annual report

the Berlin Commissioner for Data Protection and

Freedom of Information as of December 31, 2019

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 28, 2019

Annual Report 2018 submitted and covers the period between 1 January

and December 31, 2019 onwards.

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

www.datenschutz-berlin.de

imprint

Publisher: Berlin Commissioner 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/

april agency GbR

Layout:

LayoutManufaktur.com

ARNOLD group

Sentence:

Print:

This publication is licensed under a Creative Commons

Attribution 4.0 International License and may citing

of the author, changes made and the license are freely reproduced,

be changed and disseminated. Commercial use requires prior permission

Approval by the Berlin Commissioner for Data Protection and Information Release

Ness. The full license text can be found at https://creativecommons.org/

licenses/by/4.0/legalcode.de.

Contents

Notice

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

different technical terms.

8th

List of abbreviations

Working group of German market and opinion research institutes

Treaty on the Functioning of the European Union

general equality law

Law Implementing the Judiciary Law

tax code

General safety and order law

Federal Financial Supervisory Authority

Federal Data Protection Act

Operational integration management

Civil Code

Federal Law Gazette

Federal Court of Justice

Federal Cartel Office

Abghs.-Drs. House of Representatives printed matter

ADM

TFEU

AGG

AGGVG

oh

ASOG

BaFin

BDSG

BEM

Civil Code

Federal Law Gazette

BGH

BKartA

BlnAGBMG Berlin Implementation Act for the Federal Registration Act

BlnDSG

BMI

BMG

BMGVwV

Berlin Data Protection Act

Federal Ministry of the Interior, Building and Community

Federal Registration Act

General administrative regulation for the implementation of the federal

registration law

Federal Ministry for Economic Affairs and Energy

Federal Office for Security in Information Technology

Bundestag printed matter

Federal Constitutional Court

Federal Administrative Court

Berlin transport company

Federal Association of German Volksbanken and Raiffeisenbanken

curriculum vitae

German Savings Banks and Giro Association

General Data Protection Regulation

Conference of the independent data protection supervisory authorities

Federal and the states

BMWi

BSI

BT-Drs.

BVerfG

BVerwG

BVG

BVR

CV

GDPR

GDPR

DSK

9

Digital Supply Act

European Data Protection Board

recital

E-government law Berlin

European Union

European Court of Justice

Federal IT cooperation

Joint Federal Committee

DVG

EDSA

ground floor

EGovG Bln

EU

ECJ

FITKO

GBA

GeschGehG Law for the protection of business secrets

GG

GRCh

AMLA

HTW

ICIC

IFG

IFK

IMI

ISBJ

IT

ITDZ

IWGDPT

constitution

Charter of Fundamental Rights of the European Union

Money Laundering Act

University of Technology and Economics

International Conference of Freedom of Information Commissioners

Freedom of Information Act

Conference of Freedom of Information Officers in Germany

Internal Market Information System

Integrated software Berlin youth welfare

information technology

IT service center

International Working Group on Data Protection in Telecom

nication (so-called Berlin Group)

annual report

Commission to determine the financial needs of broadcasting

shape

Artificial intelligence

small and medium-sized companies

Communications Technology and Privacy Committee

Children's University Lichtenberg

Association of Statutory Health Insurance Physicians

State Agency for Civil and Regulatory Affairs

State Office for Refugee Affairs

State Office for Health and Social Affairs

Online Access Act

Public Key Infrastructure

JB

KEF

AI

SMEs

KTDat

CUL

KV

LABO

LAF

LOCATIONSo

OZG

PKI

10

POLICIES

PStG

RBStV

RL

RSD

SenIAS

SGB

StbergG

StGB

StPO

TMG

TSG

do

UWG

VBB

VG

vig

VK

VvB

WJH

State police system for information, communication and

processing

Personal Status Act

State Broadcasting Agreement

policy

Regional Social Pedagogical Service

Senate Department for Integration, Labor and Social Affairs

social code

Tax Advisory Act

criminal code

Code of Criminal Procedure

Telemedia Act

transgender law

Technical University

Unfair Competition Law

Transport association Berlin-Brandenburg

administrative court

Consumer Information Act

United Kingdom

Berlin constitution

Economic youth welfare

11

12

Foreword Foreword

The General Data Protection Regulation (GDPR) is effective. The groundbreaking character

of this European law for data protection in Europe and also above

is becoming more and more noticeable.

So we in Berlin can look forward to an exciting and successful year

of the GDPR. It was the first full year with the new law

situation and we could observe in our work that the data protection

che sensitivity has increased significantly in almost all areas. responsible

People turn to us much more frequently with questions and problems and

gen increases the importance of good data protection management.

Above all, among the citizens, there is a strong and unflagging

of the interest in the protection of their personal data. This

Interest was with the introduction of the GDPR and in this context

intensive public discussions on the subject have increased significantly

and has since settled at a very high level. My authority has

several thousand complaints from citizens last year

processed, viewed and evaluated over a thousand reported data breaches,

intensively with other experts at national and European level

work and, last but not least, a wide range of consultations and audits by companies

companies and authorities as well as a considerable number of sanction procedures

carried out.

Increasingly, there are also large fine proceedings against supranationals

active companies in focus. Naturally, for checks in

these areas in view of the complex data processing to be found there

maintenance systems regularly require a great deal of work and time, be-



before results can be achieved. But more than a year after

With regard to the DS-GVO, we are ready to take measures for the first major cases

Securing data protection to take us while doing the new skills

to use, which the DS-GVO makes available to us. result of this development

Among other things, this was the first fine in Germany in the double-digit million

lion height.

Measures are always taken against the background of the basic idea of the DS

GMOs enact that in an increasingly digitized society dem

Data protection can only be helped to a breakthrough if violations

whose principles are punished in a perceptible way. This happens

always according to the principle of proportionality and before

due to the economic performance of the respective company or

the respective organization. Beyond the individual procedures, there must ultimately be a goal

be subject to data protection sanctions, bodies that personal

process data, to show that on the one hand it is worthwhile to actively protect data protection

operate, and that on the other hand it can hurt badly if you

does not comply with legal requirements.

The judgment of the European Court of Justice last year was also significant

to the Facebook Like button. The court found that not only Facebook,

but also website operators who use the Facebook Like button or others

Use social plugins for related data processing

jointly responsible. Already in 2018, the European Court of Justice

for Facebook fan pages the joint responsibility of Facebook and the

determined by the operators of the fan pages. We then had

Trials initiated against Berlin fan page operators, which are still ongoing.

Those responsible must make it clear that the obligations associated with such

entailed joint responsibility, cannot be fulfilled without further ado

are. The same applies to the data protection obligations,

which can be obtained through the integration of Google Analytics and similar third-party services

ten into its own website. Website operators should therefore be careful

consider whether they want to use such offers at all.

In the digital area, data protection-compliant design and use is also important

of mobile apps is an increasingly important topic. In addition to the



Foreword Use of messenger services such as WhatsApp by public authorities

increasing spread of health apps, which often contain very sensitive data

process users. In both cases, the implementation of suitable technical

shear and organizational measures as well as a transparent information

policy regarding the purpose and scope of data processing for a

legally compliant use is essential. There is still a lot of catching up to do here

with those responsible.

The more our life is shaped by digital applications, the more important it is

is the early education of people from childhood on about risks and

Rights related to the processing of your data. Only who

drive and knows one's own options for action, can protect one's

Take data into your own hands. At the same time, one can even use the sensitization

don't start early enough. For this reason, we have

work in the field of media education has been intensified in order to

to make children aware that when using digital

Media varied information is collected in the background about them and

can be misused in a variety of ways. For this we have, among other things, further on

our children's website and were delighted to learn that they

was nominated for the German children's software award TOMMI.

Even if the focus of our activities in the past year was inevitable

the implementation of the GDPR was, but things are also happening in the area of information

some freedom: In Berlin there are first signs of the creation of a transparency

visible after some federal states have already passed such laws

, which oblige government agencies, to the public on their own initiative

provide information about their work. We welcome this path

expressly and will parliament and government implement such a

according to the law in Berlin with words and deeds.

About one and a half years have passed since the introduction of the GDPR; they were on-

rigorous, but very instructive and overall very successful. Everyone with

Data processing and data protection are concerned, had to deal with the

learn new rules. However, our experience shows that not only

Citizens whose rights are sustainably expanded by the GDPR

were, have won. Companies can also benefit from the new regulations

benefit if they take data protection seriously. In a globalized and

digitized world, the GDPR has the potential to protect the fundamental right to information

to make self-determination viable for the future. It remains exciting!

Berlin, April 3, 2020

Maja Smoltczyk

Berlin Commissioner for Data Protection and Freedom of Information



Foreword 1.1. Messenger services in companies and public institutions

1 focus areas

1.1

Status essential – messenger services

in companies and public

facilities

Messenger services on private smartphones are often also used for business

material or business purposes. Especially in sensitive areas

e.g. the health and school systems – this entails high risks

Consequence. We have worked on the development of a handout for the conference of the

independent data protection supervisory authorities of the federal and state governments (DSK)

involved in the subject, a hospital chain to advise and pointers

given to the Berlin school administration.

A

and

s

i.e

e

right

P

right

a

x

i

s

The thrill of quick news

What to do when the competent medical colleague is on standby, but far

from the bedside and to make a decision as soon as possible

fen is? One, two snapshots of the relevant diagnostic results and

a request is sent via WhatsApp to the colleague who is already calling on the way

technically can give first indications for further treatment. This is a scenario

rio, which is hardly talked about and yet it is something like that now

quite common in many hospitals. The advantages for the treatment

ment (faster response times) and for the hospital (simplification of the

on-call duty and less strain on employees) are obvious

lich. An additional attraction: At first glance, there are no costs.

Ambulatory nurses travel a lot. Also for them are messenger services

an inexpensive and versatile tool. You will receive changes to the

sentence planning, can ask questions to the colleague who was at the the day before

same patient. The news is timely. Unlike

a telephone call, the current activity does not have to be interrupted in order to

to accept. Even later you can read what you can do with oral

much more likely to forget communication.

At school, too, both the pupils and

Pupils as well as the parents themselves about short-term changes in the school process

quickly informed. It represents a time-saving alternative to informing the

affected and all participants have the same

information. Those who do not want to use messenger services-

ten, but are initially excluded from this.

The hidden risks

The use of messenger services in cases such as those described above

brings with it a number of privacy issues. is reinforced

this if the communication takes place with the private devices of the employees and

the sent data is therefore subject to the direct control of the respective institution

are withdrawn.

Many of the well-known, publicly accessible messenger services are problematic

table because the service providers, above all WhatsApp, which belongs to Facebook

Ireland Ltd. with their free WhatsApp offering, not just the messages

transmit, but at the same time pursue their own monetary goals. For her it is

beneficial to know the communication patterns of the people who use their

Use services in order to be able to send you advertising messages.

In this context, the use of measuring

ger services in the professional environment.

s: When companies and authorities send their employees or communication

ask partners to use a messenger service,

in which an inadmissible use of data for the business of the messenger service

heard, then they bear part of the responsibility for this infringement.

It starts with the fact that most service providers open the address book without being asked

data from the smartphones. Also some non-commercial offers like Si-

go ahead like this.

But companies or public bodies need a legal basis

when they ask their employees to use a messenger service

and thereby cause data of private third parties in the address books

of the smartphones of the employees are included at the respective service



be passed on to bidders. Since there is no legal permission for this,

all private communications contained in the respective address book

cation partners for consent to this transmission

ten. However, this would hardly be practicable. Therefore one should

Messenger app used in the professional environment only those data to service

te providers who need them to send the respective messages to the

to be sent to the correct recipients. In practice will

only the unique identifiers of sending and receiving

persons (often their phone numbers).

The mass of critical data from the use of messenger services falls

when exchanging messages among the participants. Even if the

Because the messages are encrypted, the providers find out who is with whom

communicates. This information is what is known as traffic data.

Even if these are sometimes banal, you can use many of these traffic data

extract quite relevant information that is by no means banal. At-

for example, it represents information worthy of protection as to who is with which doctor

or which doctor is communicated, since relevant conclusions can be drawn from

current state of health can be drawn.

In addition, several factors may increase the risk that the providers

ter of the messenger services unlawfully collect the traffic data themselves
use or disclose to third parties. First, messenger services are currently subject
not (yet) the telecommunications law and thus the obligation to
special protection of traffic data. Second, some of the largest service
te providers or the groups controlling them are located in third countries,
whose legal systems allow access to the traffic data by state authorities
authorities also allow under conditions that are not permitted by European law
are covered. The latter circumstances can also change in the short term due to the
Relocation of company headquarters or change of shareholders or
dominant companies. In 2019, for example, this happened at the
Wire Swiss GmbH, the provider of the messenger service Wire. And third-
The place of data processing can also change to a legally less secure place
Relocate the environment because the service provider consciously decides to do so or
allow a cloud service provider working for it to do so.



All these circumstances also have an impact on the protection of confidentiality
quality of the transmitted data. Admittedly, encrypted
procedure for the application, which, if carried out correctly, the transmitted
Protect data also against the service provider. In some cases
these processes even have extremely high requirements. But is it
It is up to the service provider to control whether, how and with which ones
keys the data is backed up. Institutions that hold a public fair
senger service must therefore carefully check the reliability of the
respective service providers as well as the legal and technical design of the
weigh the products offered against the consequences of any disclosure
of the transferred data for the data subjects.

If an institution contacts private individuals via a messenger service

det, e.g. a bank to its customers, there are additional

Confidentiality risks stem from the fact that the security features of the devices that

used by the data-receiving persons, often far behind those of official

chen devices fall behind. In doing so, it is neither permissible to

to exclude a communication channel because they do not have a suitable device or

want to use, nor these people to a form of communication

push that endangers their own data. Therefore, in any case,

be provided that access to the communications can also be made in a different way

than is made possible via the messenger services.

In addition to guaranteeing confidentiality, each professionally

established the sending of personal data with a messenger service and

in the subsequent storage of the messages on the devices of the

communication partners also the other data protection principles

to comply with and to grant the rights of those affected. This is often forgotten: The

Institution remains responsible for data processing. Also about data that

are initially only stored on the devices of the employees involved,

it must be possible to provide information at the request of the person concerned. It must be the

There is a possibility that the data will be corrected and their processing

restricts or can be deleted. If they are no longer needed, they are

to delete them without being asked and without delay. For other purposes, the

Data will only be used if this is proportionate and with the original

common context in which the transfer took place.

A legally compliant use of messenger services not only achieves
desired effect of quick and easy communication for the benefit
of the persons concerned, but also protects their rights at the same time. In addition
the app used, the transmission service and the tools used must
councils meet basic requirements. In many cases there is also an integration
of the messenger service in the other data processing of the responsible
literally necessary to comply with data protection principles and the
to guarantee the rights of data subjects and any existing documents
to fulfill documentation obligations. The latter can usually only be implemented
if the service is provided by or specifically for the company
a processor is provided.

The messenger application must first clearly show what is happening with the
transmitted data, the traffic data and, if applicable, the usage data. If
the app is used to store sensitive data, then it may only be used after
Enter a special password and, depending on the risk, a second security
security feature grant access to the stored data. storage and
The data must be transmitted in encrypted form using state-of-the-art technology.
gen. If the app is to be used for different purposes, then it should be
enable messages to be sorted according to their purpose. she needed
also at least functions for exporting the saved messages and
for their deletion.

The delivery service must keep the messages uncorrupted and end-to-end
encrypted at the end. Information about the use of the app by private
users may only with the consent of the respective users
used by the service provider and transmitted to third parties. Data
companies are only allowed to decide about the use of the app by employees

can be evaluated by contractors if this is required by e.g.

agreement or similar there is a legal basis and the employees are informed

are. The companies may then collect and store traffic data to this extent

and evaluate how this is necessary in order to transfer personal data

Data under their responsibility for legitimate purposes, including in particular the

Data protection control to be able to understand.

21

If sensitive data is processed, it must be ensured that only authorized persons have access to the

message exchange and enter the origin of the messages

is clearly recognizable. The messages themselves belong in a memory from which

them for further use and, if necessary, documentation by the respective body

can be removed. If there is no transfer to other systems,

These memories also serve as a database for information to data subjects who

were not involved in the communication themselves. Of course they can

Messages are not stored permanently. In many cases, the messages

ten contents are no longer required a short time after dispatch. Than are

they on the devices used and, as long as no storage obligations apply,

also to be deleted in the central memory.

The devices, mostly smartphones, used for communication

den, must offer adequate security. This starts with an up-to-date

operating system on. Known security gaps must be closed quickly

the. To ensure that malware cannot wreak havoc on the devices,

the devices also receive a secure configuration. The safe configuration

ration must depend on the risks, among other things, on the access protection of the

devices, encrypting device memory, controlling the installation of

Apps whose timely updating and protection of the interfaces

cken. A central tool is required to control the configuration

the so-called mobile device management. From the sensitivity of the messages sent

depends on how strict this configuration must be kept. Should

e.g. patient data are sent between employees in a hospital

den, then all access routes for

Malware to the devices to be closed.

Since such control of their private devices cannot be expected of employees

a company that needs fast communication

wants to benefit among its employees, in these cases smartphones or

Provide tablets for official use.

Are public messengers always taboo in schools?

If a public messenger service is subject to data protection regulations by its provider

is provided correctly (this is currently not the case for WhatsApp), this can be done for



communication in the school sector can be used if the following additional

additional conditions are met:

• First, the offer of information about school operations via a fair

to make available only a voluntary offer for those affected

represent bot. It must be ensured that the information

reach students and their parents without them having to

need to use messenger service.

• Second, according to the Berlin School Act, approval is required

the school management and an obligation on the part of the teachers to observe

data protection regulations,1 insofar as teachers do not have official

have terminals. Only in such narrow exceptional cases would the use

the use of private smartphones, tablets or laptops is permitted by law.

• Thirdly, organizational requirements must ensure that on the

private end devices only data with low protection requirements are processed

the. In particular, no performance data of the students may be recorded

Student or health data exchanged via the messenger services

become.

In practice, however, this is difficult to guarantee. We have therefore

National Administration for Education, Youth and Family that we have the necessary

digkeit, for the state of Berlin to have its own messenger service in the future

to provide. This would be technically at a manageable cost

to be realized on the basis of available software, like similar projects

show in other states.

Doing nothing is not an option

The same applies to other areas in which sensitive data are processed

the. As already shown, messenger services for the

official or operational communication is used without the data

legal framework conditions are complied with. Here there is-

1

See Section 64, Paragraph 2 of the Berlin Education Act



need for action. So how can and must those responsible for the

counteract the improper use of messenger services?

A mere ban is not a sufficient option. Put the employees their

private devices, then the ban can be checked by looking at the devices

not permitted. Therefore, the respective institution must be sufficiently attractive, but

at the same time offer legally compliant alternatives. You can first

or, where acceptable under data protection law, a suitable public one

Messenger service for general organizational communication established

in which no sensitive data is processed. For the attractiveness of a

to increase such in-house messenger service and thus the use

to reach exclusively this service for official purposes, offers itself

its connection with specific internal information offers

which e.g. internal social offers or similar. may affect. The offer more appropriate

official devices and their configuration according to the security requirements

changes would be the next steps that would result in a release of the messenger service

tes also for the transmission of sensitive data within the respective work

area can culminate once secured that only adequately protected

devices can participate in the communication.

Messenger services offer a welcome facilitation of communication

tion in various institutions. But many common services go

accompanied by risks that are unacceptable under data protection law. In order to

avoid, the respective institutions must provide a suitable service carefully

select and check for risks or operate them yourself. doing nothing is not

option more.

## 1.2 Artificial Intelligence

Artificial intelligence (AI) is currently used as a generic term for various algorithms

algorithms based on automatic learning – mostly based on many

Examples - based. The increasing use of such algorithms is

have a significant impact on society. are particularly relevant

the impact on privacy, since "smart" algorithms already

efficiently analyze and use the mountains of data that have now accumulated. The question

s

i

x

a

right

P

right

e

i.e

s

and

A

Chapter 1 Focus 1 2 Artificial Intelligence

is, for what purposes this happens, for whose benefit and whether affected persons

actually given the opportunity to object to the processing of their personal

understand and control the data collected.

A main area of application for AI algorithms is decision-making

systems, e.g. systems at banks, which decide whether and to which

conditions customers are granted loans or whether a certain

unauthorized use of a credit card could potentially be a case of fraud.

This can lead to wrong decisions, which those affected often only

difficult to correct. Are algorithms used here that are based on

based on tomatic learning (the technical term is deep learning), can often

even their manufacturers or programmers no longer say why and why

on the basis of which data a decision was made in the individual case.

Advocates of algorithmic decision-making systems argue that

People tend to make biased decisions. Through

Algorithm support - careful development and testing

exposed - could be achieved that less false or discriminatory

decisions would be made. So autonomous vehicles would accidents though

cannot absolutely prevent it. The hope, however, is that the algorithms

Among other things, due to their higher reaction speed, they prevent significantly more accidents

than would be possible for people in comparable situations.

It must be countered that such decision-making systems are by no means

way are infallible, but it is not possible for them in comparison to humans,

to respond individually to the special features of the individual case. Therefore, the

thought the use of such decision-making systems would lead to exactly the opposite result-

that are by no means more objective than human decisions.

That there is, for example, systematic discrimination against population groups

due to unforeseen interpretations of personal data

Algorithms can come is already known. So was at a large

Online mail-order companies use software used to select applications

switched after it turned out that based on the previous

Previous hiring practices only male people for hiring



chose. The reason for such wrong decisions is often

that the initial data for learning the algorithms, the so-called training

depict information, prejudice or discrimination. The lack of transparency

Algorithms then lead to preference and discrimination of people

groups cannot be viewed in the system and only when

come to light.

The lack of transparency has other implications. When people

data processing and the risks associated with it, a

decision can no longer be questioned and justified, an effective

Consent to such data processing is also hardly possible. A

essential tool by which citizens control the

processing of data concerning them is undermined.

This becomes particularly clear when apparently harmless data is

execution of an automated evaluation are transferred and

shows that the algorithm used is able to draw conclusions from this data

visibly sensitive characteristics of the respective person, e.g.

your sexual orientation or psychological personality traits.

Demands on automated decision-making systems

There will be no stopping techniques like machine learning and AI

will be used more and more in the future in the course of their further development. Then

Of course, the techniques mentioned can, in principle, have many positive

have effects such as B. higher accuracy in medical diagnostics

senior Nonetheless, there are a number of ways in which controlling intervention is required. The data-

Safety supervisory authorities have recognized this and in the spring a "task force KI"

launched to address the 97th Data Protection Conference (DSK).

Hambacher declaration to prepare the data protection requirements

to artificial intelligence systems. This Hambacher Declaration was

at the 98th DSK in November supplemented by a position paper on recommended

technical and organizational measures in the development and

drive of AI systems combined with basic recommendations for a

data protection-compliant design of such systems.

The declaration2 formulated by the supervisory authorities is based on the
AI strategy published by the government and gives data protection law
recommendations for action. It assumes that for AI systems the basic
processing of personal data3 apply and their enforcement
accordingly also in this context through technical and organizational
toric measures must be ensured4.
The requirements laid down in the declaration relate to six different
different areas. In accordance with the prohibition of a purely automatic
ized decision-making5 should not be permitted by the use of AI
objects are degraded. The respective purpose for use must be specified in advance
be clearly defined and be within the constitutionally legitimate area
because of. This earmarking must also not be used in connection with the for
the data sets collected for the training of the algorithms. Further-
towards the use of AI should always be transparent, comprehensible and explainable.
be made, which is the prerequisite for non-discriminatory application
of AI systems. In particular, the careful and the respective risk of
Data processing appropriate selection of the training data is important here
tion. They must be accurate, relevant, representative and up to date. Even if at
AI systems regularly require large amounts of data in order to
To ensure appropriate training of the software is the principle of data
note minimization. This should preferably be done by
previously anonymized data is used. If this is not possible, must
the scope of the processed personal data in an appropriate
relation to the training success achieved with them. To ensure compliance
good principles and to ensure the security of the processed data,
clear responsibility when using AI systems is essential, isn't it?

lastly, so that those affected know exactly who they can contact to enforce their

rights.

2 https://www datenschutzkonferenz-online de/media/en/20190405_hambacher_erklae-

tion pdf

3 Art 5 General Data Protection Regulation (GDPR)

4 See Art 25 GDPR

5 Art 22 GDPR



Finally, the supervisory authorities emphasize the importance of carrying out technical

shear and organizational measures to ensure data protection

compliant use of AI systems. In the absence of existing standards

this in the above DSK position paper specified. Not only is the

search for a definition of the term "KI" that is as selective as possible based on the typ-

picical life cycle of an AI system. The requirements of

Hambacher declaration will now be explained in more detail and to provide an overview

possible technical and organizational measures. The measure-

measures are based on what is to be granted from a data protection perspective.

achieved result, e.g. in the transparency of the origin of the data

or minimizing the personal reference of the training data used.

In the following, two key parameters of the use of artificial intelligence

intelligence are to be considered in particular: the question of transparency and

refrain from exclusively automated decisions.

transparency

Algorithmic decision-making systems often work in a non-transparent manner. providers

and vendors consider the internal logic as trade secrets and ask

therefore insufficient information available. This lack of transparency

is particularly unacceptable when the systems concerned are making decisions

meet that have critical or adverse effects on affected people

can use.

To balance the interests of the data subjects and the providers

and providers of the decision-making systems is therefore the disclosure of the

to demand procedures against independent control bodies. Next to

the training data itself must reveal its origin and weighting,

with which they flow into the learning process of the respective algorithm; also are

to enable practical tests of the algorithms. In addition, it must be documented

how the training data was checked, in particular for

hold systematic errors. The judgment algorithm mentioned above

of applications, for example, learned from previous human attitude

divorces.



Another reason for limited transparency is the procedures used.

With a so-called neural network, the creation of a result

ses normally not readily understandable or even logical in a

justify it in a way that a human decision-maker or a human

what decision-maker could do – a “black box” is created. Before use in

critical areas, it would therefore be worth asking whether other methods would be preferable

hen whose function can be understood more easily. Anyway

are also used in neural networks or systems that use different techniques

combine, research methods that improve traceability.

One possibility is, for example, to repeat a decision-making process several times with each

because partially changed input values can be run through. In this way

one learns which input values are really relevant for a certain result

were and can disclose this information to those affected.

Do without fully automatic decisions

Whenever possible, fully automatic algorithms should be avoided.

to make table decisions. Art. 22 Para. 1 General Data Protection Regulation

ordinance (DS-GVO) says: "The data subject has the right, not one

exclusively on automated processing - including profiling -

based decision to be subjected to the legal

effect or significantly impair it in a similar way." Rather

should algorithms support employees when making decisions

support based recommendations so that clerks can understand

can make hard decisions.

If the algorithm used is not able to provide a reason, it may

also not make a recommendation, but at most a pre-selection after

meet data to be checked.

An example from our test practice: A test is carried out in the state administration office in Berlin

AI-assisted examination of subsidy invoices to detect possible fraud

to identify cases. For this purpose, a service provider examines pseudonymised

courses. The AI only marks billing processes that have changed significantly

differ from the norm. This does not constitute any suspicion or even a prior

division. In any case, an internal manual check of the data takes place,



which either shows that the deviations can be explained or

suspicion is justified and must be investigated.

In time-critical areas, such as controlling autonomous vehicles,

it is hardly possible to involve a person in the decision-making process.

Instead, more emphasis must be placed on the detailed preliminary check of the algorithm

rithms and a clear allocation of responsibility for possible errors

become.

There are areas, such as the military, that are particularly reliant on the restriction

of fully automatic decisions must be passed: an al-

algorithm to decide whether people die by triggering a weapon

ben. However, not only ethical aspects speak against the use of autonomous weapons.

pects. Such a development would also lead to a new arms race

and ultimately lead to the uncontrollability of future military conflicts,

when different sides use autonomous systems and human

mando chains are far too slow to prevent or

limits.

However, a decision-making system that is fully automated in the first step can

be accepted if the impact on those affected is minimal

and the decisions made can be revised. In this case

it would only be necessary to provide opportunities for objection.

The use of AI algorithms to process personal data

Data needs a design that respects privacy and ethical issues

included in advance. Transparency must be established, the effects

for individuals and society must be considered, discrimination

avoided and humans in their control over the algorithms and their

turn to be strengthened. Developers and users have a duty to

benefits that can be achieved with AI in a fair manner and the rights of the persons concerned

to realize a respectful way.



Chapter 1 Focus 1 3 Address rental for advertising

1.3 Address Rental for Advertising

A large number of the complaints we receive relate to processing

of contact data by organizations6 for advertising purposes. Contact while doing so

Companies and organizations not only people who give them their contact

provided the data themselves. They often “rent” datasets from

other companies, which they then use for their advertising. At this

Address rental does not transfer the records to the advertising organization

passed on: The advertising organization provides a sample sales letter

the rental company. This (or a service company)

then inserts the leased addresses into the letter and sends them. The

In this case, the renting organization has no knowledge of which persons

the advertising was sent in detail, as long as it was not sent via Post-Return

runners or contacts of the recipients their data

experience.

A

and

s

i.e

e

right

P

right

a

x

i

s

Is this allowed?

The question of the extent to which this practice is permissible has been the subject of several

difficulties that we had to decide. Specifically, we lay, for example

Complaints against a mail order company. The company

had the addresses of his customers to process the orders

queried and saved. The company then sent these addresses

rented to organizations without the consent of the customer,

who wanted to advertise themselves. The complainants

then received advertising letters from one, especially in the run-up to Christmas

number of organizations with which they otherwise had nothing to do.

The use of postal addresses for advertising purposes is not legal (anymore)

expressly regulated. The legal situation changed with the introduction of the GDPR

changed. Until May 25, 2018, the Federal Data Protection Act (BDSG)

It is true that companies are required to use lists of addresses that they have collected themselves.

agreed purposes (so-called list privilege). Profession-

6 In the following, this term refers to both companies and

beneficial organizations



Any addresses could then be rented out for advertising in a professional context

otherwise addresses for advertising of non-profit organizations

tion.7 This provision has been removed with the introduction of the GDPR

please. The rental of (customer) addresses for advertising letters is subject (only

nor) the general provisions of the GDPR.

After that, addresses can only be used for advertising purposes without consent

if there is a legitimate interest and insofar as protection-worthy

interests of those affected do not stand in the way.8 In the assessment, the

reasonable expectations of the person concerned based on their relationship

the person responsible are taken into account. The decisive factor is whether the

Sending advertising letters in the respective social sphere typically

is accepted or rejected.9

In one specific case, the company had argued that it was in its hands

legitimate interest in renting out his customer data for advertising purposes. It

has indicated that this is also the case in its general privacy policy

stated.

