

"Electronic Identity" - This is a

NEN electronic proof of identity (with chip), with

whose help electronic processes are carried out

can.

The content of a data transmission is encrypted

rare that only the receiver specified by the sender

decrypt the data d. H. make readable again

can. intermediate stations such as B. E-mail provider se-

only encrypted data.

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 dated

network provided communication

means to market, e.g. B. by changing the side of Face-

book users recommended or

shared in the "circle of friends" of the users

becomes. The fan page is also a public profile and

can be accessed by people outside the network

be fen it will appear in the relevant search engines

rails indexed, d. H. listed in the result list.

In contrast to the profile page, which is used by private individuals

is used, it is not about "befriending", but

more about using the page z. B. directly with customers

to communicate in the network or to gather "fans" together

melt

gamification

geodata

GovData

A device's firmware is software stored in electronic

niche devices is embedded to their basic

to ensure function. It is by user/

inside not or only with special means or radio

functions interchangeable. Firmware is functionally fixed with

connected to the hardware; one is without the other

not usable.

From English "game" for "game"; denotes the use

of game-typical elements to increase motivation

tion and behavior change among users

users.

Digital geological data, e.g. 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

these accessible in their respective open data portals

have done.

GPS / GPS transmitter

global positioning system; German: Global Posi-

on determination system.

hash function

hash value

It is a cryptographic hash function

is a mathematical calculation rule,

from any output data such as

a document or even just a word or a

Phone number a unique check value with fixed

length calculated. This calculation is not inverse

bar – the output data can be derived from the test values

cannot be calculated back. In case of repeated

calculation with the same initial data results in

but always the same test value.

The hash value is the result (the check value) of the

use of a [above] cryptographic hash function

tion. This is a mathematical one

Calculation rule resulting from any output

data such as a document or also

IP address

IT architecture

coherence method

link

Market place principle

just a word or a telephone number

unique fixed-length hash value.

Understands the preservation of the integrity of data

to protect them from accidental loss or

unintentional falsification or the correct function

tion of systems.

Internet protocol address = the address of a computer

ters on the internet.

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

found by the supervisory authorities involved

can be, the European data protection

shot within the framework of the coherence procedure

che resolutions. In addition, in the coherence

proceed with the aim of uniform application

of the DS-GVO also opinions of the European

Data Protection Committee − 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 covers this

non-European companies operating on the European

ic market, even if they are not

authorized in the European Union. By the

Market location principle should be uniform

ments are created for all companies that

goods and services on the European market

offer gene.

Glossary metadata

microblogging

One stop shop

open data

The data generated during data transmission and

is divided into content data – for example the text

an e-mail - and all other so-called metadata that the

relate to communication circumstances, d. H. Time,

Sender, recipient, locations for mobile devices

ten as well as technical addresses/identification numbers of the

devices used for communication.

Microblogging uses short SMS-like texts

created in a blog or short message service

to be set. It doesn't work with microblogging

about going thematically in-depth, but

within a short time and without great effort

set up to produce all kinds.

The one-stop shop principle means that both

every citizen and every company

can contact the local supervisory authority.

This also applies in particular if personal

collected data are processed across borders,

e.g. B. through social networks or other international

nationally active companies. The supervisory authority at which

a complaint has been filed, informs the

Complainant about the status and the result

of the procedure. For companies with branches

genes in different member states is the supervisory

authority at the headquarters of the central administration

interlocutor. All of these regulators are on

involved in and respect regulatory procedures

together that the rights of women citizens

and citizens are preserved.

Databases that are available to citizens

as the economy without restriction to free circulation

be made freely accessible for further use.

Open government

Opening of the state and administration to the citizens

citizens and the economy.

OWASP10 criteria

Criteria established by the Open Web Application Security

Project, a global foundation dedicated to the advancement of

Network Security, have been published.

Glossary Pixels

PNR data

pre-recording

function

Privacy by default

Privacy by design

profiling

test value

Small graphics on websites, which are usually only 1x1 Pi-

xel measure and when calling up a website from a

servers are loaded. The download will be regis-

and can be used for evaluations in the field of online

line marketing can be used.

PNR stands for Passenger Name Record. These are flight

guest records, which include contact, travel, and

Payment information also information on nutrition

ing habits and the state of health of the

travelers can count.

Denotes the recording and storage of a

pre-allocated time range in an endless loop,

i.e. i.e. it is a recording function,

in which a few seconds before pressing the

recording button to save the data

follows.

Products are made with the most privacy-friendly

delivered with presets.

The manufacturers already take data protection into account

in the manufacture and development of products.

Profiling includes any type of automated evaluation

certain personal aspects of a natural

chen person to understand. About these aspects

such as work performance, the economic situation, the

Health, personal preferences, the interests that

reliability, conduct, whereabouts or

possible changes of location of a person belong. target of

profiling is to carry out an analysis in this regard

men or to make a prediction. profiling is coming

e.g. B. in the field of advertising and in the initiation of contracts

used, but the police are also increasingly using

based on corresponding prediction methods.

The test value is determined using an irreversible cryptic

tographic hash function from the phone number

calculates.

185

Pseudonymize Glossary

Source code

registrant

ring memory

proceedings

score value

sensitive data

Social Plugins

Pseudonymizing is replacing identifying

Information such as name, address, date of birth or

their unique identifiers or characteristics

another designation (e.g. a sequential number

mer) such that an inference to the person without

Knowledge of the assignment rule not or only with in-

proportionate effort is possible.

The program code (technical basis) of a software

were.

Person who registers a website with an organization

organization that registers internet domains

(at the so-called registrar).

Stores data continuously in a certain time-

space and overwrites it after one expires

predetermined time again to free up space for

release new data.

Numerical value representing the credit worthiness of a

person describes. The score value is

and credit bureaus using a mathematical

table-statistical method and serves as

Basis for contract decisions.

Special Types of Personal Data. In addition

include information about racial and ethnic

origin, political opinions, religious or philo-

sophistical beliefs, union membership

health, or sex life.

A program code that is integrated into the website

and the browser of the user

Zers of the website caused content from a

to request third parties and to provide data to these third parties

transmitted, e.g. B. Facebook “Like” button

or "Twitter" button.

telematics tariffs

tracking /

Cookie Walls

wearable

The social sphere is the area in which man

is in exchange with other people.

This is both private and professional

area includes.

Insurance tariff, the contribution of which depends on the

Vehicle usage is calculated. included

the z. B. the number of night trips, trips in risky

edged areas or on accident-prone roads

and compliance with speed limits

and the acceleration behavior. For this purpose

intensive electronic monitoring of the

witness activities and transmission of the data to the

Insurance. These tariffs are also known as “Pay as

you Drive” tariffs.

Preventing the use of a website if you do not

accept cookies.

Wearable computers, or wearables for short, are

computers that are so small that they don't have a room

still need a desk, otherwise

because e.g. B. worn as a bracelet and glasses or in

Clothing can be incorporated. During the

application they are on the body of the user

and often directly connected to the Internet

the. So e.g. B. a blood pressure monitor, which

permanently or for a longer period of time on the arm

is worn, quite as a device from the area

called wearable computing.

web tracking

Observation and analysis of users

Users for business and marketing purposes.

WIFI base stations

device for wireless data transmission; will mostly

used for wired internet access

mobile devices in the vicinity of the use of the

nets without having to connect cables

senior

187

Glossary WiFi tracking

A technique with which the movement of people

can be tracked using location data,

which, with recourse to the smartphone of this person

be recorded.

188

Glossary Index

A