However, when we weighed up the interests, we came to the conclusion that the

Rental of customer addresses for advertising purposes usually the protected

contrary to the interests of the customers. Because it corresponds

not the general expectations of a person who mail order something

ordered that they subsequently receive commercials from various organizations

holds.

Customers in the mail order business typically provide their address data

wise for the purpose of contract processing, in particular for sending the

ordered goods, available. They regularly do not expect their

Address also an unknown number of third party organizations for

is made available for promotional purposes. Because stand by these organizations

7 § 28 Para. 3 No. 2 and 3 BDSG old version

8 Art 6 Para 1 lit f GDPR

9 EC 47 GDPR



her in no way. That this is the case is particularly evident from the

frequent complaints against these address trading practices.

The mere fact that a company rents out its customers

addresses in the privacy policy does not mean that the

Customers must reckon with the conclusion of the contract that

receive limited promotional mail. The data protection declaration is not intended to

create justification for data processing. those responsible must

first check whether intended data processing is permitted. Only if they

determine the admissibility of the processing and then want to carry it out,

they must inform the data subject.10 On the other hand, data processing

processing for which there is no legal basis is not permitted because the

processing is informed.

As a result, renting customer addresses for advertising purposes without

consent is generally inadmissible. Companies that store the addresses of their customers

Customers and customers who want to rent them out for advertising purposes must sign up for this

regularly obtain separate consent from them.

Who is responsible?

Another question that we have examined in this context is whether

who is responsible for this form of data processing, i.e. against whom we

may need to take regulatory action.

We received several complaints about unsolicited advertising from organizations

nizations that rented addresses for their advertising from other companies

had. The promotional letters were sent on behalf of these organizations

and looked like they came straight from there. Based on our request

these organizations often insist that they are not responsible for data processing

be responsible. After all, they would never have owned the data themselves, would they?

processed. While this may be the case, it absolves the organizations concerned

not in any case from their responsibility. According to Art. 4 No. 7 DS-GVO is for

a specific data processing responsible, who alone or jointly with

others about the purposes and means of data processing. About the

10 Art 13 GDPR

33

However, the purposes and means of data processing can also decide who

does not process data itself, i.e. has no access to it.11

In the case of address rental for advertising purposes, the advertising (rental

tende) Organization significantly involved in the purpose of using the addresses:

It is she who is responsible for the data processing associated with the rental of the address.

only initiates and makes possible. She is therefore also in common with the

renting company responsible for data protection for the processing

processing. Accordingly, it is also our responsibility to supervisory procedures

rer authority against organizations come the addresses for advertising purposes

had rented.

What information must the advertising company provide?

Recipients of advertising mail often turn to

the advertising organization and ask them what data they have stored

chert and where they come from. You have a right to this information.12

They then regularly receive the simple answer that there is no data from

saved. This is also true in principle (see above).

However, this information is not sufficient. Because as together for the

those responsible for processing13 must also ensure that the advertising organization

that those affected receive all the information to which they are entitled. This applies

even if they do not have this information themselves. The advertising organization

tion must then at least identify from whom they received the relevant data

has rented, and ensure that the rights of those affected by the rented

tending organization are met.14

Companies usually need the consent of the data subjects

obtain their addresses for advertising purposes to other companies

or organizations want to rent. If addresses for advertising purposes

are rented, for this data processing are both the renting

11 ECJ, judgment of June 5, 2018 – C210/16 – Wirtschaftsakademie Schleswig-Holstein,

EU:C:2018:388, paragraph 38

12 Art 15 Para. 1 GDPR

13 See Art 26 GDPR

14 Article 26 (3) GDPR





and the advertising organization jointly responsible according to Art. 26

GDPR. This means, among other things, that the advertising organization is jointly responsible for

literal is that data subjects receive all information upon request,

to which you are entitled under Art. 15 GDPR.

## 1.4 fine concept

The DSK has a concept for assessing fines for violations of the

GDPR passed by companies. The aim of the concept is a uniform

correct, transparent and comprehensible application of the legal requirements

of the GDPR for the assessment of fines15 by the German supervisory authorities.

The publication of the concept took place after the first negotiations

European level for the concrete assessment of fines had taken place, in

to whom the draft version of the concept was submitted by the German representative

had been brought.

A

and

s

i.e

e

right

P

right

a

x

i

s

The declared aim of the GDPR is to standardize the practice of fines.16 There are

an express regulation, according to which a harmonization of the determination of

Fines should be promoted through guidelines.17 Therefore, on May 25, 2018, the

European Data Protection Board (EDPB) in its first plenary session

guidelines for the application and determination of fines.18 These

Guidelines outline a unified approach to the principles of

setting of fines, but do not yet contain any specifics on the setting

method. It is reserved for later EDPB guidelines, the content of which

currently being discussed at European level.

Until the EDPB has drawn up final guidelines, the fine concept of the German

technical supervisory authorities should be the basis for sanctions practice in Germany,

to ensure the application of uniform standards when assessing fines

create. Due to the lack of practical experience,

15 Art 83 GDPR

16 EC 150 GDPR

17 Art 70 para 1 lit k GDPR

18 Article 29 Working Party WP 253 endorsement of 3 October 2017



changes and additions to both the concept and the practice of

supervisory authorities through new findings from the Europe-wide votes in

possible in the future.

The fine concept was chaired by the Sanctions working group of the DSK

developed by our supervisory authority. It takes place in the assessment of fines in

drive against companies within the scope of the GDPR, but not with

Fines against associations or natural persons outside their economic

chen activity application. The concept also develops no binding with regard to

the setting of fines by courts.

In the development of the fine concept, the parties involved initially contacted each other

the procedures for setting fines by the Federal Financial Supervisory Authority

performance supervision and oriented by the Federal Cartel Office. Both institutions

calculate the specific fine based on the size of the

ning body, which uses its annual turnover of a certain size

group and the severity of the individual case.

With a view to determining a basic amount, the basis for the calculation

of the concrete amount of the fine, the parties involved also have to contact each other

those on which the calculation of fines is based in German criminal law

so-called daily rates. Daily rates are a unit of calculation for monetary

penalties, which are based on the average daily income of the accused

is formed.

According to the fine concept, the concrete fine is calculated in five steps:

First, the affected company is assigned to a size class (1.),

then the average annual turnover of the respective sub-group of size

class determines (2.), then determines a basic economic value (3.), this

Basic value by means of a factor dependent on the seriousness of the circumstances of the crime

multiplied (4.) and finally the value determined under 4.

general and other circumstances that have not yet been taken into account (5.).

36

Chapter 1 Main points 1 4 Fine concept

1. Categorization of companies according to size classes

Based on its size, the affected company is assigned one of four

assigned to classes (A to D) (Table 1).

The size classes are based on the total global

total turnover of companies19 and are subdivided into micro-enterprises, small

and medium-sized enterprises (SMEs) as well as large companies. It applies according to EC 150

DS-GVO the term "company" within the meaning of Articles 101 and 102 TFEU20 (so-called functional

onal company concept).

The size classification of the SMEs is based on the previous year's

zes in principle to the recommendation of the Commission of May 6, 2003 (2003/361/

EC).

The size classes are used for a more concrete classification of the companies.

divided into subgroups (A.I to A.III, B.I to B.III, C.I to C.VII, D.I to D.VII).

Table 1

micro, small and medium-sized enterprises

Enterprises (SMEs)

large companies

Distinction according to annual sales in millions of euros

A

B

C

D

micro

take: ≤2

≤0.7

A I

AII

≥0.7-1.4

AIII ≥1.4-2

small sub

take: ≥2-10

B I

BII ≥5-7.5

BIII ≥7.5-10

≥2-5

medium

take: ≥10-50

≥10-12.5

C I

C II

≥12.5-15

CIII ≥15-20

CIV ≥20-25

C V

≥25-30

CVI ≥30-40

CVII ≥40-50

Large companies:

≥50

D I

≥50-75

DII ≥75-100

DIII ≥100-200

DIV ≥200-300

DV ≥300-400

DVI ≥400-500

DVII ≥500

19 See Art 83 (4) to (6) GDPR

20 Treaty on the Functioning of the European Union



2. Determination of the average annual turnover of the respective sub-group

size class

Then the mean annual turnover of the subgroup in which the company is included

was classified (Table 2). This step is used to illustrate

ment of the determination of the basic economic value based on this (3.).

Table 2

micro, small and medium-sized enterprises

Enterprises (SMEs)

large companies

Distinction according to annual sales in millions of euros

A

A I

AII

A III

0.35

1.05

1.70

B I

BII

B III

B

3.50

6.25

8.75

C

D

C I

C II

CIII

C IV

C V

C VI

C VII

11:25

13.75

17.50

22.50

27.50

35.00

45.00

D I

DII

DIII

D IV

D V

D VI

D VII more concrete

62.50

87.50

150.00

250.00

350.00

450.00

Annual sales*

* From an annual turnover of more than 500 million euros, the percentage fine limit of 2%

or 4% of the annual turnover as a maximum limit, so that the respective

companies, a calculation is made based on the actual turnover.

3. Determination of the basic economic value

The mean annual

resales of the sub-group in which the company is classified

divided by 360 (days) and thus an average

calculated daily rate (Table 3).

Chapter 1 Main points 1 4 Fine concept

Table 3

micro, small and medium-sized enterprises

Enterprises (SMEs)

large companies

Distinction according to annual sales in €

A

972

2 917

4 722

B

9 722

17 361

24 306

B I

BII

B III

A I

AII

A III

C I

C II

CIII

C IV

C V

C VI

C VII

C

31 250

38 194

48 611

62 500

76 389

97 222

125 000

D

173 611

243 056

416 667

694 444

972 222

1 250 000

D I

DII

DIII

D IV

D V

D VI

D VII more concrete

daily rate*

* From an annual turnover of more than 500 million euros, the percentage fine limit of 2%

or 4% of the annual turnover as a maximum limit, so that the respective

companies, a calculation is made based on the actual turnover.

4. Multiplication of the basic value according to the severity of the offence

After that, based on the concrete crime-related circumstances of the individual case (cf. Art. 83 Para. 2 Sentence 2 DS-GVO) a classification of the severity of the offense in easy, medium, heavy or very heavy.

For this, according to Table 4 below, taking into account the Circumstances of the individual case based on the catalog of criteria of Art. 83 Para. 2 DS-GMO determines the severity of the allegation and the respective factor with which the basic value is multiplied. With regard to the different fines There are frameworks for formal (Art. 83 Para. 4 DS-GVO) and material (Art. 83 Para. 5, 6 DS-GVO) violations to choose different factors in each case. In the Choosing the multiplication factor of a very serious crime, it should be noted that the individual fines are not exceeded.

39

Table 4

| degree of severity | Factor for formal violations according to Art. 83 Para. 4 DS-GVO | Factor for material violations according to § 83 para. 5, 6 DS-GVO |
|---|---|---|
| light | 1-2 | |
| middle | | |
| difficult | 2-4 | |
| very difficult | | |

4-6

>6

1-4

4-8

8-12

>12

5. Adjustment of the base value based on all other pros and cons

Concerned speaking circumstances

The amount calculated under 4. is based on all for and against the person concerned

or adapted to the circumstances of those affected, insofar as these have not yet been made

under 4. were taken into account. This includes in particular all perpetrator-related

Generic circumstances (cf. catalog of criteria of Art. 83 Para. 2 DS-GVO) and others

Circumstances such as a long duration of proceedings or an impending payment

ability of the company.

The fine concept guarantees a comprehensible, transparent and

individual form of fine assessment. At the same time it is through the

Consideration of all circumstances in the concrete procedure of the individual case

right. This enables comprehensive judicial review and

Enforceability of fine assessment possible.

1.5 The cooperation of the data protection supervisory

authorities of the EU is picking up speed! - The

Service center for European affairs

The GDPR obliges the data protection supervisory authorities of the EU member states

states to cooperate closely in cross-border data processing.

In order to do justice to this new task, our authority has the service

set up European affairs.

40

s

i

x

a

right

P

right

e

i.e

s

and

A

Chapter 1 Focus 1 5 The Service Center for European Affairs

Incoming complaints - but also all cases that we raise ex officio

attack and data breaches reported by companies – will initially

checked whether the objected processing of personal data

relates to cross-border data processing.21 This is particularly the case

the case when the person responsible is in more than one member state of the

EU is established and processing in several of these establishments

he follows. However, even in cases of only a single establishment in the EU

there is also cross-border processing if the processing

tion has a significant impact on data subjects in more than one

member state has or can have.

The Berlin Commissioner for Data Protection and Freedom of Information accordingly

speaking not only complaints against Berlin companies and authorities,

but also complaints that companies headquartered in other EU countries

affect member states. According to the so-called one-stop shop principle

cross-border data processing, the supervisory authority at the headquarters

of the company as the lead supervisory authority is the sole contact

partner for those responsible.

The GDPR stipulates that a co-

surgical procedure is carried out and intended measures between

these are to be coordinated.22 For this reason, cross-border

cases, an examination of whether the case processing in addition to the responsible

supervisory authority, other affected supervisory authorities are also to be involved.

The coordination in such matters takes place via the entry into force

The electronic internal market information system (IMI) set up under the GDPR.

All communication between all European clients takes place via IMI.

supervisory authorities. Incoming complaints with cross-border

train, our service point reports European matters as a first step

in IMI to determine the lead and affected supervisory authorities

den ein.23 To do this, she opens a new process in the system and summarizes the content

21 Art 4 No. 23 GDPR

22 Art 56, 60 ff GDPR

23 Art 56 GDPR



of the complaint and names the suspected responsible party and the

supervisory authorities presumed to be affected. Then the various

Authorities have a month to review the process and claim to be concerned

or lead authority. Even if by a leadership of

Berlin Commissioner for Data Protection and Freedom of Information can be assumed that

the service point registers the complaint in IMI so that other authorities concerned

to inform.

However, the determination of the lead supervisory authority does not take place in

all cases easily. In one case, a complainant complained

e.g. via a company that offers its services to German-speaking people

customers, but according to the data protection declaration, the headquarters are in a different

ren Member State has. However, the supervisory authority of this member state shared

that the company is not registered there and that no location can be

be. After our authority contacts the branch in Berlin

had informed us that the branch had meanwhile

had been given up and the main branch was located in another

member state.

If it is confirmed in the procedure described that the spring guide at

the Berlin Commissioner for Data Protection and Freedom of Information is

we will continue to process the complaint and contact the person responsible.

In the event that the lead management is assigned to another European supervisory

authority, the service point for European affairs forwards the complaint

to the relevant authority for processing. For this purpose, the complaint must

English to be translated as communication between different

supervisory authorities takes place in English.

The lead supervisory authority takes over the further determination of the

behavior and drafts a resolution after the conclusion of the examination, which they all

concerned supervisory authorities. They then have four weeks to

to check the draft. Within this period you can object to the

Submit a draft.24 This ensures that a consensus can be reached between the

24 Art 60 Para 4 GDPR

European supervisory authorities on the legal assessment of the respective case
consists.

Around 822 cases were processed in IMI in 2019 to identify the lead and
concerned supervisory authorities. All cases were reported in the service
put European affairs on a possible impact or leadership
checked by the Berlin Commissioner for Data Protection and Freedom of Information. In
more than 390 cases, i.e. almost half of the cases, were affected by ours
Authority determined, so that we deal with the content of the respective facts
had to deal with.

Our authority is currently processing 35 complaints that we received from other
have been sent to supervisory authorities for processing. In addition
we already have a large number of complaints from those affected
received, which we transmit to other supervisory authorities for further processing
had to make changes because we were not in charge. Also in these cases
However, if we are the contact person for the complainants
deführer and inform them regularly about the status of the processing.

The number of complaints reported in IMI, investigations and
Data breaches have steadily increased. However, it is noticeable that the supervisory authorities
in the meantime have already conclusively checked for many companies
who is the lead regulator, so many incoming complaints
can be transmitted directly and the procedures are already
accelerate. This also leads to an increase in draft decisions that
Coordination between the European supervisory authorities published in IMI
become.

Our authority has already raised objections to resolutions in several cases

thrown in by other supervisory authorities, so that these

the authority had to be revised again. This concerned, for example, a case

in which the lead supervisory authority does not refer to one at all in terms of content

breach of data protection alleged in the complaint had been received. she planned

despite a clearly existing data protection violation, the procedure

ren. With the help of the objection, our authority still wants to do this

unresolved case that the data protection violation is established



and appropriate supervisory measures by the lead supervisory

supervisory authority to be met.

That against draft decisions in cases with a cross-border connection with

can be proceeded with the help of objections, the cooperation

between the supervisory authorities. This way you can

the decisions of the authorities are mutually reviewed until an agreement

agreement is reached or a dispute between the supervisory authorities

the EDSA, which was set up when the GDPR came into force

Working level, non-solvable cases final and binding for all EU

authorities to decide.

A particular problem is caused by the use of different national

onal procedural rules. In some member states25, for example, a so-called

amicable agreement as a measure to end the procedure. Through this

measure, numerous complaints are received from some supervisory authorities between

between the responsible company and the complainant.

settled with the complainant. The complaint is then deemed to have been withdrawn

and the data protection violation is neither determined nor subject to a regulatory

subject to measures.26 In the GDPR, an amicable agreement is

However, driving end measures are not provided, with the exception of the

Mentioned in a recital, which, however, only applies to a specific

limited scope.27 This led to conflicts between the

shared regulators. In our opinion, the application of good

Agreements as a measure to end the proceedings are extremely problematic.

Because with the amicable agreement, the coordination provided for in the GDPR could

agreement procedures between the supervisory authorities can be circumvented if the

Complainant to the assertion of claims

data protection rights are waived and the data protection violation is not sanctioned.

The application of such a national legal instrument can

25 So in Austria, Belgium, Czech Republic, Finland, Greece, Hungary, Ireland, Italy,

Lithuania, Latvia, Netherlands, Poland, Sweden, Slovakia, Great Britain, Estonia In

In Germany, an amicable agreement is not regulated in data protection law

26 Article 58 (2) GDPR

27 EC 131 GDPR



Chapter 1 Focus 1 5 The Service Center for European Affairs

not be wanted under European law, because the desired European unity

agreement in the area of data protection is impeded.

As already mentioned, the EDPB decides in cases where the supervisory

authorities do not have the lead or the legal assessment of a

agree on the facts. The so-called cohesion provided for in the GDPR for such cases

procedure28 is intended to ensure a uniform level of data protection in the member states

worry. In the event of disputes between the supervisory authorities, the EDPB issues a

A binding resolution to settle the dispute in cases where the

the supervisory authority concerned an objection to a draft decision of the

lead supervisory authority.29

An example from our case practice is based on a complaint that

received from our authority and from the supervisory authority of another

Member State has been processed as the lead authority. the complaint

führer complains about an incorrect data protection declaration on the website of a

bel company. In addition, the person concerned complains about an inappropriate

casual use of cookies on the company's website. As part of

of the cooperation procedure, the lead supervisory authority has

supervisory authorities concerned first submit a draft resolution to

mood.30 The lead supervisory authority did not present any

violation of data protection, but announced that the proceedings would be discontinued. There

however, in our opinion, there have been multiple data protection breaches

we appealed against this decision. We have argued that

the company has violated transparency regulations, for example. Besides that

were users in the data protection declaration only generally about the use of

Cookies informed, but neither in relation to the deployment and use of

Analysis services nor in relation to the integration of third-party providers (Facebook,

Twitter, Criteo). Since the revised draft decision of the responsible

supervisory authority did not remedy these deficiencies, the EDPB must now coherently

decision on the case if the lead supervisor

I still don't hear improved.

28 Art 63 GDPR

29 Art 65 Para 1 lit a GDPR

30 See Art 60 Para 3 Clause 2 GDPR

The European cooperation procedure is in the year after the entry into force of the

DS-GVO has been filled with life. Our authority works in a variety

of cases with other supervisory authorities. conflicts between

Supervisory authorities have so far been rather rare and are usually agreed

solved, so that the EDPB has not yet had to make a decision.

But such a thing could soon be imminent.





## 2.1 Berlin administration on course for success?

Online portals are becoming the virtual entrance to the town hall. With just a few clicks

should citizens and companies digitalize their concerns and claims

tal and can process them completely electronically.

### Current status of digitization

The Online Access Act passed by the federal legislature in August 2017

(OZG) stipulates that by the end of 2020 administrative services for citizens

and businesses need to be available online, with traditional

walkways, e.g. B. by post or via a citizens' registration office, should continue to be open

len. With the establishment of a portal network, all administration portals of

Federal, state and local governments are networked with each other. From any location

From now on it should be possible to use every online service.

A

and

s

i.e

e

right

P

right

a

x

i

s

The implementation of the OZG is coordinated jointly by the Federal

Ministry of the Interior, Building and Community (BMI) and the Federal IT Cooperation

tion (FITKO), which promotes cooperation between the federal, state and local governments

coordinated. The federal and state governments, with the involvement of the municipalities

575 administrative services to be digitized were identified in 14 different

various subject areas were summarized. Each topic should now

leading in each case a tandem of representatives of the

technically responsible state ministry and the technically responsible federal

departments, supported by representatives of others

interested states. The preparation of the digitization of the concrete

Administrative services for the individual subject areas are carried out by the authorities

comprehensively jointly by the experts from the federal and state governments in these

tandem groups. The developed solutions can then be used by all federal states

otherwise be taken over.

47

The State of Berlin, together with the Federal Ministry of the Interior, is responsible for the topic

responsible for "cross-section". It is about administrative services that

apply to several subject areas; These include e.g.

wise, such as presenting a birth certificate. If within the scope of inheritance
Provision of an electronic administrative service, e.g. the submission of a
birth certificate may be necessary, this could be realized in various ways
be ted. In order to avoid media breaks, it would be conceivable that the data
the birth certificate with the consent of the user directly at the respective
Birth register can be queried. Also uploading a scanned
birth certificate by the user in an administration portal appears possible.
However, if this is not desired, it should remain possible
submit a copy of the proof in paper form.
With increasing digitization of administrative services, there are increased
Requirements for the transparency of administrative actions towards users
to end. Art. 5 of the General Data Protection Regulation (GDPR) sets the
essential principles for the processing of personal data.
Personal information may only be obtained lawfully, in good faith
processed in a manner that is comprehensible to the data subject
become31. The so-called data protection cockpit is of particular importance.
The purpose of the data protection cockpit is to show citizens
are what data from them, in the context of providing an electronic
Administrative service, “from where to where” flow. The requirements of a
Data protection cockpits are currently being carried out in a so-called digitization laboratory under
division of various actors32 defined. We are involved.
Current status of state legislation
As part of the implementation of the Federal Online Access Act (OZG),
State of Berlin state regulations for the implementation of administrative
gearing prepared. In our last annual report we discussed this in-
formed that the Senator for Interior and Sport a draft law

to improve online access to administrative services of the Berliner Ver-

31 Art 5 Para 1 lit a GDPR

32 Including a Federal Ministry of the Interior, for Building and Community as well as various specialist administrations, including the Berlin Senate Department for the Interior and Sport, the Federal commissioned for data protection and freedom of information etc





administration (Online Access Act Berlin – OZG Bln)33. This year
the parliamentary legislative procedure was initiated. Because our im
Previously expressed criticisms were only insufficiently considered, ha-
If we present this again to the responsible technical committees,
brought. Fortunately, this has meant that we are once again with the
Senate Department for the Interior and Sport to enter into the professional discourse and
significant improvements in data protection law.

Again and again we pointed out that it is necessary and expedient
It is reasonable to have your own legal bases for the processing of personal data
to create data in the Service Account Berlin and the other basic ICT services34
fen. To base the data processing solely on the consent of the user,
as originally intended by the Senate Department for the Interior and Sport,
would therefore lead to considerable difficulties in practical implementation
problems, as consent can also be revoked at any time. It is
very gratifying that the Senate Administration ultimately followed our advice. Then
to ensure that the use of the digital service is voluntary
the introduction of consent was not required. The voluntariness
the use of the digital offer is ensured by the determination
provision in the E-Government Act Berlin35 that citizens also know

afterwards can decide whether they want a service on conventional

Art or want to apply electronically.

In terms of the best possible transparency of administrative action, it was us

also important that a provision in the law ensures that citizens

citizens in cases where the required for a service

Evidence (e.g. a certificate) requested directly from other registers

or retrieved, can view them again in advance.

33 JB 2018, 2 1

34 These are information and communication technology applications

genes that are used by various administrative procedures of public bodies,

to provide electronic administrative services

35 Section 4 (7) E-Government Act Berlin



The digitization of administrative services can only be successfully

run when the users are ready to perceive them. For the necessary

Widespread acceptance is a far-reaching transparency of the electronic administration

action is essential. Clear legal regulations help here. We

will continue to actively support this process.

2.2 Digital key board for authorities

necessary

s

i

x

a

right

P

right

e

i.e

s

and

A

Berlin authorities are increasingly communicating with the help of digital communications

means of communication, such as email. This applies to both communication

between the authorities and citizens as well as for the municipalities

communication between the authorities. The confidentiality of the so transmitted

messages must be ensured. It is particularly important to

reliability if these messages contain sensitive data such as health

or social data are transmitted.

Both the sender and the recipient of electronic

technical and organizational measures must be taken

which are suitable for protecting the confidentiality of the messages transmitted

to guarantee. It is the task of the receiving authorities to

Provide the opportunity to receive messages confidentially. task of

It is up to the sender to use this opportunity. A suitable measure here

for is encryption, especially end-to-end encryption. At

The messages are encrypted before they are sent using end-to-end encryption

secured with a key and only then sent. Before the message

s, it must first be unlocked again using the associated key

be decrypted, which is known only to those authorized to receive it. will be one

encrypted message on the way to the recipient

intercepted or copied, unauthorized third parties can still not get the message

read because they do not have the appropriate key.

Of course, this creates a problem: In order to be able to decrypt the

the receiving station must have the appropriate key. At





the classic, so-called symmetric encryption methods, this is

same key as used for encryption. So in order to

To protect the confidentiality of the content of the message, the key must also

such as the message while maintaining confidentiality to the recipient

recipients are transmitted. The original problem of warranty

the confidentiality of these procedures is only dependent on the confidentiality of the

Transmission of the message on the confidentiality of the transmission of the key

sels postponed.

Fortunately, today there are technical methods that solve this problem.

If you use so-called asymmetric encryption methods, there is instead

of one key two keys. One of these keys is a lock-

development key, the other is a decryption key. Because news

only encrypted and not decrypted with the encryption key

can be used, it is no problem to give this key to other people

split. The confidentiality of the encryption key is not a prerequisite

tion for the confidentiality of the message encrypted with it. Because the

encryption key can be publicly known, it is also called the

public key. However, the decryption key is mandatory

be kept secret, as the transmitted messages are decrypted with him

can become rare. That is why it is also called the decryption key

private key. In order to transmit a message in encrypted form, the

sending body only the encryption key of the recipient

Get recipient, encrypts the message with it and transmits it like this

encrypted message. The recipient decrypts

the message so received by means of her or his own decision-

development key.

If a message is encrypted with an incorrect encryption key

seldom, the recipient cannot de-

encrypt because he or she does not have the right decryption key.

Was the sender intentionally given an encryption key by

foisted on someone who has the appropriate decryption key

sits, he can then decrypt the message that is not intended for him

was. So there has to be a way for the sending body to ensure

use the correct key. A suitable way to solve the problem



solve, is a central body that the sender trusts and the

confirms with a certificate that a key belongs to a recipient

belongs to a recipient. Such a digital key board is called "Public

Key Infrastructure" or PKI for short. A sending body procures itself in this

this method from any source - e.g. from an unprotected sent

E-mail message, from a directory service, from the recipient's website

gers – the encryption key and certificate and checks it. falls that

If the test result is positive, then the body knows that you have the right key

present.

In addition to protecting the confidentiality of a message, the keys

and the certificates issued to them are used to pass messages through

reliably assign digital signatures to their authors and their

to confirm integrity. The consistent use of digital signs

naturen also helps to identify forged documents as such

and to be able to reject them without having to open them for viewing,

so that any malware they may contain will not run

becomes.

To create a digital signature, a checksum36 of the

generated document and then with a matching to the certificate

encrypts the secret key. The public

che key can then be used by the receiving body to

to decrypt the checksum. If the checksum of the document with

the decrypted checksum is identical, the receiving body can

rest assured that the document will come from the specified sending location

originates and has not been modified by any third party. So can by using

of certificates and the associated PKI not only confidentiality, but

the authenticity and integrity of a message are also protected. Both

can be combined depending on requirements, but also individually

be set.

36 This is a short string uniquely identified from the document with a standard

ted process is formed



In Berlin, the IT service center (ITDZ) operates such a PKI for the

Berlin administration. Unfortunately, this service is currently only offered by a few

authorities used. In addition, the certificates issued by the ITDZ follow technical

technically outdated standards that are not suitable for protecting the confidentiality of

to ensure communication. We have therefore pointed out to the ITDZ that

the state PKI - the digital key board operated by the ITDZ - to the aktuell

technical specifications specified by the Federal Office for Information Security (BSI)

adapted to niche requirements.

With the modernized PKI, all authorities must then consistently and comprehensively

be provided with keys so that the confidentiality and the

Integrity of the digital communication of the authorities can be guaranteed.

This applies in particular to communication between the authorities. But

must also give companies and citizens the opportunity

be opened up with the various authorities while maintaining

Communicate confidentiality and integrity digitally in a simple way.

Authorities and citizens need a way to

to communicate with each other digitally in order to maintain confidentiality and integrity

adorn. Encryption and digital signature offer this possibility,

However, there are certified keys. The ITDZ PKI as a digital key board

for the administration must be modernized for their provision and the authorities

must be equipped with keys across the board.

53

2.3 Data protection-compliant use of

windows 10

s

i

x

a

right

P

right

e

i.e

s

and

A

The transition of administration to the current version of Windows 10 is over

essential for reasons of IT security, unless they rely on alternatives37

can or wants to give way. For data protection-compliant use of Windows 10

however, there are some hurdles to overcome. We have been working on

nes test catalog involved, with which the conference of independent data protection

zoversight authorities of the federal and state governments (DSK) to those responsible

Help for the decision about the use of Windows 10.

Much has already been learned about the telemetry functions integrated in Windows 10

professionally reported. Telemetry means "remote measurement" and in Windows 10 means

it that background services, i.e. certain programs that are

NEN and users work invisibly, collect data and analyze it regularly

transmit to Microsoft servers. It is particularly problematic that micro

soft itself determines which data is involved: the definition of

The type and scope of the data to be transmitted is constantly indicated by Microsoft

fits, which makes it difficult to assess the transmission under data protection law.

In addition, Microsoft is part of the control of the telemetry function

Windows 10 also any programs on the users' computers

and user can execute. It is possible, among other things, to import content from the memory of the

computer to Microsoft. Microsoft establishes the collection and

Transmission of this telemetry data with it, troubleshooting and product

wanting to make improvements.

Entities deploying Windows 10 can limit the scope of the transfer of

Set telemetry data only in levels specified by Microsoft. while standing

the most data-saving variant "secure" only users of the "Enterprise" variant

of Windows 10 available, which is not sold to private individuals. U.N-

37

In some German cities, the switch to other operating system software

like Linux tested - and in the case of the city administration of Munich also carried out - in order to

reduce vendor dependency The alternative operating system

Software has the further advantage that the program logic is open and from third parties

checked and, in principle, further developed

54

Chapter 2 Digital administration and justice 2 3 Data protection-compliant use of Windows 10

depending on the set telemetry level, however, micro-

soft determines which data is collected as a result. Although there are various

measures to reduce the amount of data transmitted. those featured there

However, measures do not help in the long term. At the latest with the next update

the settings must be checked and adjusted again if necessary.

In autumn 2019, the DSK therefore developed a test scheme for data protection for win-

dows 10 released as an application note. With the help of this test scheme

those responsible can ensure and document that the data protection

Legal requirements are met at all times when using Windows 10

become. To ensure this, depending on the type of data processed

if necessary, additional technical measures to prevent accidental

allowed transmission to be used.

Such measures must also be taken by the Berlin authorities,

which replace the previously used Windows 7 with Windows 10. Since Microsoft

regular support for Windows 7 ended on January 14, 2020, Win-

dows 7 can only be used in compliance with data protection from this point in time,

if additional support services purchased for a fee are used

be taken. The ITDZ has a concept for the so-called Berlin PC as an inventory

part of the ICT workplace, which in the future will be used almost everywhere in administration

tion is to be used, which also includes the safety and

should meet data protection requirements.

We have discussed this concept with the ITDZ and rate it as fundamental

Suitable for using Windows 10 in administration in compliance with data protection.

The ITDZ achieves this by providing the specialist users required by the administration

be operated without internet access and it is available on the respective work

platzcomputer also has a separate environment for internet use.

If the concept is implemented consistently, the requirements of the

DSK are complied with. We will continue to support and review the project

whether the concept is implemented in the administration in compliance with data protection.

Since by far not all Berlin authorities use the Berlin PC and the

Windows 10 is also used every day in non-public areas, it will

The topic of telemetry data will probably keep us busy for some time.

55

The use of Windows 10 is not permitted under data protection law as long as not

technical and organizational measures are used to avoid personal

son-related data from the use of the software or even from the content

ten documents submitted to Microsoft for use for its purposes

become. A test scheme from the German supervisory authorities helps those responsible

verbal, to ensure data protection-compliant use.

2.4 Malware infestation at the Superior Court

s

i

x

a

right

P

right

e

i.e

s

and

A

A malware infestation at the Superior Court has serious weaknesses

protection of sensitive data processed by this court. We

have had the safety measures explained to us, which on the one hand prevent

and on the other hand taken after the infection to cope with the problems

fen have been and have made recommendations for further troubleshooting.

We also had corresponding discussions in two universities, which are in a similar way

way were affected.

In September, the Court of Appeal was informed by the ITDZ that

a computer from the Court of Appeal's network would try to

reach servers used by criminals to send commands and software

ware to be sent to malware running on the computer. A da-

An investigation carried out immediately uncovered a number of computers

Infection with Emotet malware. The locally installed on the computers

virus scanners had not noticed the infection.

Emotet was originally developed as a banking Trojan. He is currently in

used in combination with other malware components to

and harm authorities and extort funds from them. This

is often done by thoroughly encrypting all data that the malware

goods can be obtained. Those affected should then pay a “ransom”

before they – at best – receive a key with which they can retrieve the data

can decode. They cannot rely on that. The first infection

through such software is often done through a manipulated file that

sent to other people by email. To this file and the one that accompanies it

To make e-mail appear as believable as possible, the software uses templates,



which they communicate to a communication partner of the intended victim in a

infestation steals. Therefore, when infected with Emotet, it is not just with one

loss of access to certain data, but also with their disclosure

unauthorized third parties.

Based on the information provided by the ITDZ, the internet access of the

Superior Court deactivated, a little later the Superior Court also from Berlin

State network separated and almost the entire information technology of the court

shut down. These measures were taken before the malware data

could encrypt. However, it is unclear how the initial infection took place

took place and what steps the malware subsequently took

men has. It is therefore not certain which and how much data has been lost.

From the above reasons, however, it can be assumed that Emotet from the infected

ten computers has at least forwarded e-mail messages.

Since the Court of Appeal does not have a system with which it can reliably

Malware-free old systems and the data stored with them

ten, it decided to rebuild its entire network.

In this context, most are required by the Court of Appeal

Services relocated to ITDZ. The documents originally stored in the old system

remain isolated and are only available as an archive for inspection

tion This consistent approach stands in positive contrast to the clear

more limited measures, which include those also affected by the virus

universities have taken. These checked some, but by no means all

Locations where the malware could have nested and saw

no reason to make structural changes.

The reorganization of the information technology of the higher court is this the

Possibility also open up the structure of networks and applications better

set up than was previously the case. So the new system should have a

sharp separation between the internal for the different specialist procedures

components used and the external components for internet use and

have email communication. Only by sealing off those connected to the internet

net connected components and a division of the network into separate,

mutually separate areas it is possible to prevent an infection from spreading

spread to all information technology.

57

Another important step consists in equipping the judges

Judges of the court with mobile service devices that allow them to work in their

re home environment allow. So far, this homework - on legal

public basis – with private devices. As a result, data between

uncontrolled from these private devices and official information technology

exchanged, primarily via USB sticks or by sending them by e-mail. The

first form of data exchange, the court has to immediately after the incident

right locked. But the second form, which is still permitted, also offers malicious software

ware a way into the inner web of the court.

However, the understandable desire to work from home can also be

threat to data security are met in such a way that official data

Do not leave the specially protected internal area. have to

the laptops intended for working from home can be configured in such a way that they

can only connect to the internal network of the court and the

used office programs all processed documents exclusively on server

save vern of court. The configuration of the laptops must ensure

that the security measures used cannot be circumvented.

Lessons from the incident are not only for the Court of Appeal, but for everyone

authorities and public bodies of the State of Berlin. These differ-

which are reflected in measures to prevent infection and those that

available when a malware infection occurs.

For the state authorities, the implementation of the e-government

puts Berlin (EGovG Bln) to the centralization of data processing

contribute to future software running in an environment in which

security can be guaranteed with bundled expertise. the high

schools who will continue to operate their information technology themselves,

should expand their data centers to such environments and not just them

Administration, but also the processing of all sensitive personal data

Relocate data to these secure environments for research purposes, to the extent

this is possible without restricting the freedom of research.

All public bodies will provide additional advice in particular on safe

administrative practice, the design of networks and risk analysis

necessitate. There needs to be a centrally provided service that has the capabilities

detect potential risks in files beyond the usual anti-virus software

which the authorities can reach from external sources, in particular via e-mail

chen. And in the event that an infection with malware nevertheless occurs,

the public authorities require a guideline and a computer emergency

fall team that will be at your side quickly.

The mixing of the processing of private and business

data, both in the business environment and when working from home. who in

Home office works, requires a company-provided device. We recommend that

Legislators, the regulation of § 23 of the law on the execution of the court

constitutional law (AGGVG), the judges and

public prosecutors the use of private information

technical devices allowed.

The security of the systems used is a prerequisite for data protection

former official activity. Therefore, it is imperative that the architecture

the information technology used with regard to protection against

to design software. Private and business must be strictly separated. With

decisive, proactive action must prevent further infections with harmful

countered by software and infections that have nevertheless occurred must

closed, contained and eliminated competently and quickly.

## 2.5 Cooperation with official data protection officers of the courts and state legal offices

For almost ten years we have held regular working meetings with the official

chen data protection officers of all Berlin courts and public prosecutors

through. Here we discuss current data protection problems and questions

from the practical work of the data protection officer.

There have been regular meetings between our agency and the

official data protection officer of the district courts. We continue this tradition

59

A

and

s

i.e

e

right

P

right

a

x

i

s

since 2011 on a larger scale. The reason for this was one of us

Conducted seminar on "Data protection in the judiciary" in the Judicial Academy

demia in Königs Wusterhausen38. At this event, many participants

the desire for a regular meeting to discuss

tion of data protection issues and the exchange of experiences.

The official data protection officers of the courts and public prosecutors

Most of them have legal training and lead in these rounds

to have very qualified and committed discussions with us-

the data protection issues.

Recurring topics are those related to the implementation of data protection

technically necessary organizational measures in the courts and

to proceed on the admissibility of the use of court and administrative files

cross-border purposes. From the colleagues in the houses

In addition, regular questions about employee data protection are sent to the international

approached a data protection officer, who we did at our work meetings

discuss together. In addition, the role, the tasks and the

Rights of the official data protection officers discussed.

The work of the official data protection officer is therefore particularly important

so important because these data processing processes and their weak points

know each other very well on site. From this knowledge we can

work and exchange benefit, and in turn the internal data protection

assisting those responsible in fulfilling their duties.

38 Central training center for the judiciary of the state of Brandenburg and for the higher

ren service of the state of Berlin



Chapter 2 Digital administration and justice 3 1 Threatening letters to the left scene with data from police databases

Home and Sports

3

3.1 threatening letters to the left scene with data from

police databases

The threatening letters to the left scene kept us busy in 2019.

various institutions classified as politically left were in December

2017 letters with personal data (including names and photos) and a

text that is threatening to those affected. The photos used and

Information indicated that they were obtained from police databases

came from. Therefore, immediately after this case became known, we

extensive tests carried out and a lengthy correspondence with the

police and the public prosecutor's office in Berlin.39

A

and

s

i.e

e

right

P

right

a

x

i

s

After we received notification in October 2018 that a police

official of the State of Berlin as the author of the threatening letters and against him

a penalty order had already been issued, we contacted the police again

fluent. A further examination was necessary as we had no information on this

templates, where the personal data contained in the letters sent came from

Data specifically came from, how the author was able to get this data and

whether he had obtained it himself or whether it was in the ranks of the police

internal or accomplices. A central question was to what extent the perpetrator

had the technical authorization to access the data of the persons concerned

to access and download (image) files from the police databases

and store externally. In contrast to the criminal sanctioning of

specific incident by the judiciary, we wanted to identify possible weaknesses

in the technical and organizational measures for the use of the data

bank systems of the police in order to recommend suitable counter-

measures to prevent such incidents in the future as far as possible.

To clarify the open points, we have received several written

taken by the police. On the other hand, we have log data from

39 See the detailed description in the 2018 Annual Report, p. 55 et seq



police database POLIKS in the period relevant to the offense

evaluates in order to check the access to the data of the persons concerned.

Unfortunately, it could not be clearly explained how the author

the threatening letters to the personal data of those affected, in particular

the image files. It is conceivable that at an earlier point in time he

had permissions to download and store POLIKS content.

However, it cannot be ruled out that the data may be accessed by other authorized persons

were made available, even if the pro-

record data no clear indications of specific accomplices

have revealed.

Admittedly, misuse of the police databases by individual police

license employees cannot be completely prevented. The police are though

encouraged to take appropriate technical and organizational measures

access the protection of personal data in the databases

ensure the best possible.40

3.2 Control of the police information

systems POLICIES

In particular, the difficulties in identifying the perpetrator, the threatening letters

to the left scene with personal data from police databases

had sent,41 were reason for us to fundamentally limit data processing in political

licensed information system POLIKS as part of an on-site inspection

check over.

The audit focused on checking compliance with the POLIKS

applicable review and erasure periods and investigating the possibilities of

employees of the police to inspect POLIKS.

40 See 3 2

41 See 3 1





We found that the police have been using automated deletion since June 2013

switched off completely in POLIKS. The reason for this was an instruction from

Senate Department for the Interior and Sport, no files and files "with references

on right-wing extremism” to destroy or delete it to ensure

that the investigative committee of the German Bundestag on the so-called "NSU"

access to all relevant data and documents.42 This directive

has been renewed annually since then. It was also replaced by a second extinguishing

ratorium on the occasion of the attack on Breitscheidplatz in December 2016

added.43 The police should ensure that no files or data are

be deleted or erased "that are or are connected with the attack

hen”, since the appointment of a committee of inquiry was expected

became. In the meantime, appropriate investigative committees have been set up

the Berlin House of Representatives and the German Bundestag. Also

the Breitscheidplatz extinguishing moratorium has been extended annually since then. One

Since then, data has only been deleted manually by the police on the basis of

specific inquiries or deletion requests for specific processes.

Failure to delete personal data in POLIKS is legal

contrary to the extent that storage is not required to fulfill the responsibility of the

Police lying tasks or for purposes of the committees of inquiry to

so-called "NSU" and the Breitscheidplatz assassination is required.44

Those that are ready for deletion, but are continuously stored due to the deletion moratorium

At least up to the time of our examination, data were not

limited grip. The police only started moving in September 2019

of this data in a protected area set up for this purpose.

This lack of access restriction was also illegal. As far as the data

could continue to be stored due to the deletion moratoria, they would have

must be withdrawn from general access via POLIKS.45 This is the only way

guarantees that those authorized to use POLIKS exclusively

42 NSU deletion moratorium

43 Solicited Breitscheidplatz extinguishing moratorium

44 See §§ 48 Para. 2 Sentence 1 No. 1; 42 para. 1 sentence 1 General security and order

tion law (ASOG)

45 See Section 32 (1) No. 5, Section 50 (3) Sentence 1 No. 5 of the Berlin Data Protection Act (BlnDSG)



the personal data covered by their access authorization

have.46

Furthermore, we found during our examination that the police within the framework of the

Access control at POLIKS also does not carry out any suitable random sampling

leads. The controls currently being carried out by the police are being

not from an organizationally and thematically separate and thus independent

carried out at a certain point, which weakens the validity of the results.

In addition, the controls are obviously not effective, because so far in no

recent case, irregularities or unauthorized access have been detected

are, although our authority regularly makes unauthorized retrievals in POLIKS

Police employees are reported and also punished by us. For this reason

and due to the large number of retrievals that take place in POLIKS every day, there is a high

dark figure to be feared.

Particularly problematic was the finding that the system setting of

POLIKS enables data retrieval without giving specific reasons. at the domestic

Person searches possible within the database can in part be very general

my query reasons such as "processing" or "other reason"

to be chosen. For the necessary addition to the selected query

Basically, it is even sufficient to enter any three characters such as "xxx" in a free text field.

to enter A tracing and verification of the legality of queries

thus becomes impossible. General keywords contain by themselves

no statement about the specific reason for the query and are therefore not revised

onssure. Only formally fillable free text fields represent a subsequent transfer

verifiability not sure.

The current system of people tracing is unlawful.47 The law writes

stipulates that queries from POLIKS are also logged with regard to their justification

Need to become. The legislative aim is to guarantee the subsequent

Liability to verify the authorization of the queries by the data subjects,

by those responsible as part of an internal audit and by the people of Berlin

46 So called access control

47 See Section 62 Paragraph 1 No. 3, Paragraph 2 BlnDSG

Commissioner for data protection and freedom of information. The logging is in-

as far as elementary for the enforcement of data subject rights and last but not least

for the fulfillment of the legal task also of our authority, the application

to monitor and enforce data protection regulations.48

We complained to the police about the identified violations and

legal adjustments required.

POLIKS is one of the most important electronic work tools for the police and

accordingly holds a large amount of personal data, some of which is very sensitive.

It is therefore extremely important that the police check the admissibility of the

data storage and access to this system are closely

quickly and effectively controlled and allows for retrospective reviews.

3.3 Delayed response to information

inquiries by the police

We received more and more complaints about the fact that the police

Requests for information and requests for deletion have not yet been received, even after a long wait

had been answered.

We asked the police for their opinion on this and pointed out that

that the response to the above-mentioned requests will be received regularly without delay

should follow. The police must take the necessary organizational measures

took meet. We were then informed that the average

Processing time for applications to the police at the moment due to the enormous

given number of applications takes about seven months. With the processing are regular

moderately employs three people and two assistants.

A

and

s

i.e

e

right

P

right

a

x

i

s

Our own letters to the police authorities are often only delayed

answered. Regular reminders are required, which is an unnecessary one

48 See Section 11 Paragraph 1 Sentence 1 No. 1 BlnDSG



meant more work for us. This also means that the processing

delay reporting complaints to us.

In a conversation with the chief of police, we pointed out the problems

matic. She justified the long processing time with staff shortages

senior However, you will have it checked whether other employees are responsible for the fulfillment

of these tasks could be used. We recommend at least a preliminary

Temporary personnel reinforcement of the area to process the previous ones

requests.

The right to information about the storage of personal data and

the deletion of such data is part of the rights of those affected

are a core component of the right to informational self-determination. To the

The procedural procedure must be designed efficiently to ensure these rights

and possibly also more staff to process applications.

3.4 fine procedure: file number visible

in the address field

For all automatically created letters from the fine, the police authorities

money office in addition to the address and the file number of the respective fine

procedure in the visible address field of the letters to those affected. about this

one of those affected complained to us. We have the reason for the complaint

taken to examine this addressing practice of the police.

During the investigation, the police informed us that the playback of the

tenzeichen in the address window is necessary to the official delivery of

Writing to request the proper completion of a postal delivery certificate

possible. Only by matching the file number on the letter

envelope with the file number on the postal delivery document

would it be possible to prove that the specific document was also granted

was placed. We agree with this assessment.

and

A

Chapter 3 Internal affairs and sport 3 4 fine procedure: file number visible in the address field

However, only certain letters, in particular the penitentiary

notice of payment as part of fine proceedings, by means of a postal delivery

certificate officially delivered. For all other automatically created letters

such as hearings, warnings and reminders, the announcement takes place

immediately by dropping it in the mailbox. In these cases, too, one believed oneself

authorized to print the file number in the address field at the police station, because one

thus have a sorting criterion for undeliverable returned mail. Added

come that from the specification of the file number no gain in knowledge regarding

that a concrete act is possible and that one can also use other means (online,

by telephone or on site) no information solely through knowledge of the respective

ten sign.

However, the question of the admissibility of data processing is not decisive

dend whether third parties can thereby obtain further information. Rather is

decisive whether the printing of a file number in the address field of letters

required for the police. With the file number of a fine procedure

is it just in connection with an address a personal

genes date, the specification of which in the address field of a letter for normal delivery

It is not necessary to send a letter by post. mail returns

can also be processed without this sorting criterion, since the identification

of the persons concerned via the address data and, in cases of doubt, the person concerned

Envelope can also be opened.

We have therefore asked the police to stop the existing practice and

adjust the templates. The police then said a change of address

planning practice.

Only in the case of notices of fines that are officially delivered may the file reference

be visible in the address field of letters.

67

3.5 Data processing in the population register:

Mix-ups & more

s

i

x

a

right

P

right

e

i.e

s

and

A

Registration authorities49 are legally obliged to work within their area of responsibility

to register the persons residing in order to determine their identity and residence

to be able to provide and prove. To do this, they keep a register of residents

certain data are entered that were collected from the data subject,

transmitted by public authorities or officially known in any other way

become. Section 3 of the Federal Registration Act (BMG) determines which personal

no data may be stored in the population register. Further dates or

Wise may only be stored under certain conditions. The

Registration authorities are also authorized to provide information from the registration register
the execution of tasks of other authorities or other public
to cooperate and to transmit data. Personal data may
however, will only be processed if this is regulated by law.50
In 2019, we received numerous inquiries and complaints about the
data processing by the registration authorities. As part of the investigation of complaints
has become visible how important it is to deal carefully with the context
with the storage and retrieval of the data contained in the population register.
What effects it can have if errors occur here should be
are presented below using a few selected cases.
One of those affected told us that he was contacted by various official bodies
received letters in which he was written about as the owner of a motor vehicle
ben. These included a notice from the Berlin Motor Vehicle Registration Office
authority, a letter on a seizure and confiscation order
main customs office in Berlin and a reminder regarding the due date of a vehicle
Tax of the main customs office in Frankfurt/Oder. The person concerned explained to us afterwards
enforceable that he is not the correct addressee of this letter
because he had neither a driving license nor a motor vehicle. With us
49 In Berlin, these are the district offices and the state office for civil and regulatory
opportunities (LABO) - see § 1 para. 1 BlnAGBMG
50 See the regulations in § 2 BMG for the aforementioned tasks and powers


Seren investigations turned out that the letters due to a
mistaken identity had been sent to the complainant and
actually concerned a person with both the same first and last name

than was born on the same day and in the same city. only in

the two other first names of the complainant differed from his

Data from the actual owner of the motor vehicle. A government agency had one

Initiated a civil register query to find out the new address of the person with the same name

to find out. Since such a population register query as information on

Personal identification usually only a first name plus the last name and

the date of birth is entered, the querying agency received the address

our complainant. On the two other first names, on which the two

the persons should have been distinguished, was apparently not respected.

In another case, a person received information about the issuance of a

nes certificate of good conduct, although she had not applied for one. The responsible authority

Circumstances admitted that this was due to a mistaken identity

was. A person of the same name had in the consultation hours of a mobile citizen

office to issue a certificate of good conduct. Due to technical

problems and the numerous waiting customers decided

the clerk to initially only record the application data for this, the

Administrative fees to levy and the application afterwards in stationary

to process citizenship. However, when accepting the application, he forgot

date of birth of the applicant. In the later processing

processing of the application, the search for the applicant was carried out via

the search mask of the editing software only with the prefix and family

names. It was overlooked that in Berlin two people with this name

are reported, but differ with regard to the date of birth.

For the application processing, the wrong data was inadvertently taken from the

Register selected.

Finally, two of those affected contacted us, who repeatedly wrote about the

had received from the police, with whom she was the guardian of an underage refugee

have been written to. Although they had the guardianship of a

taken over by young people who had fled, but not for the

minors addressed in this letter. When asked, the police said

inform those affected that the data for the police summons letter

69

were obtained from the population register. So it had to be assumed

that incorrect data was stored in the population register. It is stipulated by law

that in the dataset of minor children also certain personal data

Data of the legal representatives are to be entered.51 Information on this will be provided

regularly directly with the persons concerned, e.g. by filling out the registration form

sham, raised. In addition, the registration authorities can

also due to legally mandated data transfers from other

received from public authorities or through investigations ex officio

raise. As part of our audit, we found out which district office

the two complainants as legal guardians in the dataset of the person concerned

had saved underage refugees. According to the entry, the basis was

the decision of a district court in the population register, which, however, is no longer

was to be found. Due to the lack of documents, it was not possible to conclude

need to clarify what had led to the registration of false guardianship.

Since the youth welfare office is the district office, however, the actual legal guardians

communicated, must be due to an oversight on the part of the responsible district office employee

be assumed when entering the population register.

In practice, people with the same name are not uncommon. To per-

to avoid confusion when retrieving data from the population register

avoid, the official body must provide sufficient information when searching for a person

Information to identify the data subject entered as search characteristics

ben. Unequivocal identification is regularly possible, if at least

the surname, if applicable the maiden name, the first name or names, the

date of birth and last known address. Even with care

of the population register data, the registering body must proceed carefully in order to

to ensure that only correct data on the respective persons is

be saved.

51 § 3 para. 1 no. 9 BMG



3.6 Blocking information in the population register due to

change of first name or

gender

A

and

s

i.e

e

right

P

right

a

x

i

s

As part of a complaints procedure, a citizen informed us about

Difficulties in connection with the establishment of an information block

in the registration register. During an appointment at the Citizens Registration Office, the person concerned had

an application to set up a blocking of information due to the change in the

named according to § 1 Transsexual Act (TSG). The clerk

of the Citizens' Registration Office mistakenly assumed that he was blocked from providing information because of a

Danger to life, health, personal freedom or similar things worthy of protection

Interests52 wanted to apply and gave him the corresponding application.

Only as part of the further processing of the application by the state office

for civil and regulatory affairs (LABO) and after we adhere to the

LABO, it became clear that the person concerned actually had a blocked

correction of his data set because of a change of first name.53 For this

no application would have been necessary at all, because those affected have in

In these cases, you are entitled to an automatic blocking of information. The LABO checked

then the data records contained in the population register for the person concerned and

informed us that the complainant was already due to a

another district office actually already carried out a name change

information ban had been set up.

This case has shown us that the procedure for setting up a transmission

Registration ban in the population register due to a change of first name or

Apparently not all of those affected and citizens' offices

tern is known, so that the misunderstanding described or not

proper processing of the citizens' concerns could come.

Persons who do not choose their birth sex but a different sex

badly feel that they belong, have the right to appear in a judicial

change their first name and their gender characteristic (marital status) from female

52 See Section 51 (1) BMG

53 See Section 51 (5) BMG in conjunction with the Personal Status Act (PStG), TSG



male or vice versa. The TSG sees two procedures

with different legal effects. On the one hand, this concerns the

change of the person concerned without changing the date of birth and registration

deregister registered gender (§ 1 TSG) and on the other hand the

judicial determination of a change in gender (§ 8 TSG).

If the court decision is final, then at the time of

First name or gender without the consent of the decision

Applicant are not disclosed or explored in principle.54

The registration authority changes the first name or gender in the

Civil register only if, by submitting a court order, the

respective change has been proven or the registry office has

announced a change in status. For making the record lock

no separate application by the person concerned is necessary in the population register.

Rather, the blocking of information is registered ex officio if the notification

de authority a change of first name or gender in the population register

makes. The data record with the former first name or gender is also

automatically closed in the specialized procedure and a new data set is created

builds.55

Affected people already have one after the first name change according to § 1 TSG

The right to be addressed and addressed according to their new understanding of their role

to be written to.56 To ensure this, the relevant

to make changes to the population register data without delay. in the frame

With information from the population register, however, there is a fundamental risk

that by transmitting the former first name also the fact of the trans-

sexual history becomes known. Therefore, the registration authority has ex officio

to enter in the population register because of an information ban. The district offices

or their responsible bodies should familiarize themselves with this lesser-known

Familiarize yourself with the ban on coming in the population register, so that citizens

Citizens can be given appropriate advice.

54 Section 5 (1) TSG and Section 10 (2) TSG

55 See No. 3 1 1 3 in conjunction with No. 3 1 1 1 General administrative regulation for implementation

of the Federal Registration Act (BMGVwV)

56 BVerfG, decision of August 15, 1996 – 2 BvR 1833/959





## 3.7 Police Confidentiality Agreement for MPs

We were told about it by a member of the Berlin House of Representatives

informed that the police authority of him as part of his regular

shadowing, but also in regular conversations, which he in his capacity

as a Member of Parliament, the submission of a written "commitment

declaration to maintain data secrecy (“non-disclosure declaration”)

in connection with the implementation of office visits, hospital

tion and operational support”. We were asked to check in-

how far through the obligation to submit the declaration the constitutional

tasks of the deputy are limited.

A

and

s

i.e

e

right

P

right

a

x

i

s

Obtaining a non-disclosure obligation in advance of job shadowing

with authorities is common practice and represents an important measure to

of official secrets. In general, it makes sense to keep such a

declaration of security not only to refer to official secrets, but to them

also extend to personal data for the purpose of data protection.

Service secrets and personal data can have the same content

concern (e.g. patient data within the framework of medical confidentiality),

are, however, usually different pieces of information and therefore different from each other

separate. The use of a non-disclosure agreement in the context of hospital

ments with authorities, which also includes the protection of personal data, the

are taken note of by the respective trainees is therefore fundamental

to be endorsed and recommended.

When asked about the legality of a non-disclosure agreement, the

is demanded by members of parliament, both data protection law and (national

des) constitutional aspects touched.

It is generally recognized that Art. 45 Para. 2 of the Berlin Constitution (VvB)

a constitutional right to information from members of parliament

public institutions of the country can be derived. The standardized

However, MPs' right of inspection is not unlimited. The insight-

The inclusion of a Member of Parliament in the files can be rejected if predominantly

73

This is mandatory if there are public or private interests in maintaining secrecy

require.57

Protected public interests include the protection of law enforcement

and preventive police investigations; overriding private interests

are in particular those of the protection of personal data. Are at the

Access to personal data of special categories, such as health

data, touches, Art. 45 VvB conforms to European law in the light of Art. 9 DS-GVO

about the admissibility of the processing of such sensitive data

the result that in this case is mandatory by an overriding private

interest and a requirement of secrecy is to be assumed.

It can thus be stated that a non-disclosure agreement that it

MEPs are generally prohibited from processing personal data,

would disproportionately restrict MEPs' right to information

and would therefore be inadmissible. A statement stating that disclosure of

to refrain from sending personal data of special categories58 to third parties and

not to publish any of this data, on the other hand, would be permissible. This also applies to

a statement prohibiting MPs from taking pictures, private

letters and telephone numbers of individuals to third parties

or to publish.

We have submitted this opinion to the Senate Department for the Interior and Sport in a

communicated with a written statement. The text of the statement, which initially

contained the obligation to stop any processing of personal data (as well as

operational and/or criminal-tactical information) was

changed afterwards.

Against the use of the revised version of the "Obligation to

Maintaining official secrecy (“non-disclosure agreement”) in connection

menhang with the implementation of office visits, job shadowing and

Operational accompaniment of the Berlin police" also for members of the

tenhauses von Berlin does not have any basic data protection laws

57 Article 45 paragraph 2 sentence 2 VvB

58

i S v Art 9 DS-GVO

74

Chapter 3 Interior and Sport 3 8 Consent to "mini-championships" in table tennis

To ponder. This also applies to the regulation that a transfer of personal

related data (especially in the case of special categories of personal

drawn data) to third parties as fundamentally inadmissible. However, should

the term "third party" is defined in more detail here. To the extent that the regulation

orderly would be prevented from gaining insights that they

particularly in the context of their parliamentary activities

People within the parliamentary space (e.g. other MPs)

passed on, their function as a control body of the executive could be inappropriate

be casually restricted.

3.8 Consent for "mini-championships"

in table tennis

The German Table Tennis Federation e. V. organizes for the purpose of membership

winning the so-called mini-championships, in which children up to 12 years without

prior registration can participate. The children could give their consent

consent to the processing of the data so that the next

learn about the locations and dates of the championships. There was a complaint about this

with us.

A

and

s

i.e

e

right

P

right

a

x

i

s

In principle, data processing cannot be based on the consent59 of children

otherwise be supported. In children of the age group in question, it is absent

it regularly falls short of the ability to give informed consent. Then

such consent requires that the children accept the consequences of the

understand how their data is used and are also able to

exercise rights independently.

Under certain conditions, however, the processing of the data can be

based on the GDPR as the legal basis60. Accordingly, it would be permissible

if they are necessary to protect the legitimate interests of those responsible

is, “unless the interests or fundamental rights and freedoms of the persons concerned

59 Art 6 Para 1 lit a, Art 7 GDPR

60 Art 6 Para 1 lit f GDPR

person who require the protection of personal data prevail, in particular

especially when the data subject is a child".

The recruitment of members through the events of championships without

Prior registration represents a legitimate interest of the Table Tennis Association.

The collection and storage of the data is also necessary because the children

one does not always know the next event dates and locations, for

whose only the data of the children are recorded, which are for the next

qualified for the round. Although the European legislator61 points out that

that, particularly in the case of children, there is a predominance of their interests

going out to eat. However, an examination in individual cases can result in

that the balance of interests is in favor of the organizer. This is off-

depending on the specific design and the protective measures taken

men. In this case, the children should only be sent once by post and exclusively to

written notification of the date and place of the event. About it

In addition, the parents of the children should have the right to object to data processing

be granted. After the cover letter and the implementation of the next

In addition, the data should be deleted. Therefore is merely of minor

to assume impairments.

Children under the age of 12 cannot regularly provide informed consent

to grant data processing, as they only accept the consequences of their consent

difficult to estimate. A case-by-case weighing of interests can

however, lead to the result that data processing in such cases

is nevertheless permissible.

61 Art 6 Para 1 lit f last HS DS-GVO

Chapter 3 Internal Affairs and Sport 3 9 Publication of contact details on a sports portal

3.9 Disclosure of Contact Information

a sports portal

The Table Tennis Association Berlin-Brandenburg e. V. published private con-

clock data of persons elected in functions and team leaders

(mobile phone number and e-mail address) in the publicly accessible area

their website. This should limit communication related to table

enable tennis tournaments. The data were collected from a club of the federation

set on the platform.

A

and

s

i.e

e

right

P

right

a

x

i

s

The table tennis association uses for the organization of association games between

member associations a website. This portal serves primarily as a communi-

cation platform and to publish tournament results. It has a

publicly accessible area and a password-protected member

rich.

In the present case, both the association that manages the platform

provides, as well as the club itself, which the data in the section "club information"

made publicly available.

If the data subjects have not given their consent, publication

Disclosure of the private contact details of club members only lawful,

if they are to protect the legitimate interests of the person responsible or

of a third party is required and the fundamental rights and freedoms of the

met not outweigh62. While providing the ability to communicate

in connection with the tournaments organized by the Table Tennis Association

legitimate interest. However, the publication of the private con-

Clock data in the publicly accessible area is not required for this. To that extent

a less drastic means is available. The contact details must

can only be viewed by participants in the tournament. Since the

Table Tennis Association also a closed member area of the portal to

available, it would be possible for the club and the table tennis association

wesen to publish the data deemed necessary there.

62 Art 6 Para 1 lit f GDPR

77

The publication of private contact data in the publicly accessible area

a website of a sports association is usually not necessary and

with unlawful. It is sufficient if such contact information is in a suitable

word-protected member area.

78

Chapter 3 Interior and Sport 4 1 Jelbi" – the BVG mobility app

4 Transport and Tourism

4.1

Jelbi” – the BVG mobility app

The BVG is increasingly pursuing the goal of expanding its own offerings as well

transport companies in the sense of “intermodal transport” via their own

to offer apps. Offers that are different are referred to as intermodal

Combine and match modes of transport to get the one you want

route of the user to develop the best possible connection

wrap. This can mean, for example, that a route that

interested parties have always traveled by car in the past, they now have an alternative

in a combination of local public transport and rental bicycles

will beat, since this is an even faster, more ecological or even cost-saving

viable alternative would be.

A

and

s

i.e

e

right

P

right

a

x

i

s

Through such offers, various means of transportation should make sense

be linked together. In addition to other providers who offer such services

for a long time, the BVG has now also proposed a

published its own app called "Jelbi" a few months ago, which, in addition to driving

also offers bookings and payment for travel options.

The BVG's approach to promoting intermodal transport is fundamental

quite welcome. However, with such offers also very

a lot of personal data to63, which is treated in accordance with data protection

must. This was largely disregarded during the development of the "Jelbi" app.

tet. The application was developed by the BVG rather and the public

presented without the Berlin Commissioner for Data Protection and Information

Onsfreiheit informed in advance about the project and asked for an opinion

would have been.

63 U a Movement data, means of transport used, address data, possession of a driving license and

payment details



Unfortunately, we were only able to check the offer after we left the

press learned about the project. Even with a cursory review

of the offer, we identified various data protection violations. That's how they became

Movement data of the users initially only insufficiently anonymized, where

created by customizable movement profiles. To complain about was

In addition, there is insufficient transparency towards customers

with regard to the third-party companies commissioned as part of the "Jelbi" offer

men. Even for small amounts, creditworthiness information has already been

commissioned payment service provider, unless the user has previously

were already known. This even in cases where a credit check has already been carried out

therefore would not have been necessary because - e.g. when paying with a credit

ditkarte - the payment is already guaranteed by the card-issuing institution.

It was further noted that when looking for suitable means of transport

sometimes personal data of the user is then passed on

ben when only traffic information was desired and still

no binding booking. When booking, the detailed information was missing, which

Master data is passed on to the respective mobility partner. Provided

a driving license was required, e.g. when booking rental cars, must

asked the user to confirm the authenticity of the information contained in the driver's license

Personal data in addition to your driver's license, your identity card and a

Submit video or image to service provider Veriff for verification.

Overall, it has been shown that the BVG still has various data protection problems

had to lift and the "Jelbi" system was not considered at the time of our review

could be considered data protection compliant.

We have therefore instructed the BVG to remedy the problems mentioned and

to ensure a data protection-friendly option for using the offer

carry. The BVG then began subjecting its apps to a data protection

subject to legal review. In addition, for the time being, the spoke

Apart from the processing of movement data at “Jelbi” until the BVG has a mature

has developed an anonymization concept.



In terms of increased convenience for customers and

Promotion of sustainable and environmentally friendly mobility are intermodal

Transport offers like “Jelbi” are to be welcomed. However, here should always

the expected benefit of the technology with the possible data protection

legal risks are weighed. In addition to data security and

Data protection is also sufficient transparency towards customers

important to employees and customers so that they are always fully informed

which data may be collected and which bodies have access to their data

have. Only in this way can the right to informational self-determination of the user

can also be effectively implemented. We will further development

therefore observe carefully with "Jelbi".

4.2 A complete database? – The free one

BVG student ticket

The Berlin Senate has decided to offer a so-called free

to introduce a special student ticket for local public transport. The application

of the ticket is only possible online with the BVG using a form

to which a passport photo of each student must also be uploaded.

We have therefore received several complaints and general inquiries about this

procedure and the storage of the data at the BVG. A worry

was that the BVG is building a database of all students.

A

and

s

i.e

e

right

P

right

a

x

i

s

Reduced monthly and annual tickets for schoolchildren were

already sold by subscription. They were subsidized by the state of Berlin

tioned, which is why they are regularly significantly cheaper than regular subscriptions

were. The Senate has now decided to enter for all students

offer a free annual ticket, which is still a subscription

ment, not simply free travel for all schoolgirls

and students, for which, for example, the student ID would suffice as proof.

The only difference from the previous situation is that the families

now receive a 100% subsidy from the state of Berlin for these tickets

received instead of the previous partial subsidization. The subscription model

was chosen because on the one hand the BVG in this way through



the free school tickets with the state of Berlin

account and the Senate in return can understand, among other things, how many people

take advantage of this offer.

The free student ticket is used by all Berlin local transport companies,

i.e. the S-Bahn, the Verkehrsverbund Berlin-Brandenburg (VBB) and the BVG,

issued. Parents, guardians or students

conclude a subscription contract with one of these local transport companies

men. The BVG collects the data for this contract and stores it during the

Term of subscription in one database along with other active ones

Subscription Contracts. If the contract is not continued, the data in

moved to a separate and restricted system. In this system

the data will be stored for as long as this is required by commercial and tax law

is mandatory.

The BVG, like the other transport companies, is opposed to the

State of Berlin accountable. She must therefore prove how many

certificates were issued to receive the compensation payments and this

to be able to prove in detail in the case of an audit. accordingly

Accordingly, the BVG is obliged to collect and record data from all persons

store who subscribe to a free student ticket.

In principle, there are no data protection concerns. We

However, we are currently checking to what extent there is still room for improvement in individual

possible, e.g. whether all the required data is actually

need to be collected, such as the date of birth of legal guardians.

In addition, the BVG has to adjust the storage periods in detail to the absolute emergency

reduce agile; here too we are still in the process of testing. sample

Unfortunately, the photos for the ticket are currently only deleted after eight weeks,

to reissue a ticket in case you lose it

can. A significant reduction in the deadline is conceivable here. Another point

is the requirement to upload a copy of the student ID card in order to

additional authorization for the student ticket. Here the BVG checks whether

it must keep the copies for an audit by the state or

whether these are deleted immediately after verification of authorization

can. The other data collected, including the e-mail address of the person who



ordered a ticket online are part of the collection and storage obligation

Documents.

However, there was also some criticism that the applications were exclusively online

line can be placed. It is not mandatory for the BVG

to also accept applications by non-electronic means. Since the

BVG had to adjust to a large number of new applications at short notice

the exclusively electronic application procedure in this situation perhaps

still been justifiable. In accordance with the obligation of the Berlin authorities,

The BVG as a public institution should also be able to accept applications in the same way64

Right as a data protection-friendly alternative, however, will also be available again in the future

provide non-electronic application process.

The BVG continues to take out subscriptions for the free student ticket

ment contracts with parents, legal guardians or students

students themselves. Within the framework of these contracts, it is authorized to collect data

and must temporarily keep these documents for its accounting purposes. Included

However, each individual date must be checked for its necessity.

Technically, attention must be paid to current encryption standards.

4.3 Why Bicycles Motion Profiles

create

Since November 2017, there have been several thousand rental bikes from Mobike Germany

GmbH (Mobike) on the streets of Berlin. As well as other rental bicycles, rental scooters

or cars can be borrowed via an app. was viewed critically

above all that the Mobike app collects a lot of data that is processed on behalf of China

be worked.

A

and

s

i.e

e

right

P

right

a

x

i

s

The Mobike app records the user's movement data while they

are looking for a bike with the app and continuously select

the driving time as long as the app is running in the background. You can during the

driving time but also be closed; in this case no further

64 Section 4 (7) E-Government Act Berlin (EGovG Bln)

83

Movement data recorded. Aside from that, the bike shares everyone via GPS itself

four hours Mobike with his location. Linking these via GPS with

Shared location data of the bike with the data of the app does not take place.

Furthermore, Mobike collects a variety of device data from the smartphone such as the

Hardware model, the unique device identifier or optionally the unique

advertising identifier of a device.

In order to process the loan agreement, only the absolutely necessary

gen data are collected. In the location data, this is the respective start

and target point. Hereby the rental period as well as possible violations of the

Rules of Mobike for parking the bicycles are determined. Also the

Collection of device data is only permitted to the extent that the app

information needed to function. Additional data collection

Exercises are only permitted with a legally permissible reason or a voluntary one

User consent permitted. Mobike was able to do both in our test

not present. A complete capture of the route is neither to protect against

Theft still necessary for other reasons. Also the transmission of

unique device identifiers to improve the app is not allowed.

We have asked the company to clearly limit the collection of data

and set him a deadline of early 2020 to do so.

Mobike has the data collected from its parent company based in Beijing (China).

process on behalf of companies. Both companies have signed contracts

closed, which exceeds the scope of permissible processing according to the DS-

standard contractual clauses that are permissible under GMOs.65 This is legally required

formally not objectionable to the current state of knowledge, however, the

Standard contractual clauses just reviewed by the ECJ.66

65 These are contracts based on the standard contractual clauses according to the decision of

European Commission of February 5, 2010 on Standard Contractual Clauses for the

Transfer of personal data to processors in third countries

of Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU)

66 ECJ proceedings on Az C-311/18 (so-called Schrems II proceedings)



Chapter 4 Transport and Tourism 4 4 Sightseeing with Spam escort

On the basis of a contract between a person whose data

processed and the companies responsible for processing

only the data that is essential for the contract may be processed.

Data that is collected beyond this may only be used with legally verifiable

reasonable justification and taking into account the impact on the

informational self-determination of those affected.

4.4 Inspection accompanied by spam

Every day we receive many inquiries about the unauthorized sending of advertising e-

mails. These are, for example, complaints such as: "When registering

on an online platform also had to be included in the sending of promotional emails

be consented to" or "I am receiving unwanted emails to my email address

Newsletter, although never given consent to receive newsletters

became".

A

and

s

i.e

e

right

P

right

a

x

i

s

One example out of many: a family wanted for the forthcoming visit to Berlin

Tickets for a sight and a table reservation in the local

Book a restaurant. Here she was informed that with the registration

also a consent to the sending of messages from the provider, e.g. for

Newsletter or similar, submitted. The corresponding information text suggested consent

due to a corresponding presetting. However, this cannot

be considered sam because it involves a clear action (e.g. setting a

Hakens) and the voluntary nature of the declaration of consent is missing.

We tried to convince the provider, if only for reasons

of customer satisfaction to change the notice to effective consent -

finally the sight i. i.e. R. visited by tourists who, after their

Hardly interested in further information about the restaurant etc. on the return journey

should. However, that was not successful.

After initial reports to the contrary, the provider then made it clear that

that he does not send any advertising e-mails at all, only the customers

Ask customers to give him feedback on their visit. This assessment

Information requests would be sent after each visit.

85

This is to be assessed differently than, for example, sending a newsletter. The Zusen

tion of individual, simple customer satisfaction surveys as a follow-up to a

The order is made in the legitimate interest of the provider, which - in contrast

for pure advertising - the interest of customers not to receive such inquiries

hold, prevails. However, only on the condition that the customers

and customers receive a clear and conspicuous indication of this procedure

and can object at any time.

However, even for a request for an evaluation, customer data must not be endlessly

be saved. If the storage of an e-mail address for the purposes

for which it was collected or processed is no longer required

erased within a reasonable timeframe. For the implementation of customer

The satisfaction surveys would be at most a period of one month after

the visit to the respective sight can be justified. The obligation to

Deletion also means that those responsible must fulfill their obligation to

independently and continuously.

A deletion concept for old entries in the advertising list existed in this specific

th case obviously not; corresponding inquiries regarding the storage period

and deletion concept were only answered with the information that customers

Customers could object via email or unsubscribe link. So we check

the initiation of administrative offense proceedings.

In principle, e-mail advertising is not an inadmissible harassment

go to In the case of existing customers, the storing position in the

However, as part of the customer relationship, the e-mail address is used for further advertising

use if the following conditions are met:

• A company has related to the sale of a product or

the provision of a service the electronic postal address of the customer

or the customer received

• the company uses the address for direct marketing for its own similar

chemical goods or services,

86

Chapter 4 Transport and Tourism 4 4 Sightseeing with Spam escort

• the customer has not objected to the use and

• When collecting the address and each time it is used, it becomes clear and concise

pointed out that the use can be contradicted at any time

can.

The newsletter is only valid if all the requirements specified here are met.

ter shipping is legally authorized and does not require separate consent.

There are remedies and against the sending of unauthorized commercial e-mails

Ways. Should an objection not lead to success, the responsible

help regulator.

87

5 Youth and Education

including

media literacy

Film and photo recordings of children –

Uncertainty due to data protection

basic regulation

5.1

s

i

x

a

right

P

right

e

i.e

s

and

A

In our last annual report we reported that with the

The General Data Protection Regulation (GDPR) coming into effect in

look at the handling of personal data during production and

Publishing film and photo recordings of children is a special one

Uncertainty has arisen.67 Confusing press reports about the alleged

Necessity to redact all personal information about

the children still have this uncertainty for data protection reasons

strengthened.

Interest in the subject has not diminished this year either. Still

we always receive numerous inquiries and complaints about the

data protection-compliant handling of film and photo recordings of children, in particular

special in day-care centers. However, the topic can also be

at schools or events in which children take part, e.g.

positions, expand as you like.

First of all, the production of film and photo recordings of cinema

and possibly also their publication for data protection reasons

is not inadmissible from the outset, but with the appropriate consent

declarations of consent can be designed in accordance with data protection regulations. explicit

Consent is required, however, since the production of photos and films

67 JB 2018, 5 4

88

Chapter 5 Youth and education including media literacy 5 1 Films and photographs of children

taken by children in day-care centers or schools for the

care of the children or school-related tasks is required and

with also cannot be covered by data protection regulations. This is how

speaking recordings do not rely on the fact that these are supposed to safeguard

the legitimate interests of the person responsible, i.e. the institution or the

school, are required. In this case, it is necessary to check whether the need for protection

of the data subject prevails, especially when it concerns her

a child.68 The GDPR expressly assumes the special protection

poverty of children and makes special demands in terms of

processing of their data. Therefore, regardless of the question of whether legitimate

interests of the person responsible in relation to the preparation and publication

of photos exist to assume that the interests of the affected

from the outset predominate if these are children.

del. Such recordings can only be made without exception on the basis of consent

support.

When designing corresponding declarations, the following requirements apply

observe:

Consent to be obtained from parents must be voluntary and informed

take place. In concrete terms, this means that the parents are made transparent

must state for what purpose, as precisely described as possible, the recordings

are to be manufactured. Parental consent must explicitly refer to both the

production as well as the publication of the recordings on the homepage

or in another way (e.g. print publications, notices on the premises)

related, so that in the declaration between production and publication

should be distinguished. In practice, it makes sense for the different

technical purposes, e.g. taking photos on trips or events, showing

of film sequences at a parents' evening or use for the creation of

Teaching material, checkboxes to be provided in each case. In view of the

dangers to personal rights associated with the public

Possibility of global retrieval or the possibility of using search engines

to find and misuse, we recommend in our counseling

speak regularly, also clearly pointing this out in the declaration of consent

68 See Art 6 Para 1 lit f GDPR



point. It is also important to specify in the declaration of consent what

should be done with the recordings and how long they will be kept, where and how

the. It is also necessary to inform the parents in the declaration that

that you have the right to revoke your consent at any time

revoke for the future. This is according to our experience in practice

often forgotten, but is a necessary criterion for the effectiveness of a

declaration of consent. Finally, parents should be made aware

that the acceptance of your child in an institution does not depend on the granting of a

may be made dependent on a declaration of consent and neither can you

Disadvantages may arise if you later revoke your consent.

It is our concern to make the institutions aware of the uncertainty that has arisen in the

to take pictures and filming of children. That interest

the topic is still high, shows us the demand for our

Guidelines on data protection for image, sound and video recordings69,

which we together with the Senate Department for Education, Youth and Family

have issued. At the beginning of 2020 we will therefore, together with the Se-

natsverwaltung create a new edition of this guideline in which

we will take into account our first experiences with the GDPR.

5.2 Who is allowed to see what in the youth welfare office?

For several years we have been reporting on the introduction of the administrative

effective specialist procedure ISBJ70 as a central IT solution in the Berlin

genämter, with which the business processes in youth welfare are standardized

should be.71 This also includes defining how the

rights of access for employees to the necessary personal

gene data are to be technically restricted. In practice, this requires

an adaptation of long-established procedures to the new ones

circumstances.

s

i

x

a

right

P

right

e

i.e

s

and

A

69 https://www datenschutz-berlin de/fleadmin/user_upload/pdf/publikationen/informati-

onsmaterials/2018-BlnBDI_Flyer_Privacy_Content_Web pdf

Integrated software Berlin youth welfare

70

71 JB 2018, 5 3; JB 2017, 2 3; JB 2016, 5 4





We were informed that within a youth welfare office the

Specialist software limited access to individual organizational units, each

perform different tasks, was circumvented by the fact that help

feplans were now exchanged in paper form between the units.

These help plans contain all the specifications for educational needs,

the type of help to be granted and the form and success of the help

in each individual case.

Specifically, families in the youth welfare office are supported by the regional social pedagogical

schen Dienst (RSD) pedagogically supervised. Economic youth welfare (WJH)

is another organizational unit that takes care of the financing of the

th services. For this, both bodies need information about the

th families. Because of the differences in the perceived duties of these

both organizational units in the youth welfare office are the required information

however not congruent. Just the socio-educational care required

it, also very sensitive information about the problems in the families

know. In many cases, however, knowledge of this is not necessary in order to

to ensure that the aid is delivered. For this reason, the access options

ten to the personal data in the specialist software.

A transfer of the help plans in paper form by the RSD to the WJH is included

Data protection principles are just as incompatible as the transfer

in digital form, since not all information is available for the financing of the services,

necessary for the pedagogical work with the families.

We asked the youth welfare office to tell us how a data protection

procedure is to be established. The youth welfare office informed us that

that various measures would be examined. A form is developed

been made, by which it is ensured that only the really necessary data is

be passed on within the youth welfare office. It will also be checked whether they are not

required data could be blacked out in the assistance plans. We have

pointed out that it is crucial to ensure, organizationally,

that only the data actually required between the two organizations

units are exchanged. In addition to the master data that can be accessed in

the specialist software is granted, the WJH may only use those additional data

take note of the specific circumstances in each individual case for their

task completion is required.

91

We assume that the youth welfare office will establish a procedure

that meets the data protection requirements. The example

shows that the conversion of processes to IT solutions is very suitable

can be to back up long-established but inadmissible procedures

ask in order to develop a data protection-compliant state.

5.3 On the use of Office 365 in schools

s

i

x

a

right

P

right

e

i.e

s

and

A

Again and again we receive inquiries from schools about admissibility

the use of Office 365. This is a product of the company

company Microsoft Corp., which usually the Office applications in a

provides a cloud-based variant. Since the question of the admissibility of the

sets not only in Berlin, but nationwide and also for other parts

of public administration is relevant, the data protection supervisory

Federal and state authorities have been using Microsoft for several years

Discussion about how the product can be used in compliance with data protection regulations.

The basic problem is that Microsoft due to the assignment by

an authority becomes aware of data that is also used for the company's own purposes

be used without any apparent legal basis for this

were. In addition to the content that the authority processes, the data

also asks for information about the users, whether they are employees

or students. This is done in particular via the

the software.

In principle, it is conceivable under data protection law to use cloud-based services

private providers can also be used in public areas such as schools.

However, which requirements must be met in order to meet the specifications of the

Compliance with the GDPR is the subject of discussions between the data protection

regulators and Microsoft.

A particular problem is that between those responsible and micro

soft to be concluded contracts for order processing by Microsoft

dar. Microsoft requires the clients that they

Further processing of your possibly personal data by Microsoft also for



Allow for product improvement purposes. For a corresponding

carried by public authorities and a provision of personal

Data relating to employees or citizens is one

Legal basis not recognizable.

The German data protection supervisory authorities are currently in a

close coordination process on how to be achieved towards Microsoft

that such data use is omitted. Until then it stays

leave it up to those responsible to use Office 365 in such a way that the personal

Genetic data only without using the cloud in their own information

technology are saved.

We are well aware that the time with those responsible who deal with

the question of the admissibility of using Office 365 in their institutions

employ, urge. We are therefore intensively involved in the clarification process

of legal and technical issues to deal with schools, as well

the other actors in the public administration for legal certainty

care for. We assume that the conference of independent data

protection supervisory authorities of the federal and state governments (DSK) promptly

suspensions for a permissible use of Office 365. It

will be up to Microsoft to do its part to meet these requirements

to wear.

5.4 The School Data Ordinance – A new major

construction site on the way to digitization

After we last year the Senate Department for Education, Youth

and family regarding the adaptation of the Berlin school law to the DS-

GVO,72 this year the amendment of the school data understanding

order on the agenda.

72 JB 2018, 5 1



A

and

s

i.e

e

right

P

right

a

x

i

s

The School Data Ordinance, which dates back to 1994, was last passed in the year

Supplemented in 2010, but the main regulations are now 25 years old.

In the meantime, the actual circumstances, especially in

With regard to digitization, however, so significantly changed and further developed

that the old regulation no longer does justice to this development

becomes.

To reflect the demands of running a modern school,

especially against the background of the Berlin Digital Pact, there is

significant need for change. That's why we've had both since autumn 2018

recommended in writing, as well as in several discussions, a complete new

structuring of the regulation. This proposal is the responsible

Unfortunately, this has not yet been followed by the Senate administration, although this has

Lately elapsed time should have been possible without any problems.

The last draft available to us for an amendment from August 2019 is required

still a major revision. In addition to unclear regulations on

School statistics and data processing by the Senate administration within the framework of the

Vocational and study orientation were in particular regulations with which

to react to the increasing digitization is insufficient.

In order to create legal certainty for those involved in the school sector and

grew" must be in a modern school data regulation

Framework conditions for the use of digital media are defined. As re-

In particular, the use of private devices by the

teaching staff and the student body, the use of social networks and of

Learning platforms, the requirements for the network installation and the

to name the development of messenger services. For this we have the Senate Administration

intensively advised. It is urgently necessary that the school data regulation

planning now goal-oriented and passed as quickly as possible and this

important topic is not delayed any longer.

In order to ensure data protection-compliant implementation of digitization in the

the senate administration must quickly take the necessary

Create a legal framework that schools can use as a guide

can ren.





5.5 Research with the files of the youth welfare offices –

possibilities and limits

In the past year we have the Senate Department for Education, Youth and

Advised the family several times as to whether and under what conditions they should apply

by researchers upon inspection of files or upon transmission of individual files

youth welfare offices can grant.

The files of the youth welfare offices are popular objects for scientific research

ing. However, it should not be forgotten that these files

contain particularly sensitive social data of the affected families. One

The transmission of social data to third parties is therefore, with good reason, subject to strict

suspensions linked.

A

and

s

i.e

e

right

P

right

a

x

i

s

Whether youth welfare offices use the social data they process for research purposes

may transmit to third parties, regulates the Social Code (SGB).73 The strict

Prerequisites provide that the youth welfare offices - and other social services

carriers – are not allowed to decide for themselves whether social data is passed on to researchers

to spend Rather, because of the special need for protection, the legislature

activity of social data, an approval requirement is provided. That's what it takes

prior to the transmission of such data, always obtain approval from the highest level

Federal or state authority responsible for the area from which the data comes

is responsible.74 Is responsible for research in the field of child and youth welfare in Berlin

this is the Senate Department for Education, Youth and Family.

The first requirement for approval is that it is not “any”

research project, but a concrete project that refers to the

social benefits area.75 Furthermore, there is a transmission of social data

only be considered if they are necessary for the implementation of the

research project are actually necessary, i.e. unavoidable. Are

73 See Section 75 SGB X

74 Section 75 (4) SGB X

75 In addition, a specific project of the scientific professional

and labor market research, § 75 Para. 1 Sentence 1 No. 1 SGB X

95

If these "entrance requirements" are met, it is also fundamentally necessary to

consent of the data subjects to the transmission of their social data. Allen

if in exceptional cases, namely when obtaining consent

is unreasonable (e.g. because the purpose of the research project has been frustrated

the would), a transmission may also be possible without the data subjects

be asked beforehand.76 In these cases, the SGB sees a further protective mechanism

nism, however, requires a weighing of interests. A transmission without consent is

therefore only possible if the legitimate interests of those affected

persons are either not affected at all or a consideration

tion shows that the public interest in research outweighs the interest of the

one person in the secrecy far outweighs.

The Senate Department for Education, Youth and Family has

research projects asked for advice. In a project in which it is about

research on domestic violence in families with children, we have

view expressed by the Senate administration towards the researchers,

that in the specific case obtaining the consent of the persons concerned

is reasonable and therefore unavoidable, confirmed and their concrete form

accompanied by instructions.

In another project that the Senate administration itself communicated to the

verity Hildesheim commissioned and in which it is also in the public

Public much-noticed review of the role of the Senate administration in the

Accommodation of young people with pedophile men as part of the so-called

"Kentler experiments", we have the Senate administration

the files prior to transmission to the researchers

to anonymize, since obtaining the consent of data subjects

and third parties, whose data were also contained in the files, practically none

would have been feasible.

We can see the great interest in inspecting youth welfare files for

Understand research purposes. Although a transmission of social

data from youth welfare offices for research purposes is not used from the outset

76 That obtaining consent sometimes involves considerable effort

may be connected does not, however, lead to unreasonableness from the outset





is closed, the strict requirements of the SGB must be observed. offered

in view of the special sensitivity of the data contained in the youth welfare files

data often requires complicated balancing of the right to

informational self-determination of the affected families and the

research interests of scientists. The practice

shows that taking advantage of our advice as early as possible

fen to achieve appropriate results.

## 5.6 Privacy and Media Literacy

Since the end of 2016, we have been developing offers for children to help them protect theirs

to sensitize one's own data in the rapidly digitizing world.77 In

This year we have further optimized our offers for children and

In particular, our children's website www.data-kids.de has been fundamentally revised

and redesigned. We have also started conducting project days in schools

to try out the developed materials with the elementary school children

try to get feedback from our target group and in this way

to gain knowledge for the further development of our offers.

A

and

s

i.e

e

right

P

right

a

x

i

s

Recent studies show that even children of primary school age regularly

use git media. The traces they leave on the Internet and on the

left behind by the devices, they are often not even aware of. Lots of kids do

first experiences with smartphones and tablets, even before they read fluently and

can write. Apps and offers are often used that are by no means

are designed to comply with data protection regulations.

It is particularly important to us to sensitize the children as early as possible

and to teach them data protection competence. With the complete redesign

our children's website www.data-kids.de, it was our goal to create games and fun

to connect with learning. In addition to the already from the previous offer

well-known robot family, which teaches children all about technology and

accompanied by self-protection, we have animal figures in a special

developed its appealing manga style. The animals mediate in the children's encyclopedia

77 JB 2017, 6 6; JB 2018, 5 5

97

the most important terms related to the topic of data protection with interactive maps,
Explanatory videos and lots of colorful graphics. In addition to the offers for children, such as
Games and craft materials, we also want parents and teachers useful
provide offers. Therefore, in addition to an extensive link
collection e.g. also workbooks available, which can be downloaded and stored with us
can also be obtained free of charge in paper form.
We were particularly pleased that this year we launched our children's website
have been nominated for the German children's software prize TOMMI. For this
Prize meets a jury of experts from the fields of media and media education
and educational sciences a selection from the submitted software
products, such as games or apps. She gives this to a children's jury for the final
towards voting. We have the finals of this year's competition
reached. We were certified that our offer www.data-kids.de was the first
Offer of its kind aimed at children of primary school age for data protection
sensitized. The nomination shows us that we are on the right track
have.
For the year 2020 we have decided to continuously expand our range of
to develop. In addition to new content and materials for our children's web
page we will evaluate the projects carried out at the schools and
Develop concepts on how these can be better established in order to
to reach as many schools as possible. However, a focus is also
werkarbeit lie in order to work with other actors from the media-pedagogical
to enter into cooperations in the state of Berlin and thus the mediation of
Data protection competence to be as broad as possible.

98

Chapter 5 Youth and education including media literacy 6 1 Health apps with insufficient protection

6 health and care

## 6.1 Health apps with insufficient Protection

The development of health apps is one of the main areas of activity digital health economy in Berlin. Since such apps with sensitive data ten, it is important that the processing also takes place in the cloud systems, behind the apps runs safely. In an example we have seen how successful the operators are.

A

and

s

i.e

e

right

P

right

a

x

i

s

Those who shy away from going to the doctor's office will find a number of support offered online, often in the form of apps for smartphones. The federal Government is driving the supply of digital health services and has in particular with the Digital Supply Act (DVG) the legal prerequisites stipulations for the financing of these services by the statutory health

insurance created.

Health apps are used for counseling and therapeutic purposes

puts. In both cases, they can only work if the users have medical

Enter niche data in them or send this data to the operators in another way

submit the offers. This results in high protection requirements

of confidentiality and integrity of the data processed by the operators. Egg-

Some of the offers are also to be classified as medical devices and are subject to

thus particularly high demands on reliability.

The small or medium-sized companies founded as start-ups, which

operate offers, often do not use their own computing technology, but

Cloud offerings from major providers. These make the networks available,

drive the software and the databases and at the same time also offer security

functions. Application development is also largely based on external

operated services. The software is created from these development environments

largely automatically transferred to the IT systems with which the user

data are processed.



The conventional measures to ensure information

operational safety only to a limited extent. For ensuring security comes

no hardware and software that has been checked carefully and over a long period of time is used,

which is rarely revised or replaced. There are no more cable connections

ments that determine which devices can be addressed from the Internet and thus

are vulnerable, but easily changeable software settings. Therefore

The security measures have been adapted to the new dynamic environment

become.

In addition, new risks arise that are inherent in the nature of extensive claims

use of cloud services. Your own security measures must

with which the cloud providers are intertwined in such a way that the same security

level of security, as is the case with an operation based on its own information technology

uniform control would be possible. This also applies to the control over the

Access to individual systems and services. To prove that a human

or software for using services in the cloud and setting

settings, sequences of letters to be kept secret,

Digits and other characters, so-called access keys, are used. whoever

individual possesses these keys, has power over parts of the information technology

nik of the company, possibly even across the entire system. goes the

Losing control of the keys opens the door to misuse.

We were interested in the extent to which companies with the challenges ad-

äquat bypass, resulting from their decision, completely in the cloud

switch. Data protection law obliges you to notify the supervisory authorities

to prove that they respect the confidentiality and integrity of the data entrusted to them

can guarantee.

The result of our audit of a company with a

impressively large number of users was not satisfactory. It was

shown to us that a whole series of useful individual measures

were taken. However, these did not fit into an overall concept

together, with which the risks would have been reduced to an adequate level

can. The company's perspective was too limited to common methods

methods for cyber attacks to which its information technology is exposed. Not

on the other hand, e.g. the possible tapping of access information

information on the developers' computers and other

other storage locations or the possible manipulation of data that the services

be handed over for processing, or the derivation of security-critical

cal information from the observable behavior of the services and systems.

However, the complete consideration of possible hazards is

of far-reaching consequences, because an incomplete risk

analysis usually also includes an incomplete range of security measures

men.

Where necessary, we will use our remedial powers to

checked companies for a risk-based design of their service

move. At the same time, within the scope of our capacities, we will

tronic health services into our testing program.

Some risks are inherent in using eHealth services

unavoidable because many private individuals do not use smartphones

equipped to guarantee an adequate level of security. Besides that

However, every person can expect that when processing their health

data, whether with the service providers, the IT infrastructure

ture in the healthcare system, the service providers and also in the private sector

a uniformly high level for non-physician providers of healthcare services

level of security is provided.

Whoever offers electronic health services is a reliable

reliable protection of confidentiality and integrity of the processed data

obliges. If new approaches - e.g. the continuous development

development and operation in the cloud - to provide the services

are used for a large number of people, is in the data protection

beforehand, a thorough analysis of the

identify associated risks and determine countermeasures

conducive.

101

6.2 Open Medical Records at the Hospital

s

i

x

a

right

P

right

e

i.e

s

and

A

We checked whether the two major hospital operators in Berlin,

the Charité and the Vivantes Netzwerk für Gesundheit GmbH, with saved

information on the treatment of patients who have already been discharged

as required by law, in particular whether they have the right to

accessed the data no later than one year after the completion of the treatment lock

and delete them after the retention period has expired.

Hospitals have the obligation to document medical treatments

mention. Here, quite legitimately, large amounts of sensitive data are stored

chert These must last for a legally prescribed period of between ten

and retained for thirty years. Within this period, additional

Access to the data is only possible after the respective treatment has been completed
if there is a special need for it. Accordingly, they must
Access authorizations are severely restricted during this period. After
Expiry of the deadlines, however, further storage is only permitted
sig if there is a specific reason for it.
In both hospitals examined, we found that these requirements
requirements are not met. Patient data also remained in the Charité
Discharge and billing of the treatment in the long term in access to the majority
ing majority of employees, which is a gross violation of the law
represents specifications. Vivantes restricted access much more. the
right from the start, the options available were based on the needs of the treatment
aligned. In addition, after the end of treatment, they were in most
cases limited in time. However, this restriction did not apply consistently and
came too late in some cases.
Confronted with the legal requirement, both houses immediately took
measures were taken to eliminate the deficits. The Charité laid an ambitious
ned plan with measures to upgrade or replace the tested ones
technical systems and setting up time-defined access restrictions
known. Just a few months after the exam, she was able to report that
in one of the tested systems the protection of patient data against an un-

justified access now corresponds to the legal requirements. vivid
also acted quickly and presented a plan with which the existing
Access options should be adjusted and gaps closed.
In the case of data from outpatient treatment, we checked whether they were after expiration

be deleted after the retention period of ten years.78

we found deficits in both houses. These must now be

fetching deletion and the establishment of regular deletion routines

become. The hospitals are at liberty to provide patients,

who wish to do so, also to offer longer storage.

In the following, we will closely work together to rectify the deficiencies at Charité and Vivantes.

follow and, should unexpectedly unacceptable delays arise, from

exercise our remedial powers.

Hospitals must ensure that the data of patients

patients who have already been released, only a narrowly defined personal

circle available for well-defined purposes and after the end

be deleted after the retention period.

6.3 Termination with multiple unknowns?

Improving the appointment management of medical practices can improve

serve to improve health care and is therefore to be welcomed. However is

it is imperative that the processing of patient data is carried out for the

patients remains transparent and additional services such as

reminders via SMS or email, only with the consent of the patient

and patients take place.

A

and

s

i.e

e

right

P

right

a

x

i

s

In 2019, we received repeated complaints from citizens who

were reminded of doctor’s appointments via SMS or email without them being included

78 Data from inpatient treatment, on the other hand, must generally be recorded for thirty years.

maintain; however, none of the systems examined included data from treatments that

so far behind

103

had consented. The sender of this message was a Berlin company that

the appointment reminder for patients as a service provider for medical

practices.

The appointment reminder was in a specific individual case as an additional

service designed for the doctor, which, in addition to taking over the entire

th appointment management was offered. Only by getting the memory

were those affected referred to the appointment management outsourced by the doctor and the

underlying service provider carefully.

The desired goal of the additional appointment reminders is to optimize the

workflows in practice. The reminders are intended to count the number of appointments

which are canceled because the patients forget an appointment,

be reduced.

In addition, the company offers by knowing the times that are still free

the doctors the patients the opportunity to

a website to book appointments directly.

Patients who themselves have a user account on the Internet

have a page, select the reminder function actively. However, if not

is the case, an appointment is arranged by telephone or directly in the practice

and the practice staff does not draw attention to the reminder function,

the patients are surprised by such news.

Such an appointment reminder system is particularly critical, especially

half because it can contain data that is very sensitive. One can

Appointment reminders for doctors specializing in

point out the state of health of the patient.

A legally permissible form of outsourced appointment management

of medical practices is in principle quite possible. However, this presupposes

that the doctors contact the respective service providers as part of the

obligation to secrecy. If this is fulfilled, a

Service providers then themselves subject to the statutory duty of confidentiality.79

79 See Section 203(4) of the Criminal Code (StGB)





According to the GDPR, a doctor's practice may only use the data of patients

Patients are processed to fulfill the respective treatment contract

are required.80 For appointment processing that goes beyond appointment management

however, the consent of the patient is required

ducks, since the reminder of the appointment does not carry out the treatment

itself is necessary and insofar not due to a legal processing

authority can take place. Responsible for obtaining this consent

is the place where the appointment is made. Are appointments about the

booked on the website of the service provider, the latter must ask the user for consent

ask for a loan. If the appointment is made by the staff of the doctor's office,

the practices responsible for it. However, service providers from medical practices are available

in the obligation to inform the practices about the requirement for consent.

When doctors hire a service provider with appointment management for

commission their practice, they must give this to their patients

make them transparent to each other. Especially when it comes to health data

It is particularly important that those affected are aware of the bodies through which

their data will be processed. Providers of such services should

Compliance with their legal obligations is so easy for doctors

do as possible. This also includes being unequivocal on this

obligations are pointed out.

6.4 Resolution of an old dispute? quality

security at the statutory health insurance

Association Berlin

In the last annual report we have the verdict of the regional social court

Berlin-Brandenburg on the quality assurance process of panel doctors

Vereinigung Berlin (KV) reported.81 Through this we became in our legal

opinion confirms that quality assurance by the KV patient data

data may only be collected in pseudonymised form.

80 See Art 6 Para 1 lit b i V m Art 9 Para 2 lit h GDPR

81 JB 2018, 6 1



A

and

s

i.e

e

right

P

right

a

x

i

s

With effect from July 1, 2019, the Federal Joint Committee (GBA)

Due to its directives resulting from the Social Security Code (SGB)

petenz82 the "Quality assessment guideline for contract medical care"

ben and recast. The guideline of the GBA is for the KV as well as for

Statutory law binding on insured persons and contract doctors. The

Guideline of the GBA now explicitly provides for the submission of treatment

mentations in non-pseudonymized form in all cases of quality assurance

planning.

This change in the legal starting point means that we have to

KV the implementation of quality assurance with identifying data now

had to assess as admissible.

However, we have considerable doubts as to whether the issued directive is subject to a judicial

would stand up to scrutiny. This is how the guideline authorization of the

§ 299 SGB V expressly stipulates that the data collection is usually based on a

sample of the affected patients is limited and the insured

Data related to data are pseudonymised. Only in exceptional cases

if, for example, the correctness of the treatment documentation is the subject of the

quality check, identifying data may be collected.

The GBA has stipulated in the guideline that in all quality tests for which

the policy applies, the accuracy of the treatment documentation

is the subject of the examination.

With this determination, the rule-exception-specified in § 299 SGB V

relationship is not only reversed, but even ignored, since it is envisaged that in all

collect identifying data from patients in such cases.

By adapting the guidelines for quality assurance by the GBA

a regulation was made that applies to both the KV and the affected

ven doctors is binding. To what extent this guideline

would stand up to judicial scrutiny is very doubtful, given that by

82 See § 299 SGB V





stipulation laid down by the federal legislature that the data collection “in the

rule" with pseudonymised data, through the directive um-

will go.

## 6.5 Nothing going on without moss? – The claim to a copy of the patient file

In the past year we have been asked by doctors several times

have been confronted with whether they want patients who have a copy of their patient

require duck files, even after the GDPR has come into effect

may charge for the costs incurred.

Background: The Civil Code has been clearing since 2013

(BGB) patients explicitly have the right to a copy on request

to receive their medical records. The prerequisite is that they pay the costs for this

wear.83 The professional regulations also provide that doctors are

are only obliged to issue copies if they bear the costs

be reimbursed.84 In other words: at least in the past, the

Legal position clear.

A

and

s

i.e

e

right

P

right

a

x

i

s

But how has it been since May 25, 2018? The regulations in the BGB and

in the professional order have not changed. With Art. 15 Para. 3 GDPR

however, a provision has been added that has a similar regulatory content

having. Specifically, this regulation provides that every person responsible - and

Of course, this also includes doctors – the people affected

provide a copy of their personal data upon request

must. However, this provision contradicts the German Civil Code: a claim

the DS-GVO grants the person responsible for an appropriate fee

expressly only for "all further copies" - the first copy, however, is

always given free of charge.

83 § 630g paragraph 2 sentence 2 BGB

84 § 10 paragraph 2 sentence 2 professional regulations of the Berlin Medical Association

107

So how do you deal with this contradiction?

Our answer: European law takes precedence over German law. the cost

In any case, the patient's obligation to bear the

be preserved when the patient first receives a copy

request their personal data.

Under certain conditions, the GDPR generally allows

Restriction of the rights of data subjects, including the right to information or

the “right to copy” counts, by member state legislation. The

However, due to the social

overriding economic interests and at the same time proportionate

be.85 However, these prerequisites are not present here. In particular, the

Obligation to bear costs according to the BGB is not a necessary measure for protection

of the rights and freedoms of doctors. That the fulfillment of

enforcing rights for those responsible sometimes also entails costs, is a thing in itself

no reason to assume that their rights have been violated.86

The fact that the GDPR does not smoothly integrate into the member state

inserts legal law and legal uncertainties can sometimes arise,

not surprising. Ultimately, however, it is up to the federal legislature to

to ensure harmony again by adapting the BGB. Until

then doctors would be well advised not to hand over the pa-

A copy of the patient file when the patient first requests it

not to be made dependent on the assumption of costs.

6.6

Informed consent for research

plan – not a discontinued model!

In the field of research, in our consulting practice, we will always

who is confronted with declarations of consent, which are made to the best of our knowledge and

were written conscientiously, but did not meet the requirements of an internal

85 Article 23 (1) GDPR

86 Art. 15 Para. 4 DS-GVO can be used to restrict the restriction of Section 630g Para. 2 Sentence 2 BGB

therefore not supported - this provision is not about

an opening clause for the member state legislature





form consent. It should be noted that the specific

purposes, consent obtained in the research area even after effective

sam the DS-GVO will continue to be the norm.

The processing of personal data is based on a

Consent of the persons concerned is only possible if this declaration

met strict requirements. It must be voluntary and - based on a specific

voted case - in an informed manner.87 In addition

the persons concerned must be informed that they can revoke their consent

can currently be revoked and that the revocation violates the legality of

no data processing took place on the basis of the consent until the revocation

is touched.88 Is intended to include special categories of personal

to process data (e.g. health data), the declaration must express

may also refer to this information.89 Compliance with the written form, on the other hand

is not (any longer) required by law. An unequivocal one is enough

Expression of will in the form of a clearly confirming action (e.g. active

click on the "Agree" button). Of course, the written form remains

casual and possibly also useful.

On the one hand, to ensure that the persons concerned are informed

deliver and on the other hand not to deliver the actual declaration of consent

freight, it has proven itself in practice in research projects to

affected persons in addition to the actual declaration of consent

to provide separate information text. The people concerned

should be written in clear and simple language90 about the respective research

project and the associated data processing are explained. So

should they be able to make decisions in the first place?

whether they agree with the intended processing of their personal data

are understood. This information is therefore essential for the effectiveness of a

Consent.

87 Art 4 No. 11 GDPR

88 Art 7 Para 3 GDPR

89 Art 9 Para 2 lit a GDPR

90 See EG 42 GDPR



The general information requirements91 from the

DS-GVO, which basically affect every responsible person - independently

whether this personal data is based on consent or

processed by law. These mandatory disclosures overlap

in terms of content with the information that is required to

mated consent” (e.g. indication of the person responsible and

the purposes of data processing). However, they are not entirely congruent.

Our experience shows that this distinction often increases in practice

ambiguities in the demarcation.

But what exactly is the problem in practice? – It is possible from our experience

essentially two aspects:

On the one hand, we have to state again and again that the explanations presented to us

ments or information letters do not do the intended data processing

reflect sufficiently or even incorrectly. A “classic” is about here

the incorrect indication that the processing is "anonymous", although it is actually one

Processing takes place in pseudonymised and therefore personal form92.

On the other hand, it is always the language used itself

is often not taken into account by those responsible for the project, to which target

group the information is aimed at. For example, technical terms do not belong in one

information letter. These are easy to formulate and generally understandable.

and should also be limited to a reasonable length.

If these requirements are not observed, the study participants can

and participants also do not have a comprehensive picture of the scope of their declaration

make. This is at the expense of informational self-determination.

Departing from the principle of obtaining consent for specific purposes

Even after the GDPR has come into effect, there is still no indication of this. That is

scientific research has made simplifications in many areas of the GDPR

91 See Art 13, 14 GDPR

92 This is the case, for example, if – as is often the case – the names of the participants

mer can be replaced by an identification number and a list containing the assignment

between names and numbers still exists



genes,93 but that doesn’t mean that researchers will no longer be able to

specific purposes of data processing must be specified if they

ask participants for their consent. The GDPR points out in its

Recitals94 indicate that data subjects may be allowed to do so

should, their consent for "certain areas of scientific research"

admit. The Conference of Independent Data Protection Authorities

The federal and state governments (DSK) have now made it clear that only in individual

case and only if the specific design of the research project

foreseeable until the time of data collection a complete purpose

absolutely does not allow the explanation to be a little more "open" on this point

or "broader".95 However, one of the prerequisites is that specific

cal security measures are observed.96

Informed consent is still the norm. A departure from

the principle of clear purpose in the field of scientific

Even in times of the GDPR, research is only possible in rare individual cases

and only possible if concrete compensatory measures are planned

are.

93 For example, the legislator has given the member states the

Possibility granted to exercise the rights of data subjects under certain conditions

restrict if data processing for scientific research purposes

The German legislature has done so with Section 27 (2) of the Federal Data Protection Act

(BDSG) use is also made of Art. 14 Para. 5 lit b DS-GVO, for example, a

Statutory possibility of exemption from the information obligations in the case of so-called "third-party

gene"

94 EC 33 GDPR

95 See decision of the 97 DSK on the interpretation of the term "certain areas

scientific research" in recital 33 of the GDPR of April 3, 2019

96 E.g. Use of a usage regulation that can be viewed by those who consent

Direction of an internet presence through which the study participants

be informed about current and future studies

111

7

integration, social and

Work

7.1 Complaints office for refugees

People – without data protection?

s

i

x

a

right

P

right

e

i.e

s

and

A

As part of consultations with the State Office for Refugee Affairs

(LAF) informed us that the Senate Department for Integrity

ration, work and social plan, a complaints office independent of the LAF

to create for refugees who have "low-threshold" complaints about

the facilities and operations related to the accommodation

should accept. In view of the extensive

The LAF asked us to process personal data about the refugees

for advice on data protection law.

The plan is, in addition to the official and residential

internal complaints system to create an additional complaints office

intended to be operated independently outside of shelters and government agencies

neutral and low-threshold contact point for those affected. On the one hand, this

Complaints office offer consultation hours and on the other hand through so-called integra

tion guides offer advice directly in the facilities.

There are still essential questions about the establishment and, in particular, about the legal nature

of the planned complaints office were open, we initially put the LAF on the

legal problems of the processing of personal data by private

informed third parties in the context of the performance of state tasks and

these concerns also at management level towards the Senator for Labour,

integration and social issues. In particular, we have problematized that

quality assurance is a state task, which is also

can only be carried out by a state body such as the LAF. The

The task cannot simply be assigned to a private third party like the one planned

Complaints office can be transferred. We have asked several times for us

further information on the legal classification of the complaints office





to let men. Unfortunately, we have the requested information from the Senate

administration but not get. After several months, it came in the fall

for a personal discussion on a technical level with the participation of the co-

Ordinance office for refugee management of the Senate Department and the LAF.

We made it clear that we would support the Senate Administration

the approach followed when setting up the complaints office, the inhibition threshold for

the residents of the facilities to deal with a complaint

to turn to a state institution, to disparage as much as possible, very much

can understand well. We were also able to

tion of the complaints office related data protection difficulties

clarify. However, on the part of the Senate administration, we were

informed that the creation of an authority-independent complaints office

is intended, without the existing legal instructions and

touching on responsibilities. It is therefore not planned at the moment, the tasks

of the complaints office to be enshrined in law. The use of the complaints office

the Senate administration has been involved in a pilot project in ours since 2018

authority was not involved, tested. The knowledge gained from this

tures should be used in 2020 for the complaints office now

to establish permanently.

We have explained that in the absence of a statutory assignment of tasks for the

Complaints office also the processing of personal data of the residents

residents cannot rely on data protection regulations,

but only on consent. However, since a declaration of consent is only

is effective if all data processing processes are precisely

are mentioned, a variety of practical problems arise.

In particular, practical problems are to be expected when feedback

gene from a statutory complaints procedure, e.g. at the LAF

or in connection with objection proceedings at the district social

offices to which independent complaints bodies are to be addressed. in case of

about third parties, e.g. with regard to any assaults by roommates

or roommates or the staff of the facilities or by security

heitsdienste, their data could not be based on the consent of the

complainants are processed. The independent complaints body

113

could then not take action, but would have to report to the state authorities

point.

We pointed this out and recommended the tasks of the complaints office

to be enshrined in law in the future. have concrete suggestions

we also submitted. We discussed this intensively with those involved.

Since there is political will to also use the complaints office for

difficult to open to homeless people should be checked at an early stage,

how a legal anchoring of this position could be implemented. the consent

From our point of view, a solution should only be taken in view of the great time pressure

considered as an interim solution for the start of the complaints office

become.

The Senate Department for Integration, Labor and Social Affairs and the LAF will

the planned tasks of the independent complaints office based on the

review the aspects discussed. We assume that the still to be

winding declarations of consent are submitted for review. The

opportunity shows that if our authority is involved at an early stage,

data protection requirements for setting up the complaints

could have been taken into account from the outset without valuable

full time would have elapsed. We assume, however, that the started

constructive exchange is continued and the establishment of the

continue to support the difficult point in an advisory capacity.

7.2

Census of homeless people in

Berlin – “Night of Solidarity”

At the beginning of the year, the Senate Department for Integration, Labor and Social

ziales for advice on a project to count living

clueless people approach us. From the documents sent to us

the specific course of the project was not clear, we

natsverwaltung initially offered discussions on a technical level in order to open

To clarify questions and to accompany the project from the beginning. As part of a

114

s

i

x

a

right

P

right

e

i.e

s

and

A

Chapter 7 Integration, social affairs and work 7 2 Count of homeless people in Berlin - "Night of Solidarity"

meeting in May we discussed the data protection aspects of the project

discussed and asked to consider our suggestions in further project planning

considerate and promptly provide us with the necessary information for our

lay to forward. Following this conversation, we were given the necessary

Unfortunately, no data protection concept was presented. Only in October and after

the Senate administration had set up a completely new project group

contacted us with a request to meet again. After these initial difficulties

However, the data protection aspects to be taken into account could then cause problems

technical level can be discussed constructively.

Since the Berlin Senate only estimates the current number of

street people are available, these should in future regularly with the help of

volunteers in the entire city area are counted in one night.

A first count is planned for the night of January 29th to 30th, 2020.

The background to the census is that homeless people benefit from the existing aid

system have so far only been insufficiently achieved. Based on the determined

In the event of emergencies, qualified planning of the offers of help for the homeless should be carried out

people are enabled.

In addition to the count, the Senate Department wants those on the street

people encountered also collect data. It is planned that the residential

loose people from the helpers involved in the count

receive a questionnaire in their native language.

Participation should be voluntary. Based on the questionnaire, the residential

information on gender, age, nationality,

asked about the duration of the homelessness and, if applicable, about the marital status. This

so-called survey characteristics are - as far as possible - broadly defined or in

divided into categories. When specifying the age, the answer options should

ties to age groups (e.g. "21 to under 25") and in the case of nationality to the

Categories "German", "other EU" and "other" be limited. names and

Dates of birth are not requested.

The mere counting of homeless people on the street is data protection law-

This is not a problem, since no personal data is processed here

become. When processing the data from the questionnaire, the Senate

administration, however, ensure that identification of the individual

115

asked people is not possible afterwards. Although this is already through

makes it difficult for neither name nor date of birth to be processed. But also

the other information must not be used to draw any conclusions about the respective residential

enable clueless people. Furthermore, the persons questioned must later

testing prior to the survey about the associated data processing

ments and that participation is voluntary.

The planned project of census and survey of homeless people

in Berlin is a concern of the Senate that is worth supporting with regard to the

Improvement of the personal situation of the persons concerned and

Combating homelessness in Berlin. Nevertheless, data protection

legal aspects are taken into account during implementation. We will

continue to accompany the project to ensure that the personal

related data - insofar as their collection is necessary at all - data

be processed in a protective manner.

7.3 New ID - Old Photo

s

i

x

a

right

P

right

e

i.e

s

and

A

A citizen told us that she had contacted the State Office for Health and

ziales (LAGeSo) applied for the issuance of a severely handicapped pass

and sent a current passport photo. Then the LAGeSo gave her one

Severely handicapped pass sent, which instead of the current passport photo of the

Citizen with a 25-year-old photo of her was issued.

It turned out that it was a passport photo that the

Gerin had submitted to the pension office a few decades earlier to get her

to exchange an old GDR severely handicapped ID card. We tried that

Clarify the matter with the LAGeSo. As a result, it must be here

have acted around an unusual individual case, in which the old photograph

probably since the 1990s in the severely disabled case of the citizen in the

chiv "slumbered". Apparently, when the new ID card was issued, it wasn't

noticed that the photo was no longer up-to-date.

As part of the examination of the individual case, we were able to determine that a

recurrence of such a case is unlikely. At the exhibition of



Severely handicapped ID cards, the photos will be sent immediately after notification

digitized, the photo will then be destroyed immediately. The digitized data

tei is regularly automatically deleted after four weeks.

The LAGeSo took the matter as an opportunity to contact us

to coordinate a procedure that, in the sense of customer orientation, includes written

With the consent of the applicant, the storage of the photo for the

Duration of ten years provides for the processing time at the issuance

of a new or lost ID card. Against

the declaration of consent, there are no data protection concerns

ken, so that we contribute from a normally data protection-compliant procedure

the issuance of severely handicapped ID cards.

7.4 Do health insurance cards belong in the

social security record?

A citizen complained to us about the fact that the social welfare office from him at the

Applying for social security benefits Copies of his identity card

and the electronic health card from his health insurance company

had.

The social welfare office admitted the facts and informed us that the presentation of the

son ID was necessary for identity verification. The template of

electronic health card from the health insurance company was required in order to

Check health insurance information. The request

the copies served the purpose of a personal visit to the social welfare office

to avoid.

A

and

s

i.e

e

right

P

right

a

x

i

s

In accordance with data protection law, the social welfare office is entitled to

to demand the presentation of an identity card. In any case, this applies

when benefits are requested for the first time. Not covered by this power

is, however, the storage of the documents in the service file. Because after

The following identity verification is the identity card to check the claim

not relevant anymore.

117

The need to present the electronic health card of the health

checkout we could not understand. It is sufficient if the name of the

Health insurance and the insurance number are named in the application form

the. In the specific case, the complainant received a disability

pension, so it was to be assumed anyway that the contributions for his social

insurances are paid directly by the pension provider and insofar as one

Knowledge of the data on health insurance would hardly have been necessary

should.

We have informed the social welfare office about our legal assessment and this

requested to establish a data protection-compliant procedure for dealing with personnel

documents and electronic health cards. the social

office has assured us that the procedures involved in receiving the application and

adapt to further processing according to our specifications.

118

Chapter 7 Integration, social affairs and work 8 1 Extent of information requests from employees

# 8 Employee data protection

## 8.1 Scope of the request for information from employees

The complainant was co-managing director of a Berlin company men. After her departure, she asked the company to provide her with information about their personal data. This particularly affected her Emails (including those sent after she left) since they are her E-mail address also used for private purposes. The company also post no information for a quarter of a year.

A

and

s

i.e

e

right

P

right

a

x

i

s

We have identified a violation at the company. The responsible che is legally obliged to inform the data subject within one month after receipt of an application certain information is available

97 The company did not comply with this obligation to provide information in good time after. However, the right to information does not grant a comprehensive right to

Release of all communications sent via a company’s email system

company.

A complete release of all emails from the company's system,

in which the complainant's name appears is for that reason alone

not possible because the right to issue a copy of the data98 by the rights

and freedoms of other persons is restricted.99 In the

Numerous other people showed up for the email communication requested

(in particular other employees of the company and external parties) so that

extensive conclusions about personal data of third parties are possible here

would have been, in which the complainant also had no specific interest

eat had presented. Furthermore, with a comprehensive publication

knowledge of internal processes, company secrets and

97 Art 15 para 1 and Art 12 para 3 sentence 1 GDPR

98 Article 15 (3) GDPR

99 Art 15 Para 4 GDPR



know-how of the company or of companies affiliated with it

been bound. This conflicted with legitimate corporate interests.

As a result, the data from conversations that the complainant

to the permitted extent for private purposes, to her

ben. However, the purely business-related correspondence was due to the

termination of their employment relationship is not a legitimate interest of the

defuhrin (more) to accept.

Former employees are fundamentally entitled to have their private

to receive personal emails.

8.2 Deletion of data after the end of the

employment relationship

s

i

x

a

right

P

right

e

i.e

s

and

A

One employee had a termination agreement with her employer

termination of employment. This one contained the

Obligation of the employer, no later than six weeks after the end of the

employment relationship, the profile of the employee on the website of the company

to delete. The Complaints Office received confirmation of this deletion

leader a little later. In the time that followed, however, she realized that

luck to find her CV on the company's website

was. After she had lodged an objection to this, the company

these links will be deleted immediately.

Notwithstanding any consent given by the complainant

during the employment relationship the processing of her life

is inadmissible in any case after the end of the employment relationship. That is

the DS-GVO does not know a period of validity of a consent, but is subject to it

also the processing of personal data on the basis of consent in

within the framework of an employment relationship, the requirement of earmarking.100

Considering this requirement, it must therefore be assumed that

100 See Art 5 Para 1 lit b GDPR





consent to the publication of a curriculum vitae for the period of

employment is limited.

Personal data of employees are after the end of the work

to delete the employment relationship immediately if it is no longer required

or the data subject has withdrawn consent.101

## 8.3 Deletion of applicant data for the judiciary

A

and

s

i.e

e

right

P

right

a

x

i

s

The Senate Department for Justice, Consumer Protection and Anti-Discrimination

planned to increase the retention period for the selection notes on rejected applications

applicants for the post of judge from originally ten years

limited to five years. Which was still very long retention periods

with the peculiarities of the Berlin procedure for selection and recruitment

justified by judges. This comes as an independent organization

gans to the administration of justice a prominent role, which is why the decision

for a specific person in the selection process on as complete a

permanent factual basis is to be met. In this respect, the Senate administration

tion necessary for a selection decision, provided that female applicants

and applicants had previously applied, previous decisions

to include. This can be used to determine whether previously recognized deficits

continue to stand in the way of a positive selection. In view of the limited

th number of case situations discussed in the selection interviews would

rejected applicants also through prior knowledge from early

job interviews a significant competitive advantage over other

whose applicants receive that also against the background

of data protection hardly in accordance with the constitutionally guaranteed

Performance principle102 is to be brought.

101 See Art 17 Para 1 lit a and b GDPR

102 See Art 33 Para 2 Basic Law (GG)



Pursuant to Section 26, Paragraph 1, Clause 1 of the Federal Data Protection Act (BDSG)103, applicants may

Training documents are only stored for as long as this is necessary for the decision

about the establishment of a specific employment relationship

is. However, the data should be available for a new hiring decision

following a negative decision on the establishment of an employment

contractual relationship. Another retention of data

of those affected in connection with an unsuccessful application, however

regularly only to justify the decision not to be hired, e.g.

in the context of a lawsuit based on the General Equal Treatment

law (AGG), permitted.104

In addition, a retention period of five years would be disproportionate. Five

Years-old application documents and interview logs or assessments

genes have no or only a very limited meaning, because they do

after a short time there is a personal development of the applicant

or the applicant conceivable.

Due to the special features of applications for the office of judge, we decided

with a storage of the selection notes for one on the absolutely necessary

agreed to such a shortened period of up to two years.

We have the Senate Department for Justice, Consumer Protection and Anti-Discrimination

asked to carry out an evaluation after two years as to whether this

retention period is actually required.

Data from rejected applicants is fundamental

after the end of the selection process and after the deadlines for

gene to delete. However, special features in individual cases must always be taken into account

and to take into account.

103 In this respect, the German legislature has relied on the opening clause of Art. 88 GDPR

Made use of and thus carries out the special legal regulation of § 32 BDSG

old version continued

104 See Art 17 Para. 3 e) GDPR

8.4 Internal WhatsApp Group

One complainant's employment was terminated without notice. The

Termination became public because the letter of termination from the manager

rer photographed and in a WhatsApp group chat of the company, the

is used for coordination, has been published for all employees to see.

It was clear from the letter of termination that the complainant

Loan granted by the company to meet private payment obligations

to balance gene. Upon request, the company informed us that the business

fuhrer accidentally put the letter of resignation in the WhatsApp group

set.

A

and

s

i.e

e

right

P

right

a

x

i

s

Personal data of employees may not be used for employment

contractual relationship are processed if this is necessary for the decision on the

Justification of such or after justification for its implementation or

termination is required.105

The posting or forwarding of a letter of termination to a

internal whatsapp group can hardly be necessary and is therefore regular

unlawful. In the present case, the fact that

it was an oversight on the part of the manager.

Incidentally, the use of WhatsApp in the employment relationship is also for

Coordination purposes in the company with specifications for employee data

protection, such as storage limitation and integrity and confidentiality106

hardly compatible and had to be stopped here immediately. Opposite the

we have therefore issued a warning107.

The use of WhatsApp in employment involves considerable risks

ken for the personal rights of employees and is therefore regular

inadmissible.

105 § 26 paragraph 1 sentence 1 BDSG

106 See Section 26 (4) BDSG in conjunction with Art 5 GDPR

107 See Art 58 Para 2 lit b GDPR



8.5 Notes on operational procedures

integration management

s

i

x

a

right

P

right

e

i.e

s

and

A

As part of a process for operational integration management

(BEM), together with the company doctor, came up with a proposal for a solution

employees, which is later discussed in a case discussion

was discussed in accordance with the works agreement. This conversation was recorded

collided. However, the corresponding protocol was missing when the files were inspected

the employees. When asked, she was informed that a corresponding

Protocol does not exist or has not yet been released and incidentally also

would not be part of the BEM file, since these are handwritten notes of a

nes BEM participants act and therefore an inspection is not granted

that could. On the other hand, the person concerned turned with her complaint.

According to the DS-GVO, the person concerned has the right from the person responsible

to request information as to whether personal data concerning you

will be or were working.108 The person responsible has in particular one

Copy of the personal data that is the subject of the processing

were to be made available to the person concerned or, as in the present

the case desired to allow inspection of the data.109

According to a decision by the Federal Administrative Court, notebooks, daily

booklets etc. no personnel processes, insofar as they are due to individual

approval of the owner of the booklet for the exclusively personal

personal use, even if their content is official

has.110 The only prerequisite or condition for the management of such

Notebooks or notebooks with personal notes are one after this decision

secure storage against access by third parties or other persons (e.g.

colleagues, cleaners, etc.).

108 Article 15 (1) GDPR

109 Article 15 (3) GDPR

110 Judgment of the Federal Administrative Court of October 19, 2005 − 1 D 14 04





In the present case, handwritten notes of a participant were

prepared in a so-called discussion meeting. These were intended for service

Necessary, because without written fixation or without protocols measures or

Assistance not implemented specifically and correctly and those affected not

could be comprehensively informed about the outcome of the case discussion. A

only personal use is excluded. The refusal of insight

acceptance by the applicant was therefore unlawful.

After a brief exchange of letters, the company informed us that it now has

the complainant full access to the notes on the case

granted. Because of the violation, we issued a warning

chen.111

Employees have a full right to knowledge or insight

inclusion in records and documents containing personal data about them

included - both in electronic and paper form.

111 See Art 58 Para 2 lit b GDPR



9 economy

9.1 The Perpetual Tenant File

s

i

x

a

right

P

right

e

i.e

s

and

A

The first German fine under the General Data Protection Regulation (GDPR)

in the millions we imposed on Deutsche Wohnen in October 2019

SE, the second largest German real estate company. The reason was the

increasing storage of countless documents that are required for the implementation of rental

do not contract at all or after the expiration of accounting

currency periods were no longer required.

During an on-site inspection at Deutsche Wohnen SE in June 2017,

fall that the archiving system set up by this company also

contained documents that should not have been filed there from the outset

or whose retention period had already expired. For example, the

preservation of copies of identity documents or employment and training

contracts for the execution of an ongoing tenancy is not required

lich and therefore also not permitted. We informed the company afterwards

to the examination at that time that the system provided was not the applicable one

corresponds to the legal situation and must be corrected. Deutsche Wohnen SE

after initial hesitation, agreed at the end of 2017 to illegally store

to remove certain documents and subsequently presented a concept for this,

which is significantly based on a review of the stored documents in a

automated procedures.

In March 2019, we again subjected the database to a thorough on-site

the test to tell us about the success of Deutsche Wohnen SE's approach

to convince. We had our doubts about the company that the planned

procedure would lead to a complete cleansing of the database,

communicated a year earlier. However, it turned out that the company

do not delete a single document at the time of the check, only

started with some preparatory work. Earliest in summer

2019 should actually start with the deletion of the illegally stored data

to be started.

126

Chapter 9 Economy 9 1 The eternal tenant file

So we had to realize that Deutsche Wohnen SE had more than one and a half

years after the first examination and more than nine months after the validity of the DS

GVO neither carried out the deletion nor determined the data to be deleted,

only created the conditions for fulfilling the obligation to delete

had.

These requirements include, in particular, storing the data in a

System that has a function for deleting selected documents

adds. Deutsche Wohnen SE had expressly configured its archive system in such a way

let it be known that it was not possible to delete individual documents. she led

indicated that this was necessary for reasons of revision security. However, this is

not the case. Commercial and tax law only requires that certain

documents are kept unchanged for a legally fixed period of time. After

At the end of this retention period, deletion must take place, if not in

There are special reasons against it in individual cases. An archive system must therefore

be constructed that the legally required deletion processes also required

tene do not affect the further storage of more recent documents. This is without

More is possible with systems that have been available on the market for years.

In addition, as part of the purchase of real estate, Deutsche Wohnen SE

documents handed over by the previous owners were scanned en bloc for years

and saved the trouble of sorting out documents for safekeeping

no longer had a legal basis or had never existed before. This form

the data transfer was already inadmissible under the old legal situation. the German

schen Wohnen SE was this inadmissibility by our notice at the latest

known since 2017. It is all the more surprising that we

ten state in 2019. We were only introduced

the software solution that should do the sorting in the future.

At the same time, it became apparent that - as tests by the company had shown -

this software solution does not recognize all documents to be sorted out

would, however, manual verification in cases of doubt

wasn't planned.

The DS-GVO requires those responsible that - when determining the co-

Tel of the processing and at the time of its implementation - technical and

take organizational measures to ensure compliance with data protection



to ensure principles. One of those principles is that data only

lawfully and to the extent necessary for the respective purposes

be killed If these purposes and any storage obligations are fulfilled, then

must be deleted. Since Deutsche Wohnen SE has been such for a long time

has not taken necessary measures, we have this violation against

the requirement of data protection punished by technology design.

A sprawling storage practice cannot because of supposedly existing

obligations to retain personal data are justified.

Even large companies that have a large number due to their business model

of data must process the possibly high effort for the ca-

categorization of this data, creation of technical conditions

to enable the legally required deletion and for the implementation

accept existing deletion obligations. The creation of "data cemetery

fen", as in the present case, regularly does not meet the requirements

to technical and organizational measures, the implementation of which

GMO for the protection of those affected, and does not constitute any legal

moderate processing of personal data.

9.2 Please smile! – access to coworking

Clear only after photo shoots

Guests of users of coworking spaces112 were only granted access if

if they let themselves be photographed during registration. These photos should of

Registration of visits, averting danger and preserving evidence.

The recordings were saved for 30 days.

Guests of users of coworking office space had to find out about a

a permanently installed tablet computer as a registration app

Register visitors. This app asked both the names of the

s

i

x

a

right

P

right

e

i.e

s

and

A

112 The term coworking describes the sharing of workspaces with corporate

strangers In the so-called coworking spaces, one usually rents individuals

desks for short periods of time. Mainly freelancers and start-up companies

men use this concept





guests as well as the names of the people with whom they are registered

should. The app then started the front camera and took a picture of the

respective person. Only after completing the registration process

Guests are picked up at reception. Were saved next to the name of the

guest and the host person also the reason, the date and the time

of the visit and the photo of the guest.

Processing of the personal data of visitors

chern is only lawful insofar as it protects the legitimate interests of the

or the person responsible or a third party and unless internal

interests or fundamental rights and freedoms of the persons concerned

weigh.113 In the present case, a frictional

loose visit registration, a preventive defense against danger and a subsequent one

Evidence to be considered. However, taking photos of the visit

visitors are not required for these purposes. There was right away

tive but less intrusive measures to achieve the desired result

to achieve.

On the one hand, the transmission of the visitor's name already guarantees

te that this is the invitee. On the other hand, they will

Guests also picked up at reception. This ensures that hosts

only let in visitors who you know personally

to a previous invitation. Incidentally, through the template

A photo ID will be used to ensure that the attendee is present

person is the person actually registered.

Upon our intervention, the person in charge of the office space rental has that

procedure turned off.

The creation and storage of photographs when registering

searchers and visitors is unlawful, since milder, equally suitable means

tel are available to ensure a smooth registration.

113 Art 6 Para 1 lit f GDPR

129

9.3

Collection agency: Personal

change is not excluded

After an address query for an

forward the data of a complainant, although neither her current

schrift nor their previous address with the billing and delivery address of the

identical debtor matched.

s

i

x

a

right

P

right

e

i.e

s

and

A

The collection agency was from a company with the collection of a

open claim from a goods purchase contract has been commissioned. In this

It had context, among other things, surname, first name, date of birth, current address

and delivery address of the debtor of the claim. This was first

by e-mail and then by post to the delivery address for payment

asked about the open claim, but did not respond. Two more to the

Letters addressed to the delivery address could not be delivered by Deutsche Post

become. The debt collection company therefore applied, stating the known

Address data a request for the current address of the debtor in the case of an

future egg.

However, the answer given by the credit agency included the address and the

Previous address of a person with the same name, namely that of the complainant

included - naturally, both statements did not agree with the debt collection

already available address information. The Credit Bureau

However, the information was expressly subject to a so-called identity reservation

placed. Despite this, and without further examination, the collection agency demanded

from the complainant now the settlement of the claim against the

debtor.

Although companies can in principle use collection agencies to assert

commission the correction of existing claims from a contractual relationship

and are allowed to provide them with the necessary personal

transmit personal data of debtors. Based on the same legal

basis, debt collection companies can use the data required for the fulfillment of their

additionally required data, e.g. a new address, by requesting a

collect credit reporting. If, on the other hand, the claims are passed on to a collection agency



men assigned (factoring), this becomes your own contractual partner

the respective debtors and must have its data processing

based on another legal basis.114

The use of the complainant's address violated the specific case

however, against the legal requirements. Since the complainant

was not the debtor of the claim, the debt collection company could

objectively already with regard to the processing of your personal data

have an effective legal basis.

Personal data that are processed must be factually correct.115

From this follows the obligation of each responsible body, through appropriate

organizational and technical procedures to ensure that identity

changes are excluded. In the present case, the collection agency had

fails to develop and implement appropriate testing processes.

The collection agency has informed us that it has changed its procedure for

have changed in the meantime to avoid a mix-up of persons. Since

the changeover could result in a new address from a query at a credit agency

only be used if one of the prefixes from the address query

with the already known address of the debtor

agrees.

Companies may only process factually correct data and are

is obliged to use suitable technical and organizational procedures to ensure

ensure that confusion of identity is excluded. information

from information with a reservation of identity must never be made without careful

examination can be used in individual cases.

114 Art 6 Para 1 lit b GDPR

115 Art 5 Para 1 lit d GDPR



9.4

“Pot Secret” makes everything public

s

i

x

a

right

P

right

e

i.e

s

and

A

Since January 2019, citizens have been able to use the “Topf Secret” platform

the protocols of official hygiene controls of catering establishments such as

Request restaurants or bakeries. Total were about the platform

nearly 50,000 applications submitted. The project was funded by the consumer organization

Foodwatch e. V. and the operator of the FragDenstaat internet platform

sam initiated.

The application is made on the basis of the Consumer Information Act

zes (VIG), on the basis of which each person independently submits a request to the

competent authority.116 However, the platform not only wants to

facilitate carrying position for individuals, but the correspondence and

Also publish hygiene reports to create transparency.

If you want to submit an application via the platform, choose via the integrated

Map of OpenStreetMap117 from a restaurant. Then you have to

sen the own name and address are given. The platform

generates an individual e-mail address for each request, to which the answer

go to the authorities. If a requested authority responds by email,

these answers will be automatically published without attachments, some data

also automatically blackened. All further correspondence must die

Activate the applicant first or upload it yourself. You will

asked to make personal data unrecognizable in this context,

which enables them technically on the platform through an application program

becomes light.

The platform processes data from three groups of people: The first

are the applicants themselves, the second are the holders of the

often very small catering establishments and the third group the clerical

tend in the authorities to which the inquiries are addressed.

116 § 1 VIG

117 OpenStreetMap is an online city map that is also used as a geoinformation

system This also includes the addresses of many catering establishments

listed

132

Chapter 9 Economics 9 4 "Pot Secret" makes everything public

Our test initially dealt with the redaction program used:

This program is able to independently edit some formulations in the

Recognizing emails, such as "Dear...", and in this case automatically

to redact the name that follows. The documents that the

However, applicants and the e-mail attachments must be uploaded

redact yourself with the provided program. The platform points this out

very clearly. Despite this, in some cases these documents are not or

not sufficiently anonymised.

Since the platform is an online service, first of all is like this

it can be assumed that the people who upload the documents are responsible for the

are responsible. The providers of the platform are only then responsible for the

Responsible for content if you become aware of it - e.g. by clicking on it

informed.118 In this case, they must

care. We could not determine a systematic violation here, since

the platform when they become aware of insufficiently redacted documents

was made, this in the cases known to us within a very short time after

fetched, sometimes within a few minutes.

The inquiries themselves cannot be made anonymously, as VIG uses these

submissions are required.119 The only option on the platform is to opt out

decide to have his name displayed publicly by the user

a tick next to the statement "I don't want my name published"

light will" (opt-out). This does not constitute consent within the meaning of the GDPR

dar. Because consent is only given if an active decision for a

data processing is carried out. This would be the case, for example, if there was a tick in front of

the sentence "Yes, I would like my name to be published" (opt-in).

can be. However, the platform has set itself the goal of having one if possible

transparent dialogue between citizens and the state

promote jobs. Within the framework of this concept, it can still be

be considered appropriate to also publish the names of the applicants.

Nevertheless, clear information is missing here, when and where exactly the names

to be published. At present, it is not initially pointed out that in

118 § 10 Telemedia Act (TMG)

119 § 4 para. 1 sentence 3 VIG

133

As a rule, the inquirers are named on the website. We have-

asked the platform to insert such a note, because responsible

literal are required by law to process personal data in a manner for which

to process the data subject in a comprehensible manner and to be transparent about this

rent120 so that they can exercise their rights in a comprehensive manner

can perceive. Even if the users have decided to

not to publish, it can happen that these are in correspondence with

are not accidentally made unrecognizable by an authority before the docu-

be uploaded by the applicant or the platform. Also

the platform must expressly point out this risk.

Incidentally, there was no current data on the platform at the beginning of our

privacy policy published. Upon our notice, the statement

updated, in particular it now refers to the rights of those affected.

Complaints that reached us because the authorities required the disclosure of control

reports refused, but we could not follow up. Our

authority can, in VIG matters – in contrast to the Berlin information

tion freedom law (IFG) – do not mediate because the VIG does not have an arbitration board

and us this function by the state legislature only in relation to the IFG

was transferred.121 However, we have the authorities in the respective cases

pointed out that in principle no personal information is required from applicants

white copy may be requested.

The platform "Topf Secret" has taken some steps to

equal between transparency and data protection. What the transparency

As far as data processing is concerned, improvements are still required.

120 See Art 5 Para 1 lit a in conjunction with EC 39 GDPR and Art 12 Para 1 in conjunction with EC 58 GDPR

121 § 18 IFG



9.5 Hello Prohibition of Pairing

The company HelloFresh has added to its service when registering online

requires that with a single tick of the data protection declaration, the general

my terms and conditions and contacting Wer-

purpose is approved at the same time.

A

and

s

i.e

e

right

P

right

a

x

i

s

Collecting consent in this form is illegal. Then

consent is only effective if it is given voluntarily. voluntarily means

that one can decide for or against something without suffering disadvantages

the. In other words, consent must not be a condition for something

be made, which can be separated from other processes.122 In this case

it must be possible, for example, to order groceries without having to

understanding of the use of the personal telephone number for contact

to explain.

This ensures that the processing of personal data in order

whose consent is sought, not directly or indirectly in return for

can become a contract. Consent and contract are

two different legal bases for lawful processing

personal data. These two legal bases must not

be guided, their boundaries must not become blurred.

To assess whether such improper bundling or linking exists,

it must be determined what the scope of the contract is and what data for

the performance of the contract is necessary. Consent to the telephone

Contact for the purpose of advertising was here for the provision of the contract

trags, delivery of groceries, not required. A delivery can

can also be made to people without a telephone. This consent was therefore

lawfully linked to the performance of the service.

122 See Art 7 Para 4 GDPR, EC Nos. 42 and 43 GDPR

135

We were able to obtain consent to be contacted by telephone

has been removed from the box text. Consent to the te-

Telephone contact for advertising purposes obtained separately.

Consent to a data not required for the performance of a contract

Data processing must not be made a condition of the contract.

9.6 Asset Deal Customer Data

s

i

x

a

right

P

right

e

i.e

s

and

A

The sale of individual lines of business, assets,

product lines or services of one company to another company

business (asset deal) is part of day-to-day business in the economic sector. who in

ways of an asset deal only individual assets of a company

usually also has a great interest in acquiring the associated

existing customer data in order to purchase goods or services from the company

business branch to be able to continue to offer customers.

The sale of customer data in such case constellations is a data

processing, the legality of which is determined by the DS-GVO.123

Customer data may be passed on if an effective consent

ment of the customer to transfer the data to the acquiring company

company.124

In addition, data transfer can also be justified if it is used to

tion of legitimate interests of the person responsible or a third party

is.125 In doing so, it must be examined to what extent the interests of customers that are worthy of protection

customers oppose such a data transfer.

123 See Art 4 No 2 DS-GVO for the definition of personal data and Art 6 Para 1

DS-GVO on the legality of data processing

124 Art 6 Para 1 lit a GDPR, Art 7 GDPR

125 Art 6 Para 1 lit f GDPR





The conference of the independent data protection supervisory authorities of the federal and

of the federal states (DSK) has made recommendations for uniform administrative practice

says goodbye and agrees on a catalog of case groups that

the legally prescribed balancing of interests in an asset deal.

can be pulled.126

It must be examined in each individual case whether a transfer of customer

data is compatible with the purpose for which the data was originally collected. loading

if there is no compatibility or if the data is sensitive127, a way

Delivery only on the basis of the informed consent of the customer

customers possible.

In the other cases, the following applies: A transfer of customer data for the purpose of

Continuation of current contracts can be justified if the customers

Customers their civil law approval to take over the contract or the

Obligations from the contract by the acquiring body according to or analogously

to Section 415 of the German Civil Code (BGB). Such a civil law

che approval can regularly also be used as data protection consent

for the transition of the necessary data128, but also as for

Fulfillment of contract required129 or permitted on the basis of a weighing of interests

be sig130.

The same applies to cases in which customer data in connection with open for-

are to be transferred to a purchaser.

Here, too, the admissibility is initially based on the provisions of civil law

126 DSK resolution of May 24, 2019: “Asset deal – catalog of case groups” (https://

www datenschutz-berlin de/infothek-und-service/veroeffentlichungen/decisions-

se-dsk/); Note: The decision was made by the Berlin Commissioner for Data

Protection and Freedom of Information (BlnBDI) and the Saxon Data Protection Officer

ten rejected The BlnBDI informs the resolution under number 2 “existing customers without

current contracts and last contractual relationship older than 3 years"

sung, according to which a transmission and use of this data for purposes of legal

retention periods should be permissible, and represents the ab-

yielding legal position

127 See Art 9 GDPR

128 Art 6 Para 1 lit a GDPR, Art 7 GDPR

129 Art 6 Para 1 lit b GDPR

130 Art 6 Para 1 lit f GDPR

137

provisions of the assignment of claims131. If, from a civil law perspective, a transfer

transfer possible and an assignment of claims not by agreement

excluded,132 a transfer of the claim in connection

communication of customer data also be permissible under data protection law133.

Data from customers in the advanced stages of initiating a contract or

of existing customers without current contracts, whose last active

tive contractual relationship no longer than three years ago can get in the way

of the objection solution (so-called opt-out model). are there

to inform all those affected in advance about the planned sale and they are

a reasonable objection period of at least six weeks

should, concede. Unless an objection is declared, the transfer of

respective data to the buyer is permitted.134 In the event of an objection

claim, the data may not be passed on to the purchaser

be practiced

A transmission of the data of existing customers for whom the

last active contractual relationship was more than three years ago, to an acquisition

However, in principle, it is not permitted to be a member or an acquirer. For such

There is already a legal obligation, independent of the application, of the original

original company to delete, provided this data is relevant for the purposes for

which they were collected or processed are no longer necessary.135 A further

Further processing can only be carried out in accordance with Art. 17 Para. 3 DS-GVO, such as

on the basis of legal obligations to fulfill tax or

commercial obligations may be permissible. It is in each case in each case

to obligations of the original company, which are not based on an

advertising position are transferrable. For this reason, the transmission is such

Legacy data to purchasers is not permitted under data protection law.

Especially not according to § 399 2 Alt BGB

131 See §§ 398 ff BGB

132

133 On the basis of Art 6 Para 1 lit f GDPR

134 According to Art 6 Para 1 lit f GDPR

135 See Art 17 Para 1 lit a 2 old GDPR



Chapter 9 Economy 9 7 Businesses: Ensure processing of inquiries from data subjects!

The transfer of customer data to the purchaser

In the case of an asset deal, a company can in certain case constellations

may also be permitted without the consent of the customer. Included

However, it must always be carefully checked whether a transfer with the purpose of

original collection of the data is compatible and whether its proprietary

contrary to the interests of customers.

9.7 Business: Handling Inquiries

Ensure affected person!

In complaints procedures, the responsible bodies often raise the objection

brought, data subjects had their request for information, correction,

Deletion or assertion of an advertising objection or its revocation

of consent not to the person responsible within a company

body and for this reason a timely answer I

Your request or your request cannot be implemented.

A

and

s

i.e

e

right

P

right

a

x

i

s

The addressee when asserting the rights of data subjects is according to the GDPR

the person responsible as such136. If the person responsible takes such a

If an application is accepted, it must be processed, even if there is a different internal

referenced distribution of tasks was determined. Even e-mails that are supposed to

Real spam accepted by the mail server, but in a spam folder

been moved and not read have been received.

A responsible body is obliged to use suitable technical and organizational

torical measures to fulfill their data protection obligations

genes.137 Through suitable internal organizational measures and

process flows is a forwarding to the company responsible for this

permanent position and correspondingly timely processing of inquiries

to ensure. Responsible bodies should check their effectiveness regularly

136 See definition in Art 4 No. 7 GDPR: "...the natural or legal person,

authority, institution or other body that alone or jointly with others over the

decides the purposes and means of processing personal data;..."

137 Article 24 (1) GDPR

139

check and, if necessary, make adjustments to the processes in order to

comply with their obligations.

Companies are always obliged to take appropriate measures to ensure

ensure that all incoming data protection inquiries also

reach the contact persons responsible for them in order to

comply with legal obligations.

9.8

Internet imprint: No use of

Data for advertising purposes!

s

i

x

a

right

P

right

e

i.e

s

and

A

Again and again we receive complaints from people who work for companies,

with which they have no connection, advertising in the form of letters,

receive emails or calls. As part of the hearings we carried out

responsible bodies often refer to information published on the Internet

clock data of the persons concerned and take the view that an additional

The use of advertising is permissible in such case constellations, since there is an interest

these people in the goods and services offered

if only because of the content of the data placed on the Internet by the person concerned

website or their professional group or their activity can be assumed.

Processing of personal data for advertising purposes

be lawful if they are used to protect the legitimate interests of the

responsible is necessary, unless the interests of the data subject

predominate.138 In principle, direct advertising can be a legitimate inter-

present the responsible body.139

The data given in the imprint is generally

accessible information. However, these are not voluntarily, but expediently

bound to fulfill the legal obligation to identify providers

according to § 5 Telemedia Act (TMG). Due to a lack of voluntariness and

138 Art 6 Para 1 Sentence 1 lit f GDPR

139 EC 47 GDPR





In view of the earmarking of the publication, the legally required

relevant balancing of interests regularly to the fact that the advertising use of the

type of data collected is inadmissible.140

In addition, the processing of personal data for advertising purposes

also inadmissible if the assessments of § 7 of the law against the

unfair competition (UWG). According to this standard, in particular

their advertising by fax, automatic call or "electronic mail" such as

E-mails, SMS or Messenger only with the prior express consent of

called person allowed. The same applies to telephone advertising to Ver-

consumers, including, for example, employed legal

lawyers belong. But even personal data

by traders may only be used exceptionally for telephone advertising

be det: Required is a concrete interest of the called person, the

justifies the assumption of presumed consent. The fact that

a certain type of company always needs certain services – e.g

Telecommunications – has is not enough.

In the case of existing business contacts, advertising can exceptionally be

nischer Post" without consent.141 However, contact details are only

taken from an imprint, these requirements can never be met.

A processing of personal data from an imprint

Advertising purposes is regularly not permitted.

140 See also point 4 3 of the DSK's guidance on the processing of personal

collected data for direct marketing purposes subject to the General Data Protection Regulation

ordinance (DS-GVO) (available at: https://www datenschutz-berlin de/infothek-

and-service/publications/orientation aids/)

141 Section 7 (3) UWG



9.9

Tax consultant activity in the payroll

attitude – no order processing!

s

i

x

a

right

P

right

e

i.e

s

and

A

The question of whether payroll accounting by tax consultants

Order processing is carried out or is carried out under one's own responsibility, was

therefore controversial and repeated subject of discussion in the working group

association of the DSK. With the new version of Section 11 of the Tax Advisory Act (StBerG)

the data protection classification of the activities of tax consultants

tax consultants as those responsible under data protection law

clarified by the legislature.

In practice, there were repeated discussions about whether tax consultants

tax consultants who take over the tasks of external payroll accounting

men, legally as contract processors or as themselves under data protection law

to be assigned responsibility.

Before the new legal regulation, we took the view that for

Tax consultants who regard themselves as responsible

hen for the processing of the personal data of their clients and

corresponding contracts concluded, no order processing contract

be required. If tax consultants are against it so far

subject to the instructions of their clients that one of

Order processing could go out was our earlier opinion

conclude an order processing contract.

With the new tax law, the legislator has now clarified

ensures that tax consultants or tax consulting firms

companies when providing services according to the StBerG as data

are to be regarded as persons responsible under intellectual property law and order processing

is no longer considered.

Section 11 (2) sentence 1 and sentence 2 StBerG has been reworded as follows:

“The processing of personal data by individuals and companies according to

§ 3 takes place without instructions, taking into account the professional duties applicable to them. the person

142

Chapter 9 Economy 9 9 Tax consultancy in payroll accounting – no order processing!

Sons and companies according to § 3 are in the processing of all personal

gener data of their clients responsible according to article 4 number 7 of the data

General Protection Regulation (EU) 2016/679."

Accordingly, personal data is processed by tax authorities

raters and tax consultants or tax consulting companies under beach

execution of the professional duties applicable to them without instructions. This also applies if

within the scope of their legal obligations, they provide commercial assistance in tax

provide goods and in doing so use personal data of their clients

work.

According to the explanatory memorandum to the law142, this also includes the “booking of ongoing

business transactions", the "ongoing payroll accounting" and the "preparation of the payroll

tax registrations", which are regarded as independent activities

the. The assistance of the tax consultants commissioned with the payroll accounting

Tax consultants and tax consulting firms will close afterwards

In the opinion of the legislature, an independent examination and

application of the legal provisions. tax advisors

Accordingly, consultants or tax consulting companies are involved in the provision

of services according to the StBerG will always be responsible for data protection

literal to look at.

Tax consultants or tax consulting companies,

who perform business-related tasks of external payroll accounting,

according to the new regulation of § 11 StBerG are always as

responsible for data protection.

142 BT-Drs 19/14909, p. 58

143

9.10 Retention of Customer Data upon Cancellation

a registration process

s

i

x

a

right

P

right

e

i.e

s

and

A

One company worked with a multi-stage registration process

its online platform, in which the e-mail address and password are initially

were asked and then, in three further steps, various additional

che data. Each step was completed with a "Save and continue" button

de. It was pointed out that the entered data was saved

be completed so that the registration can also be completed at a later

can be sen. The complainant had registered in the course of the

Data entry aborted. He later received an e-mail from the platform

shape.

If someone cancels a registration process, the continued storage

of the personal data entered is not readily permissible. That is

there is a legitimate interest of platforms, an interruption and later

to allow further resumption of the registration process. However is

it is not necessary for this to collect the data of all those affected who have passed the registration

abort process to save. Just the fact that a company is about

informed about the storage of personal data does not mean that

this is permissible.143

Therefore, an explicit button such as “Cancel

and delete data" are provided so that the request to abort the program

process can be expressed in a simple and unambiguous way.

Likewise, it should have an explicit button such as "Save data to register

to continue later”; the storage period is appropriate in this case

to be determined. If someone just doesn't continue the registration without

to click one of these two buttons, it must be determined from which time

of inactivity a termination is to be assumed. It also depends on

how long it takes to fill out the respective form, including any necessary

compilation of the requested information takes time. additional

is a reasonable period of time to cover, for example, spontaneous disturbances.

143 See also the focus report on address rental in 1 3

144



If a registration process is technically designed in such a way that a storage

Storage of the data on the server only after completion of the registration process

takes place, the problem of deletion does not arise. The server storage for

later continuation could then be offered as an option.

In registration processes, it should be used both for further storage and

also give appropriate buttons for canceling. A privacy

friendly alternative would be server storage only at the end of the

process.

## 9.11 Rules of conduct according to Art. 40 GDPR - A development report

Many companies complain that the regulations of the GDPR are very general

be kept mine. In practice, it is often difficult for them to assess which

specific data processing is permissible and what protective measures are required

are required.

In order to provide companies with assistance, the DS-GVO stipulates that

Associations can develop so-called rules of conduct that the responsible

authority.144 Such rules of conduct can only be

at national level or at EU level with the resulting EU-wide

Validity to be agreed and approved.

The aim of such rules of conduct is to comply with the provisions of the GDPR for individuals

Sectors and their typical case constellations to specify and so the

Simplify GDPR compliance for businesses. The regulators

therefore check in the approval process on the one hand whether the rules of conduct

of the GDPR are in line, but on the other hand also whether they are actually one

Clarification or simplification of the GDPR requirements for companies

works. Because therein lies the added value of such rules.

144 = Codes of Conduct, see Art 40, 41 GDPR

145

We expressly welcome the possibility of such rules of conduct. in the pra

However, xis shows that creating and implementing it is very complex

are. Notable simplifications for those responsible through rules of conduct

will therefore only arise in the medium term. We support the development

rules of conduct but to the best of their ability.

European guidelines

At the beginning of 2019, the European Data Protection Board (EDPB)

tending guidelines that cover both the content and the formal aspects

Define the requirements for the aforementioned rules of conduct in more detail.145 This provides

an important aid for associations in the development.

According to these guidelines, every association must have a so-called monitoring

set up or commission a position. Such monitoring points are in the DS

GMOs are planned.146 In addition to being controlled by the supervisory authorities, they should

ensure that the rules of conduct of the companies concerned also

be respected. The monitoring bodies require accreditation

by a supervisory authority.

Until the guidelines were passed, it was disputed whether the GDPR

mandatory provision of monitoring bodies for rules of conduct. We

share the view with the other German supervisory authorities

represented that the regulations of the DS-GVO also the approval of behavior
permit tensing rules without a monitoring body. However, we are the majority
been overruled by the European supervisory authorities. Therefore behavior
tenancy rules only come into force when a correspondingly accurate
there is a dedicated monitoring body for this. This means a significant
additional expenditure of time and money for the respective associations. However
there is the possibility of complaints from affected persons in the monitoring
to channel the information point.

145 Guidelines 1/2019 on codes of conduct and monitoring bodies according to the
Regulation (EU) 2016/679 (https://edpb europa eu/our-work-tools/our-documents/
smjernice/guidelines-12019-codes-conduct-and-monitoring-bodies-under_de)

146 Art 41 GDPR





Accreditation criteria for monitoring bodies

Despite European guidelines, every supervisory authority is legally obliged to
establish and approve criteria for the accreditation of monitoring bodies
publish.147 Before publication, these criteria must be dated
EDSA to be approved. The supervisory authorities in Austria and the United
Kingdom were the first to successfully complete this process
ben.

In Germany, the working group on economics of the DSK has set up a working group
in order to expose such criteria uniformly for all German supervisory authorities
to work. We played a key role in this work. The elaborated
Criteria were decided by the DSK in November 2019 and sent to the EDSA
forwarded for approval. We hope to publish the result soon

be able to.

First procedures

We held intensive consultations with the first associations. middle

At the moment two of these associations have 148 draft codes of conduct in their

respective industry and apply for approval. In doing so,

but shown that it represents a major challenge for the associations that

to design regulations in such a way that they provide concrete action for their members

represent relief. So far we have been able to do both approval procedures

not finish.

147 Art 57 para 1 lit p 1 old GDPR

148 ADM – Working Group of German Market and Opinion Research Institutes and Federal

tion of European National Collection Associations The latter is about

a European umbrella organization for industry associations of credit management and

Debt Collection Industry The Federal Association of German Debt Collection Companies eV is one

of the member associations

147

s

i

x

a

right

P

right

e

i.e

s

and

A

10 finance

10.1 Declaration of Consent of the Savings Banks

The German Savings Banks and Giro Association (DSGV) has a data protection

che declaration of consent drafted by all savings banks in Germany

has been used. This read:

"I would like to be advised individually and as precisely as possible, supported and informed about pro-

be informed about products and campaigns: I therefore agree that the

Sparkasse links the following data about me, jointly evaluates and

turns:

1. Personal data such as name, date of birth, marital status, occupation

2. Contact information, such as address, email and telephone number

3. Data on my creditworthiness, my financial situation, my willingness to take risks

business and my credit risk

4. Checking account, debit and credit card details, such as card number, balance, credit

frame, interest, sales (without purpose and recipient) or

comparable data

5. Custody, credit, leasing and deposit data, such as product type, balances, interest

rates, security developments, maturities and comparable data

6. Data from consultation and service talks, sales activities, documentation

mentations and questionnaires, savings bank financial concepts, product

checks, as well as comparable data

7. Statistical data assigned to me using general criteria

can be used, for example for the suitability of certain financial products

by age groups

8. Data from transactions brokered for me by the Sparkasse, such as decade

Bank depot, various forms of leasing and hire-purchase, building loan

and insurance contracts and similar transactions

9. Data from the network partners about products held by me, such as insurance

insurance, home savings contracts and financial services

10. Data about my use of digital offers that the savings banks and

Association partners each offer, such as call times of websites, apps or

Newsletters, clicked pages or entries and comparable data"



Chapter 10 Finances 10 1 Savings Banks' declaration of consent

In addition, the following notice was given:

"If you do not consent or consent at a later date

revoked, this will not affect our business relationship. We can

Then process your data to the extent permitted by law (e.g. for

fulfillment of contract). Also other consents and agreements with

us or third parties are not affected by this."

Several data subjects have asked us to verify the legality of the consent

to check statement. There were also complaints nationwide because individual

Savings banks had submitted pre-ticked forms to those affected and

individual employees had claimed in conversation that

Consent is required due to the Money Laundering Act (GwG) or the

Sparkasse can terminate the business relationship without a corresponding declaration

not maintained.

Since the DSGV is based in Berlin, we have the responsible supervisory authority

Negotiations with the association about the wording of the declaration of consent

tion and the manner of data collection. We managed to

to reach a viable compromise. This essentially contained the following

agreements:

• The DSGV sensitizes the regional associations and savings banks to

hend that the customers on the voluntariness of the consent

be advised; the employees of the bank

instructed not to change the declarations of consent through pressure or the wrong

to obtain a cal presentation of facts.

• The previously used declaration of consent will be carried out as quickly as possible

replaced by a new declaration of consent.

• The old declaration of consent lacked transparency for the customer

customers and customers who provide financial advice solely on a legal basis

is based and which can only take place with express consent. The

new declaration of consent is now formulated in such a way that for those affected

it is transparent to what extent the data processing is based on a legal

basis and from when data processing is only based on a single

consent can be supported.

149

• A joint consent to all ten points of the consent

agreement waived, those affected will in future be offered a joint

consent to points 1 to 9 is requested, for point 10 a

independent consent is obtained. This corresponds to the specifications

of EG149 43 sentence 2 DS-GVO, which is used in various data processing

requires separate consent. Consent to the evaluation of

individual use of digital offers is different from the other facts

separate because it is a separate issue.

• When analyzing individual internet use, health

data (sleep disorders, dyslexia, etc.) can be determined. The new

ligung ensures that no sensitive data is lost without this being expressly stated

be processed at the will of the customer.

The agreement has already been implemented except for the separation of the separate

consent to point 10 of the declaration of consent. This should be done by May 2020.

Our negotiations with the DSGV have led to a significant improvement

the declaration of consent used by the savings banks.

10.2 Mortgage credit only with information about

family planning?

s

i

x

a

right

P

right

e

i.e

s

and

A

Customers of a Hessian Volksbank who are interested in a mortgage

Interested in counter credit must fill out a questionnaire that also

Information on family planning is to be provided. This information is not voluntary

lig, in any case a corresponding reference is missing. The bank justified its

go among other things with the fact that the question of family planning on the recommendation of the

Federal Association of German Volksbanken and Raiffeisenbanken e. V. (BVR)

successes. We took this as an opportunity with the Berlin-based

Association to have a conversation.

149 recital

150

Chapter 10 Finances 10 2 Mortgage credit only with information about family planning?

The Association of Banks submitted that the question of family planning was due to

Section 511 of the Civil Code (BGB), according to which the bank prior to provision

the consulting service u. a. about the "personal situation" of the customer

I have to inform customers. in the subsequent lending

the minutes of the consultation will be taken into account. Answering the question

after family planning, however, is neither for the allocation of a concrete

dits still a decisive criterion for its conditions.

There is a legal basis for the question of family planning

not, the bank's actions are therefore unlawful. As part of the free

willing consultation, it depends to a large extent on the customer

which advice you want. The question of family planning is

only permissible if the persons concerned expressly indicate that it is voluntary

be advised of the information. A legal obligation to query the

Family planning does not result from § 511 BGB either. The "personal situation"

includes only those events for the occurrence of which at least concrete

breakpoints are available. Otherwise, other potentially occurring events would also have to

events (e.g. relatives in need of care, illness) can be queried. Since the

Answering the question about family planning neither for awarding a

specific credit nor for its conditions is the data

also not necessary for the execution of the loan agreement.

No agreement was reached with the association. Banks that feature

Inquire about family planning must expect regulatory action.

The question of family planning in the context of a counseling session

lending is - without reference to the voluntary nature of the information - legal

adverse.

151

10.3 How many identity cards does one need

Association for opening an account?

s

i

x

a

right

P

right

e

i.e

s

and

A

An association that works for the interests of the Berlin police wanted one

Open a bank account. The first chairman and the treasurer of the association should

authorized to bank, but not the other members of the Management Board.

The association gave the bank copies of the identity cards of the authorized representatives who

tax identification number and the register of associations. The bank was also

informed that legal transactions with other countries were not planned.

The bank informed the association that an account could only be opened

when she receives a copy of the identity card of all board members.

For this purpose, the bank is due to the Money Laundering Act (GwG) and the tax

ordinance (AO) obliges. The club asked us to check whether the bank's statement

is so true.

According to the GwG, banks are obliged when opening an account for a

identify the beneficial owners.150 In the case of non-profit organizations

Associations “the legal representative, business

leading shareholders or partners of the contractual partner”151 – after that had to

the bank also identifies the members of the Board of Management who are not authorized

adorn.

Due to the excerpt from the register of associations, however, the bank already had this

the name, place of residence and date of birth of the board members. One

General identification of beneficial owners using ID cards

The law does not provide for paperwork. The identification measures have changed

according to the open formulation of the risk assessment in the Money Laundering Act152

always be based on the individual case. The appropriateness of the measure determines

first look at the risk of money laundering and terrorist financing

of the business relationship.153 As there is no particular risk in the present case,

150 See section 11 (1) sentence 1 in conjunction with section 3 (2) sentence 5 GwG

151 See section 3 (2) sentence 5 GwG

152 Section 11 (5) sentence 4 GwG

153 Explanatory memorandum to Section 11 (5) GwG (Bundestag printed paper 16/9038, page 38)



lay - this was also not presented by the bank - after the money

laundry law, the submission of the register of associations. To the same interest

one comes into consideration when applying the regulations of the AO.

The bank was therefore not authorized to

to demand copies of ID cards from members of the stand. The bank promised us

to proceed in accordance with our legal opinion in the future.

When opening an account through an association, banks are usually allowed to

not the identity card copies of the non-authorized account managers

request members.

10.4 A talkative bank employee

A bank employee recommended to his customer, who had just become a widow,

to sell her property and gave her the name of a broker he knew. The

However, the customer was not interested in contact. Nevertheless, he informed

bank clerk told the broker, who was apparently a friend of his, that in a

a house owner had died on a certain street and the widow with him

almost certainly have to sell the house. The agent managed to

this information to identify the widow and make her an offer.

They then complained to us.

A

and

s

i.e

e

right

P

right

a

x

i

s

Since the broker was able to use the information received to inform the person concerned

easy to determine is the note from the bank employee

to transfer personal data of the persons concerned. This took place

without any legal basis154 and was therefore unlawful. The bank has

cleared and reported the incident155 as well as taking labor action against her

employees initiated. We have issued a warning to the bank

spoke.

154 See Art 6 Para 1 GDPR

155 See Art 33 GDPR



Banks are only allowed to contact brokers with the will of those affected

or create brokers.

10.5 Proof of carer status

opposite a bank

s

i

x

a

right

P

right

e

i.e

s

and

A

A bank asked for a support office, which does banking for a

wanted to carry out, in addition to the supervisor ID also the

judicial decision with the justification for the arrangement of supervision.156

Caregivers have related to the care

to third parties, such as authorities, doctors, banks, etc. to be legitimate

in order to be able to represent the interests of those affected. To this end

the guardianship courts issue ID cards. Such ID cards contain in addition to the

Supervisor status also information on the scope of duties of the supervisor

of the supervisor. In the specific case, the supervisor for the asset care was

constant.

While the care card does not contain any information about the reasons for the

contains the regulation of supervision is described in detail in the supervision resolution

indicates which physical and/or mental illnesses require care

make necessary. The bank requires this additional information

but not to check whether the caregiver is the person concerned

person can represent in the care of assets. The requirement of this

lay was therefore unlawful. The bank admitted the mistake and agreed to

to only have childcare cards presented in the future.

The supervisor legitimizes himself/herself towards third parties

finally by presenting the care card.

156 See § 1896 BGB

11 video surveillance

11.1 Südkreuz remains a test laboratory for

"intelligent" video surveillance

After the S-Bahn passengers had already been tested in 2018 by the Federal

despolizei as guinea pigs when it comes to “intelligent” video surveillance

had to serve,157 the Deutsche Bahn now also uses the station as a

search laboratory. Since June 18, 2019, Deutsche Bahn has been testing at the train station in

lin-Südkreuz so-called “intelligent” video analysis systems from three different ones

providers.

A

and

s

i.e

e

right

P

right

a

x

i

s

The aim of Deutsche Bahn is in this second test series, with the new

Video technology to improve the reliability and punctuality of rail operations

improvements and impairments at the expense of rail customers

to reduce. To carry out test scenarios in the station area played until

At the end of 2019, volunteers created around 1,600 scenes based on a set script. There-

It should be checked whether the image analysis software used is able to

unequivocally recognize situations that affect the quality, reliability and safety

could impair the safety of rail operations.

The following scenes were selected for the test: People lying on the

platform, unauthorized access to defined areas (e.g. track bed), accumulation

movement of people (e.g. in front of escalators), movement of groups of people, people

sun count and stored items. When choosing the test scenarios

Deutsche Bahn has oriented itself to typical situations that have occurred in the past

have led to disruptions in rail operations. Does the technology recognize such

Scenes, the respective camera image switches to the for

monitors set up for the test. As far as an event-related activation

not done, the images captured by the respective camera will be permanently stored in

changing random sequence. The test areas in the train station are over

157 JB 2018, 4 4

155

marked in blue and are managed by those responsible on site

cared for.

As the responsible supervisory authority for DB Station&Service AG, we have

responsible for video surveillance at Deutsche Bahn stations, which

This project was already closely monitored during the preparations in the planning phase

and pointed out the considerable risks involved in a possible survey

and processing of biometric data.158

Deutsche Bahn has promised us that in this test run

The video technology used does not contain any biometric characteristics of the persons concerned

would be collected to assess the test scenarios. For data collection and

processing and to be able to evaluate, we have the German

Bahn requested to send us a list of those characteristics that are

providers should be processed. It was evident from this list that some

of the characteristics used should only serve to determine whether it is

is a person or e.g. larger objects, shadows or animals.

Under these conditions, however, it should not lead to an identification

of right natural persons.

Because the test was conducted with volunteers, it was privacy-sensitive

basically harmless. For the assessment of whether such an application after

After the test can be switched to regular operation, it is very important

to what extent the application can contribute to safety at the station and to what extent

the intensity of the encroachment on the personal rights of the passengers.

Even while the test operation was being carried out, Deutsche Bahn was

is obliged to comply with data protection principles. On the one hand, this meant

Ensuring a process that is transparent for those affected and the timely

appropriate deletion of generated recordings. In addition,

provide technical and organizational measures for video technology

to reduce data protection risks. Deutsche Bahn had to

Control the implementation of these requirements as the client.

158 JB 2018, 4 4

156

Chapter 11 Video surveillance 11 2 Biometric access control at a large publishing house

During the entire test phase, Deutsche Bahn had to ensure

that no biometric data to uniquely identify natural

Individuals are collected and processed because this is carried out for

testing was not required. Already when carrying out the tests had to

the providers commissioned with the implementation are checked. The German

sche Bahn had to ensure that the commissioned companies

comply with data protection principles and check whether they have agreed technical

and organizational measures to reduce data protection risks

implement those affected. These requirements would certainly

general operation apply. Based on the test results, we will

decide whether data protection-compliant regular operation is possible. At a

possible tender, the protection of data protection should be part of the

selection criteria for providers.

11.2 Biometric access control at a

big publishing house

A large publishing house has been testing a biometric access con-

trolls (face recognition) as part of a pilot project. This should

employees of the company have easier access to the building. In

In this context, biometric characteristics of such persons

detected who enter a marked part of the entrance area. People that

have previously given their consent are recognized by the control system as

authorized to enter, and access is granted.

A

and

s

i.e

e

right

P

right

a

x

i

s

In principle, consent in the employment relationship is only possible under very narrow conditions

conditions permissible because it is re-

according to the voluntariness of a consent is missing. This question is urgent

downright, if a biometric access control nationwide for everyone

employees should be introduced. In the present case, the employees

initially had the opportunity to register voluntarily for the pilot project.

the. Access to the workplace without biometric control is the employees

still possible without restrictions. Thus, at least during the

Test phase of the pilot project will be accepted as voluntary.

157

The processing of biometric data of those persons who do not have consent

authorization is inadmissible.159 The biometric characters

However, the system initially evaluates these people on the basis of

shear sensors, which also generates biometric features for them

160 These persons are then identified as not having access authorization.

Although the images are automatically pixelated after this process, the biometric

However, technical data of the persons concerned will be used for the purpose of data reconciliation.

still collected and processed.

In order to carry out the test in a permissible manner, it must therefore be guaranteed

that only data of those persons who are effectively included in the

have consented to the processing of biometric data. This can e.g.

be enough that the camera can only be opened by an authorized person at the push of a button

person is involved.161 In the present case, the company had certain

Edge areas of the camera image pixelated. Nevertheless, it could not

be concluded that persons who happen to enter the marked area

traverse, are also recorded biometrically. Upon our notice,

the additional partitions around the area of the face-recognizing cameras

set up to prevent accidental capture of bystanders.

We asked the company to contact us after the trial was complete

to inform the results. If regular operation is then sought

be made, it would have to be ensured in particular that participation in

of biometric access control through the possibility of an alternative

Access control remains voluntary so that corresponding consents are effective

sam can be granted.

159 See Art 9 GDPR

160 For the details and components of biometric registration, see also the position

tion paper on the biometric analysis of the DSK from April 3, 2019 (esp. S 11 f )

161 EDPB, Guidelines 3/2019 on processing of personal data through video devices,

sion for public consultation, adopted on 10 July 2019





## 11.3 Permissibility of Dash Cams

A Berlin-based company that offers its services to private

offers national transport, intends to expand its vehicle fleet with so-called

equip dash cams. In the present case, the cameras should be inside the

windshield behind the interior mirror to avoid

traffic in front of the vehicle and thus extensive public road

country to watch. On the one hand, the recordings should contribute to the preservation of evidence

Accidents serve, on the other hand act preventively by the vehicle drivers

are encouraged to drive with foresight and caution. To what extent

The latter can be achieved, however, is very doubtful.

A

and

s

i.e

e

right

P

right

a

x

i

s

The use of dash cams in vehicles that require continuous recording without cause

enable, is generally not permitted in road traffic.162 The Federal

Court of Justice (BGH) has already indicated that a data protection-compliant

set of dashcams may be possible in individual cases if due to a technical

System automatically deletes the recordings periodically after a short period of time

and is implemented on a case-by-case basis.163

Against this background, the supervisory authorities discussed under which

The prerequisites for the use of dashcams are permissible under data protection law

could be.

Ultimately, the data recorded with a dashcam must always be

telbar be overwritten and storage always with a specific

be connected to the reason for recording. Recognize (accident) sensors such as a

acceleration sensor, a collision or severe deceleration of the vehicle

tool, then a backup of the last recording interval is required

allowed. The storage over a period of 30 seconds before and

30 seconds after a recognized cause is sufficient to determine the course of an accident

162 DSK position paper of 21 January 2019; BGH, judgment of May 15, 2018 – VI ZR

233/17

163 See BGH, judgment of May 15, 2018 – VI ZR 233/17

159

to document. After a total video length of 60 seconds, Dash

delete cam recordings automatically.

A problem that has not yet been solved is compliance with the transparency obligation

when operating a dash cam. In the event that it is due to an accident too

longer-term storage of personal data, the

Those involved in the accident are informed of this. This also applies in principle

pull on people who are only fleetingly recorded.

The collection and storage of image data when using dashcams in the

Road traffic is only permitted if this is exclusively necessary and

occurs for a short period of no more than 60 seconds; a permanent

Liable collection and storage without cause is not permitted. The

Transparency of data processing must be guaranteed.

160

Chapter 11 Video surveillance 12 1 N26 Bank GmbH

12 sanctions

After the new data protection regulations of the EU came into force,

we now worked the vast majority of cases in our sanctions practice

according to the new fine regulations. The cases regularly concerned the unlawful

moderate processing of personal data.

We have imposed 56 fines totaling €14,808,400. 16

Penalty payment notices were issued by us. In four cases we have one

lawsuit filed.

When deciding on the imposition of fines and their amount

In each individual case, we use the discretionary criteria of Art. 83 Para. 2 DS-

GMO checked. In particular, the specific circumstances regarding the type, severity and

duration of the respective infringement. In addition, among other things, the

Consequences of the respective violation and the measures taken by those responsible

measures have been taken to avert or avert the consequences of the violation

mitigate, considered. Helpful orientation is provided by the conference of the

independent data protection supervisory authorities of the federal and state governments (DSK)

adopted fine concept164.

12.1 N26 Bank Ltd

The online bank of N26 Bank GmbH illegally ran a so-called "black

list" of former customers, which is why we have to pay a fine of

have imposed 50,000 euros.

For the purpose of preventing money laundering, the young company had

and surnames of former customers on a "black list"

set, regardless of whether they were actually suspected of money laundering

As a result, those affected were unable to open new accounts at the bank.

164 See 1 4



N26 Bank GmbH accepted the fine and vis-à-vis our authorities

announced a series of measures to address previous organizational shortcomings

to eliminate and thereby protect the data of their customers

improve. In particular, the company promised in this regard

to extensively increase and train its staff in the area of data protection.

When implementing legal requirements for data

processing, e.g. in this case to prevent money laundering, strictly on their

range and may only process data to the permitted extent

make. Otherwise there is a risk of heavy fines.

12.2 Delivery Hero Germany GmbH

The data of customers of the delivery service of Delivery Hero Ger-

many GmbH were stored for many years, even if they were for years

had not ordered anything. This violated the GDPR and was punished with a fine

fined.

The fines were imposed in two notices. In a fine notice

we have 18 fines for violating the GDPR totaling

including 120,000 euros imposed. In another decision against the delivery service

we have ten fines according to the old data protection regulations in

A total of 58,000 euros. Including the fees

the fines totaled 195,307 euros. The fines were issued in two

because some of the violations were still effective after the GDPR came into effect

data protection law was to be assessed. Decisive for the question of whether a

The time of the offense is to be assessed according to the old or new legal situation.

With the fines, we have various data protection violations of the

company. The majority of cases concerned non-compliance with the

Rights of data subjects such as the right to information about the processing of their own

data, the right to delete the data and the right to object. After

According to our findings, Delivery Hero Germany GmbH had

accounts of former customers are not deleted, although the affected

have not been on the delivery service platform for a long time – in one case since 2008

162

Chapter 12 Sanctions 12 2 Delivery Hero Germany GmbH

of the company had been active. Former users also had each other

complained about unsolicited commercial emails from the company. In further

cases, the company granted to the complainants

did not provide the requested self-disclosures or only after we as supervisory

had intervened.

Delivery Hero Germany GmbH informed us of some of the violations

technical errors or employee mistakes. Due to the high

number of repeated violations, however, we assumed fundamental structural

tural organizational problems. Although we give the company multiples

hints they had given were not sufficient for a long period of time

Measures have been implemented that ensure the due fulfillment of the rights of

Affected could ensure. We have the measures taken by the company

company have been taken to avert the consequences of the violation or

mitigated, taken into account accordingly in our fine notices.

The Delivery Hero brands Lieferheld, Pizza.de and foodora were launched on April 1st

Taken over by the Dutch group Takeway.com in 2019. the dem

The violations underlying the procedure were all prior to this acquisition

committed. The new owner accepted the fine notices and none

appealed.

Anyone who works with personal data as a digital company needs

a functioning data protection management system. data from customers

Customers should only be stored for as long as they use the online

bot also regularly avail. That not only helps fines too

avoid, but also strengthens the trust and satisfaction of customers

shaft.

163

12.3 Deutsche Wohnen SE

The administrative offenses165 committed by Deutsche Wohnen SE were

sanctioned by our authorities with fines in the millions.

The imposition of fines of this amount for the violations in the period between

May 2018 and March 2019 was mandatory because the GDPR obliges the

Supervisors to ensure that fines in each individual case not only

proportionate but also effective and dissuasive.

The starting point for the assessment of the fines was, among other things, the

targeted the company's previous year's sales. For the specific determination of

We then calculated the amount of the fine, taking into account all debit and credit

the legal criteria166 are used for the aspects:

The fact that Deutsche Wohnen SE had the objectionable

dete archive structure had deliberately created and the data concerned via a

have been processed in an unlawful manner for a long period of time.

To mitigate the fine, however, we took into account that the company

quite the first measures with the aim of cleaning up the unlawful access

seized the position and formally worked well with us. Also that dem

Companies do not abusive access to the inadmissibly stored

Data could be proven, we took into account reducing the fine.

In addition to sanctioning the structural violation, we imposed on the

Deutsche Wohnen SE fines due to the inadmissible storage of personal

data obtained from tenants in 15 specific individual cases.

The fine decision has not yet become final, as Deutsche Wohnen

SE has lodged an objection to the fine notice.

165 See also 9 1

166 Article 83 (2) GDPR





Data cemeteries are not only inadmissible and subject to fines, but also increase

also the risk of improper access. Therefore, companies should

urgently check their data archiving for compatibility with the GDPR.

## 12.4 NPD State Association Berlin

We have fined the Berlin state association of the NPD in the amount of

6,000 euros for unlawful publication of personal data

fixed.

The state association already published in February 2018 on its website

seite a map of facilities for asylum seekers created with Google Maps

in Berlin with the title: "An overview of the focal points of foreign infiltration in our

our city". Each location had names, phone and cell numbers as well

E-mail addresses of people working there are attached.

An accompanying text explained that everyone can now find out about

"what interesting uninvited guests are in your neighborhood,

who is responsible for the foreign infestation of our homeland, who is financially responsible for the

Hundreds of Thousands of Migrants Profited and Who to Contact

if you want to make a complaint directly on site". All data came from

from public sources. Responsible for the Google Maps map service

Company Google indicated that the card due to violations of their own

having policies locked. However, it was still easily possible to

read out the code and thus the personal data stored in the card

continue to be visible. As a result, the illegal condition continued.

The collection, processing and use of personal data is only permitted

sig, insofar as this is permitted by law or the persons concerned have consented.

There was no consent from the persons concerned. The usage

was also not permitted by law.167 According to this, the processing of data would only be

then lawful, provided that the responsible body has legitimate interests

167 See Art 6 Para 1 Sentence 1 lit f GDPR



sen pursued and a weighing of interests would show that no protection worthy

The interests of the data subjects prevail. Persons in the field of

However, those who are active in refugee aid have a considerable interest in that

not publish their data on a website with xenophobic content

(“uninvited guests”, “foreign invasion of our homeland”). The data of

affected persons were specifically assigned to anti-refugee

summarized and made visible. The legitimate concerns of the affected

here clearly outweigh any interests of the NPD

in the publication of this data.

The Berlin state association of the NPD has lodged an objection to our decision

laid, so that the competent court can now make the final decision on this

will meet.

The term "processing" within the meaning of the GDPR includes any use

processing of personal data, including collecting and summarizing

and publishing publicly available data.



Chapter 12 Sanctions 13 1 23 Broadcasting Amendment State Treaty

13 Telecommunications and

media

13.1 From the one-off data transfer

for regular data synchronization –

23. Broadcasting Amendment State Treaty

A

and

s

i.e

e

right

P

right

a

x

i

s

With the 23rd Broadcasting Amendment State Treaty, the originally

2022 all scheduled transmission of complete population register data reconciliation

be carried out for four years. In addition, restrictions on the rights of

data subjects on information168 and information169 provided.

The first complete comparison of the reporting

register data with the data of the broadcasting fee payers was considerable

data protection concerns.170 The Conference of Independent

Data protection supervisory authorities of the federal and state governments (DSK) had their

At that time, they only thought partially and only because they were only

a one-off comparison of registration data should be carried out in order to

Adjustment of the fee model to an apartment-related broadcasting fee

facilitate. Even at this point, however, there were doubts about the

assurance of the legislature that this is a one-off process

would delve. These doubts were already confirmed in 2015, when the law

lender decided to carry out a new “one-off” comparison of registration data.171

168 See Art 13 General Data Protection Regulation (GDPR)

169 See Art 15 GDPR

170 See the resolution of the Conference of Independent Data Protection Authorities

Federal and state authorities (DSK) of October 11, 2010 (https://www datenschutz-berlin

de/fleadmin/user_upload/pdf/publikationen/DSK/2010/2010-DSK-Systemwechsel_

Radio fnancing pdf) and JB 2010, 13 4

171 JB 2015, 15 4



The draft for the 23rd Amendment to the Interstate Treaty on Broadcasting that has now been presented

even a regular repetition of the full reporting data comparison in

a four-year cycle. This project represents a disproportionate

encroachment on informational self-determination and is in conflict with the

principles of data minimization and necessity.172

In the case of a complete comparison of reporting data, personal

son-related data of persons transmitted to the broadcasters who

are not liable to pay contributions at all because they either live in an apartment,

for which a license fee has already been paid by other people, or because

they are exempt from the obligation to contribute. In addition, data from all those

gene residents collected and processed, who are already at the

State broadcasting corporation are registered and regularly pay their contributions.

It is particularly relevant in these cases that the planned reporting date

comparison requests even more personal data than the contribution number

must notify the broadcaster when registering

(e.g. doctoral degree and marital status).173

related data are transmitted to the broadcasters that contribute to the

collection are not necessary at all.

The broadcasters justify the need for regular reporting

data comparison with the fact that without this regular measure, there will be a

"erosion" of the stock of contributors would come. Especially when

from a jointly used apartment, the person who

pays the radio fee for this apartment, moves out or dies and the rest

Residents of the apartment not as prescribed at the

register with the relevant broadcasting company, contributions were made for these apartments

away.

The broadcasters themselves assume that a complete reporting

comparison ultimately leads to an additional,

172 Art 5 para 1 lit a and c, Art 6 para 1 GDPR

173 See Section 8 (4) of the Interstate Broadcasting Agreement (RBStV) for the list of required

common login data





permanent registration of contributors.174 In the case of a regular

complete comparison of registration data would thus be disproportionately

the informational self-determination right of the persons concerned

grabbed. This is also not inconsistent with the fact that the state broadcasting corporations

own information through the second complete comparison of registration data in the year

2018 additional premium income in the upper double-digit million

have made rich.

It is true that the reports presented by the state broadcasters

cases actually led to the loss of income under certain circumstances

men can come. However, this problem should be specific to these cases

tailored measures are countered (which in principle also include the

creation of new information and processing powers) instead

simply a transmission of the complete database of the residents' registration

offices in relation to all adult citizens to the state

to consolidate broadcasting corporations.

The planned regulations also take into account the standards of the

General Data Protection Regulation (GDPR) insufficient: Due to

the priority of application of European regulations, national data

protection regulations can be based on an opening clause of the GDPR.

The media privilege from Art. 85 Para. 2 DS-GVO is out of the question here, since the

Data processing for the purpose of collecting broadcast contributions is not included in the

scope of this standard falls.

In the case of regulations based on the opening clause according to Art. 6 Para. 2 and Para. 3 i. V. m.

Art. 6 (1) lit. e GDPR are supported, among other things, the principles of data

minimization and necessity to be considered. After that, member states may

Regulations for the performance of duties are introduced in the public

It is of interest if they specify the GDPR, but not its limits

exceed. Regulations that refer to this opening clause must

consequently stay within the framework specified by the GDPR. In the proposed

In this respect, there are considerable concerns with regard to the current regulation

the principles of data minimization and necessity. The DSK has

asked the legislature in a decision to

not to introduce a complete comparison of registration data.175

The chairman of the DSK 2019 also acknowledged the concerns of the supervisory authorities in

the non-public oral hearing of the Broadcasting Commission of the

the one presented.

Regardless of this, the heads of government of the

At their conference on June 6, 2019, countries presented a draft of the 23rd broadcast amendment

interstate treaty, in which the complete regular reporting

ten adjustment is still included. However, a regulation was added

according to the "to maintain the proportionality between contribution justice

and the protection of personal data" a comparison of registration data should not take place,

if the commission to determine the financial needs of broadcasters

(KEF) states that "the database is sufficiently up-to-date". This assessment

the KEF should be “taking into account the development of the contribution

mens and other factors”. With this, the above mentioned constitutional and

However, data protection concerns are not sufficiently taken into account.

Rather, the supplement creates an additional constitutional problem,

by making the decision to carry out a complete registration data

comparison is delegated to the KEF without any criteria –

see the development of the contribution revenue - for this decision

to hand over. Such significant decisions in relation to the

processing of personal data of all adult residents

residents of Germany, however, must be made by the legislature itself (legislative

keep).

At the same time, the aforementioned draft also sees restrictions in other areas

of the rights of data subjects under the GDPR. In particular,

the information rights of the persons concerned176 are restricted. Instead of

as before, generally obliged to provide information with individually defined exceptions

175 DSK resolution of April 26, 2019: “Planned introduction of a regular

Complete registration data comparison for the purpose of collecting the broadcasting fee

stop" (https://www datenschutz-berlin de/fleadmin/user_upload/pdf/publikatio-

nen/DSK/2019/2019-DSK-Decision-Meldedatenabgleich_Broadcast contribution pdf)

176 See Art 15 GDPR





to be, the rule-exception relationship should be reversed in the future and the

State broadcasting corporations according to the new regulations only with regard to certain

correct and finally listed in the draft data177 information

have to share. This planned restriction of the right to information is compatible with the

Provisions of the DS-GVO not compatible: Art. 23 Para. 1 DS-GVO contains a

final list of the reasons for which the national legislature concerned

entitlements beyond the extent provided for in the GDPR itself

can know. This also includes the “protection of other important goals of the general

public interest of the Union or a member state, in particular one

important economic or financial interest of the Union or of a member

member state, for example in the areas of currency, budget and taxation as well as in the area

of public health and social security”.178 On this exception

the legislator wants to support the intended restrictions. The official

Justification for the draft noted: "The regulations made

ensure that the information obligations of the state broadcasting corporations achieve the goal

of data processing or the fulfillment of the public interest pursued with it

teresses.”179 If this were a realistic danger, they would have to

corresponding empirical values from the application of the currently existing ones

The state broadcasters are obliged to provide information. However, this is

not the case - there are no indications that this obligation to provide information

ten the protection of other important objectives of general public interest

of the Union or a member state would have endangered, as is a prerequisite for

is a restriction according to Art. 23 Para. 1 lit. e GDPR. In this respect, there are

doubts that the proposed restriction "removes the essence of the basic

respects rights and fundamental freedoms and in a democratic society

constitutes a necessary and proportionate measure”, as stipulated in Art. 23 para. 1

DS-GVO is required, and thus in the compatibility of the intended

Restriction of the right to information of the persons concerned with European law.

177 These are from the contributors themselves to the

data reported by state broadcasters, information on any exemption

from the obligation to contribute or to reduce the broadcasting fee, as well as the

Bank details and the body that transmitted the respective data

178 Art 23 Para 1 lit e GDPR

179 Official justification for No. 6 of the draft, p. 7



In addition, data “the

are only stored because they are due to legal or statutory

ger storage regulations may not be deleted or exclusively

serve the purposes of data backup or data protection control". The mountain

liner Data Protection Act (BlnDSG) contains a similar provision180; already theirs

Compatibility with the provisions of the GDPR is doubtful. However is

the regulation there is linked to further requirements: According to this, the

granting the future also require a disproportionate effort and

processing of the data in question by means of suitable technical and organizational

Satorial measures must be excluded. Such additional prerequisites

The draft of the 23rd Amendment to the Interstate Treaty on Broadcasting does not contain any regulations.

Through the regulation now provided there, the information rights of the

affected persons via the otherwise for public bodies of the state of Berlin

further restricted beyond the applicable level without there being a need for this

is visible. This regulation of the draft should therefore be deleted without replacement

the. As a provision contrary to European law, it would not be applicable anyway.

It should be positively emphasized that the previous "landlord information" for rented

ments181 deleted and the purchase of address data from private individuals in

Address trading is to be expressly excluded in the future. This authorization

From the point of view of data protection, information and their

Deletion is to be welcomed. However, it must not be overlooked that

the planned regular complete comparison of registration data, a far

comprehensive instrument of data collection, which is very dubious in terms of data protection

exercise is to be created that satisfies the practical need for a landlord

information and the purchase of private addresses can be omitted anyway.

The legislature should refrain from requiring a regular full reporting

to introduce data comparison, since the planned regulations are fundamentally

there are additional constitutional concerns and the standards of the DS-

GMOs are not sufficiently taken into account. Restrictions on the Rights of

affected persons, such as the right to information and access, may only

180 See Section 24 (1) sentence 3 BlnDSG

181 See Section 9(2) and (3) RBStV

take place within the framework provided for in Art. 23 DS-GVO. The planned EU

Restriction of the right to information that violates rape law should therefore be removed from the

Draft of the state broadcasting contribution agreement to be deleted.

## 13.2 Decision of the European Court of Justice on "Planet 49"

For several years, courts have been hearing about a lawsuit brought by the Federal

Association of Consumer Centers and Consumer Associations (vzbv) against the

Sweepstakes provider "Planet 49". This had in a sweepstakes offer in

integrated a consent box for tracking cookies, which

was already ticked. He also settled into the terms of use for the

Sweepstakes compulsorily the right to pass on data of affected persons

to a large number of third-party companies. The European

Court of Justice (ECJ) has now ruled that this practice violates applicable data

breaches data protection law.182

A

and

s

i.e

e

right

P

right

a

x

i

s

The ECJ first made it clear that both under the conditions of data

Electronic Communications Protection Directive (e-Privacy Directive for short)183

as well as according to the DS-GVO an effective consent to data processing

does not exist if the consent has been given by a preset check box

it is explained that the users will opt out of refusing their consent

(so-called opt-out).

The legal requirements for setting cookies and similar technologies

gies184 apply regardless of whether the data stored in the end device

information retrieved from it is personal data

or not.

182 CJEU, decision of 1 October 2019 – C-673/17

183 Directive 2002/58/EC of the European Parliament and of the Council

184 Art 5 para 3, Art 2 sentence 2 lit f of Directive 2002/58/EC in conjunction with Art 2 lit h of the

never 95/46/EG of the European Parliament and of the Council or with Art 6 Para. 1 lit a,

Art 4 No. 11 of the GDPR



Finally, the court finds that Article 5(3) of Directive 2002/58/EC

is to be construed as relating to the information provided by a service provider

has to give the user of a website, also information on the functional duration

of the cookies and the indication of which recipients or categories of

Recipients get access to the cookies.

The decision of the ECJ is of great importance beyond the individual case: So

In its decision, the court also specifies the requirements that must be met by a

consent are to be provided and makes it clear that any consent is an active

of the users presupposes that without any doubt a

mood is signaled and is voluntary. This is (finally) supreme court

determined that the frequently encountered design of offers on the Internet

net, according to which the mere continued use of the offer constitutes consent in

in terms of data protection law, is unlawful.

The configurations that are also widespread are therefore also unlawful

in Internet offers where consent has already been given in advance

crossed boxes are to be obtained.

With the decision of the ECJ, there could also be movement in the already since 2009

by the Federal Ministry for Economic Affairs and Energy (BMWi).

Implementation of the provisions of Art. 5 Para. 3 of the previously applicable E-Principle

vacy guideline185: A press spokesman for the ministry already said so

after the publication of the Opinion of the Advocate General in the

ren before the ECJ in September announced that one after the decision

of the ECJ also wanted to "clearly clarify" the legal situation in Germany

and that corresponding changes to the Telemedia Act (TMG)

185 An EU directive must be transposed into national law; an EU regulation

applies directly without national implementation Therefore, the regulations of the previous

gene E-Privacy Directive to be implemented by a national law which is currently

The new E-Privacy Regulation currently being negotiated at European level would

against, if passed, will apply immediately in all EU member states



be in preparation. A draft law is to be presented in autumn 2019

be laid.186 To the best of our knowledge, this has not yet happened.

The intention of the BMWi is to be welcomed. The DSK had already in April 2018 in

their position on the applicability of the TMG for non-public bodies

from May 25, 2018 (effective date of the DS-GVO) pointed out that

there is an urgent need for amendment with regard to the TMG and the

succeeded the 4th section of the TMG after the entry into force of the DS-GVO

are applicable.187

The setting and retrieval of cookies or other information contained in a

end device of a data subject are stored, is in many cases a

approval required. The Wi-

the appeals process is not sufficient. A data protection consent

requires active behavior on the part of the user, which without

the doubt signals consent and must actually be voluntary.

Pre-filled checkboxes or a pure further use of an offer

do not represent consent. Regarding the mandatory information, the website

driving about in their data protection declaration must also include the

How long cookies last and whether third parties have access to these cookies

can get. Persons responsible for Internet offers in Berlin are called

fen to implement these requirements in their offers immediately, insofar as

this has not already happened.

186 See report by netzpolitik org eV of September 11, 2019: “Economic

rium wants to propose new rules for online tracking in autumn”, https://netzpolitik

org/2019/Ministry-of-Economy-wants-new-rules-for-online-trading-in-autumn-

cking-suggest/

187 Position determination of the DSK of April 26, 2018 "On the applicability of the TMG for

non-public bodies from May 25, 2018 (https://www datenschutz-berlin de/f-

leadmin/user_upload/pdf/publikationen/DSK/2018/2018-DSK-position determination_

TMG pdf); cf. also the guidance provided by the supervisory authorities for providers of tele-

media from March 2019 (https://www datenschutz-berlin de/fleadmin/user_upload/

pdf/orientation aids/2019-OH-Provider_Telemedia pdf)

175

13.3 Regulatory Guidance

for telemedia offers

s

i

x

a

right

P

right

e

i.e

s

and

A

Which third-party content is included on websites under which conditions

may be, which range measurement and tracking measures and when

are permissible has been difficult to assess in practice. To be specific

the positioning of the DSK from April 2018188 for the processing of personal

data obtained by telemedia providers after the GDPR came into force

In March 2019, the DSK published a detailed orientation guide for telemedia

bids (restricted to non-public bodies) passed.189

After consultation with business associations and companies concerned,

The enclosed guidance initially makes it clear that when the

DS-GVO the data protection regulations of the TMG in the non-public

Area no longer applicable due to the application priority of the GDPR

the.

It also contains extensive detailed explanations

Lawfulness of the processing of personal usage data according to the

DS-GVO by providers of telemedia. Because these process

ten usage data for a large number of

purposes190, including to make the offer user-friendly and

to display additional individual functionalities (e.g. the shopping cart function)

to provide content from third-party providers (e.g. a video or

a map service), for IT security measures, for range measurement and

188 See footnote 187 and JB 2018, 12 3

189 See footnote 187

190 As far as the processing of usage data for the fulfillment of the respective (user

ment) contract is mandatory, it is in accordance with Art. 6 para. lit b DS-GVO

admissible This permission was granted with regard to the discussions on

European level on the question of the applicability of Art 6 Para 1 lit b DS-GVO im

Related to the Provision of Online Services in the Guidance

However, not discussed meanwhile, the European Data Protection Board

guidelines adopted for this purpose, which can be found at https://edpb europa eu/our-work-tools/

our-documents/smernice/guidelines-22019-processing-personal-data-under-ar-

ticle-61b_en can be retrieved



statistical analyses, for advertising purposes and much more m. Depending on the purpose and

the technical design are partly personal

data passed on to third parties. For each of these processing operations, the

Provider ensure that there is a legal basis for this

exists.

In the orientation guide, the requirements of the practically relevant

Permissible facts of the balancing of interests191 and the consent192

referenced:

Many providers base the processing of usage data on their legitimate interests

Interest according to Art. 6 Para. 1 lit. f GDPR. However, it should be noted that the

Regulation in addition to a legitimate interest of the provider

requires that "not the interests or fundamental rights and freedoms

the data subject (i.e. the user, author’s note) who

protection of personal data prevail”.

The orientation guide therefore contains information for the design of this interface

essential consideration, i.e. which interests of those responsible as legitimate

interests i. s.d. provision are to be considered, such as the necessity of data processing

processing is checked to protect legitimate interests and what is involved in the

Weighing against the interests, fundamental rights and fundamental freedoms of those affected

persons must be taken into account in the specific individual case.

Insofar as this balancing of interests for a specific usage data processing

fails in favor of the users concerned, the offer must

terin or the provider of the telemedia offer regularly before processing

a self-determined and informed consent193 from the respective user

obtain it or refrain from processing the relevant usage data.

Also the requirements for self-determined and informed consent

are explained in more detail in the orientation guide:

191 Art 6 Para 1 lit f GDPR

192 Art 6 Para 1 lit a GDPR

193 See Art 7, Art 4 No. 11 GDPR



A self-determined and informed consent requires, in particular,

that users have a real choice whether to give consent on the basis of

position of comprehensible and transparent information about the intended

consent to the data processing or not. In addition, the consent of

be explained to them by a clear affirmative action. silent

genes, pre-ticked boxes or inaction (and continued use) are sufficient here-

for not.194 Many so-called cookie banners that can be found on the Internet give

pretends to represent consent. They often meet the requirements

Unfortunately, the GDPR does not.

If a required consent is not properly granted, the respective

regular data processing does not take place. Consent is then required, for example

lich if the behavior of the website visitors in detail

is understood and recorded, such as when keyboard inputs, mouse or

Swipe movements are recorded and analyzed. Classified as admissible

on the other hand, it can happen if a website operator uses a range

recording and the number of visitors per

Page that collects device types and language settings.

We keep receiving complaints and information from affected people

to the inadmissible usage data processing by Berlin providers

and providers of telemedia. We are examining these and have already

gene responsible initiated.

In particular: integration of third-party content

Many providers of telemedia bind internal

maintained by third parties for various purposes. These include, to name just a few

to name particularly prominent examples:

• advertising networks,

• fonts,

• videos,

• map services,

194 See EG 32 on the GDPR and 13 2



• Social plugins such as the Facebook “Like” button and similar

Buttons of other companies as well

• News services such as Twitter.

This integration of third-party content is regularly associated with the transmission of personal

related usage data of the users to these third parties. Also

a legal basis is required for this. In many cases, the providers go into their

Privacy statements assume that this transfer readily available

the provisions of Article 6 (1) (f) GDPR can be supported.

In many cases it can be assumed that those responsible

a legitimate interest - including commercial interests - in the

transfer of the personal data of the data subjects.

However, those responsible for telemedia should be aware that

this is only the first part of the legality check and the result of the

if required balancing of interests in the transmission of usage

data to third parties will in many cases turn out to be to their detriment, so that

for the corresponding data processing, as a rule, the consent of the

met is required. With regard to their accountability,195 employees should

bidders therefore only integrate third-party content into their website

if they have checked and documented in advance that through the integration

triggered data processing is completely lawful.

Operators of Internet offerings that contain inadmissible third-party content

not only have to reckon with orders under data protection law,

they should also take into account that the GDPR applies high standards for such violations

threatened with fines.

Providers of telemedia should change their usage data

check work immediately. Anyone who uses functions that require consent

require, must either obtain this consent in accordance with the law or the

remove the respective function. The illegal transmission of usage data

t to third parties may, among other things, result in the imposition of a fine.

195 See Art 5 Para 2 GDPR



13.4 Use of Google Analytics & Co. for

range measurement

s

i

x

a

right

P

right

e

i.e

s

and

A

Many website operators use tools to

width measurement on. Among the particularly popular applications for the rich

The “Google Analytics” tool counts for distance measurement. This tool can

but only with the consent of the users concerned

be used in accordance with the law. The granting of a right of objection

is no longer sufficient for legally compliant use.

The use of Google Analytics has the supervisory authorities for data protection

already employed in the past.196 He was among those then given

Conditions in many cases possible without consent, in particular because

because he refers to the regulations for order data processing from the then

Federal Data Protection Act (BDSG) could be supported and thus for the

No legal basis was required for the transfer of the data to Google Inc.

However, order processing is ruled out if the contractor

or the contractor also uses the data for its own purposes.

However, this is exactly the case with the terms of use now used by Google Inc.

ments the case: It is made clear there that Google Inc. also uses the data for its own

purposes.197 According to Art. 28 Para. 10 DS-GVO, this is the

The provider of Google Analytics is therefore not (any longer) about a processor,

even if this continues to refer to the contract as order processing.

Under these changed conditions, the integration of Google Analytics

by the website operator in terms of data protection law, a transmission

communication to the operator of Google Analytics, which requires a legal basis.

According to the provisions of the GDPR and their interpretation by the DSK in the

196 See JB 2011, 12 2, p 170 ff

197 Terms of Use for Google Analytics (https://marketingplatform google com/

about/analytics/terms/de/, as of June 17, 2019, number 6) in conjunction with Google data protection clarification (https://policies google com/privacy, as of October 15, 2019, item "Measurement performance")



Guidance for providers of telemedia198 comes for this transmission of usage data, only the consent of the persons concerned is taken into account.

As already mentioned in another context199, consent is independent always dependent on the involvement of processors or third parties also necessary if the behavior of the website visitors -Visitors are traced and recorded in detail during a range measurement- can be drawn, for example when keyboard inputs, mouse or swipe movements gene are recorded.

On the other hand, it can be regarded as permissible without consent if a website operator carries out a range measurement and for this the Number of visitors per page, the devices and the language positions, even if a processor takes care of this.

The consent must be given in a way that the affected fene person clearly indicates that they consent to the processing of them relevant personal data agrees. So she has to voluntarily and unequivocally as a declaration of intent in the form of a tion or any other unequivocal confirmatory action and although for the specific case and in an informed manner.200 In addition to this the GDPR makes it clear that silence, boxes that have already been ticked or omissions activity of the data subject are not consent.201 This clear evaluation of the legislator, the ECJ also expressly stated in the "Planet49" dispute

confirmed.202

In particular, the use of Google Analytics can no longer be based on the

by the then Berlin Commissioner for Data Protection and Freedom of Information

(BInBDI) in March 2013 published “Notes for website operators with

Based in Berlin, who use Google Analytics”. On this

198 See 13 3

199 See 13 3

200 Art 4 No. 11 GDPR

201 EC 32 GDPR

202 See 13 2



We already announced the situation in November 2019 in a press release.

assigned.203

Nevertheless, we always ask when checking Internet offers

states that Google Analytics and other services are used there without

the necessary consent of the user is obtained. we love

Accordingly, there are also a large number of complaints from those affected and from

Information about the inadmissible integration of Google Analytics and similar

services.

Operators of websites that use Google Analytics and similar

services should immediately check their offers to see whether the

legal requirements for legally compliant use are met. Who

uses functions that require consent, either consent must

obtain or remove the function.

For the legally compliant use of Google Analytics, the consent of

Website visitors required. operators and

Operators of websites that continue to use Google Analytics without being legally compliant

use consent, expose themselves to the risk of regulatory measures

measures, which may include the imposition of fines.

13.5 "Facebook Custom Audience" list relationship

drive – no use without consent!

The so-called "list procedure" for "Facebook Custom Audience" enables companies

companies (mainly operators of online shops), their

To allow customers to advertise on Facebook in a targeted manner, insofar as these

use Facebook at the same time.

s

i

x

a

right

P

right

e

i.e

s

and

A

203 BlnBDI press release of November 14, 2019 (https://www datenschutz-ber-

lin de/fleadmin/user_upload/pdf/pressemitteilungen/2019/20191114-PM-Analysis_

tracking tools pdf)

For this purpose, the advertising company creates a list of data from its customers

and customers, such as email address and/or phone number. This

Data is "hashed" (i.e. one-way encrypted, using the

function on a specific date or series of dates always the same

results) and then transferred to the company's Facebook account.

gen. There the data is processed by Facebook with the data that has also been hashed

compared to his own customers. Similar results at

the application of the function then show that the respective person is both customer

din or customer of the "registering" company as well as Facebook.

On this basis, the registering company can then

advertisers and customers on Facebook for its products or services

gene or its existing customers from advertising campaigns

for its products or services on Facebook. This

may be for very specific audiences based on the

filtered out on Facebook via the characteristics known to each person

can become.

According to the provisions of the DS-GVO, the use of the list procedure is only

possible on the basis of an effective consent of the persons concerned.

The Bavarian

Higher Administrative Court.204 The court confirms this decision

a decision of the Administrative Court of Bayreuth205, in which, among other things, the following

Findings on the data protection-compliant use of the “Facebook Custom

Audience” list procedure meets:

• “Hashed” email addresses are personal data because “hashing”

does not represent anonymization.

• Passing on the "hashed" e-mail addresses to Facebook for the "Face

book Custom Audience" listing process is a transfer to third parties and

no order data processing.

204 VGH Munich, decision of September 26, 2018 - 5 CS 18 1157

205 VG Bayreuth, decision of May 8, 2018 - B 1 S 18 105

183

• A balancing of interests206 can also prevent the transmission of the "hashed"

E-mail addresses do not justify. The legitimate interest of the responsible

literal part of the transmission of "hashed" e-mail address data

also be maintained without disproportionate effort, if in individual cases

consent of the persons concerned, e.g. B. as part of an order process

is fetched. The interest in the transmission of the data for advertising purposes

the prevailing personal rights of the persons concerned that are worthy of protection

opposite.

The explanations of the two courts refer to the legal situation

Entry into force of the GDPR. However, the basics of the above decisions

also be transferred to the legal situation in the following period.

As a result, the use of the "Facebook Custom Audience" list

procedure only with the prior effective consent of the persons concerned

allowed.

We have received complaints from data subjects against various companies

that used the "Facebook Custom Audience" list method in the past

have used without the consent of the persons concerned or even this

keep doing. We are in the process of investigating these individual cases. be there

we also initiate regulatory actions including the

Consider imposing fines, particularly if the affected

fenen company after reference to the legal situation the use of the "Facebook

Custom Audience" list procedure without the consent of the data subjects

continue.

The use of the "Facebook Custom Audience" list method is only

sis of a prior legally effective consent of the persons concerned

allowed. Granting a right to object is not sufficient. offering

providers who use the "Facebook Custom Audience" list procedure

without the required consent must be approved by supervisory authorities

cal measures.

206 See Section 28 Paragraph 1 Sentence 1 No. 2 BDSG old version



## 13.6 Facebook fan pages: exams and developments

Anyone who operates a Facebook fan page processes personal data in

joint responsibility with Facebook207 In order to check whether the resulting

compliance with legal obligations, we had various at the end of 2018

Testing procedures initiated against fan page operators. In the meantime it has

Federal Administrative Court (BVerwG) decided that a supervisory authority

may prohibit the operation of a Facebook fan page, in particular without

to take action against Facebook as soon as possible.208 The ECJ also has its case law

evolved into shared responsibility. It is now supreme

confirms that even when using social plug-ins such as Facebook's Like button

there is joint responsibility.209

A

and

s

i.e

e

right

P

right

a

x

i

s

As a result of the ECJ judgment on the joint responsibility of Facebook

and Facebook fan page operators, we have a number of test procedures

towards offices of the state administration, political parties and companies

and organizations initiated, in which we are first concerned with the determination of the

The situation went.210 The DSK confirmed its position on responsibility

and accountability for Facebook fan pages and regulatory

chen jurisdiction211 our concerns.

Three of the political parties we wrote to refused to provide information

with reference to our alleged lack of jurisdiction: you would have with Facebook

agreed that the Irish Data Protection Authority will be the lead

authority and thus the sole contact for fan page requests.

driving. However, this view is already wrong at the outset, because the GDPR

207 ECJ, judgment of June 5, 2018 − C-210/16 (Wirtschaftsakademie Schleswig-Holstein)

208 BVerwG, judgment of September 11, 2019 - 6 C 15 18 (Business Academy Schleswig-

Holstein) The decision was made on the old legal situation under the Data Protection

line (Directive 95/46/EG), but essential statements are based on the new legal

position transferrable

209 CJEU, judgment of 29 July 2019 − C-40/17 (Fashion ID)

210 JB 2018, 1 7

211 https://www data protection conference online de/media/dskb/20190405_positioning_

facebook_fanpages pdf



concept of the lead supervisory authority only if the main

Establishment of a controller decision-making and enforcement authority

vis-à-vis the other branches with regard to the processing of personal

of personal data.212 The notion of the lead supervisory authority

means that there is a contact person on the part of the agencies involved

There are supervisory authorities – namely the lead supervisory authority – that are responsible for everyone

supervisory authorities is binding. Equally, though, that it's on pages

of those responsible there is only one contact person - namely the main office

approval – which is the decision of the supervisory authorities in all branches

can implement. This 1:1 ratio, which is mandatory by law,

is not in the case of Facebook fan pages.

The Article 29 Working Party, i.e. the independent European working

group, which before the entry into force of the DS-GVO at European level with the

protection of privacy and personal data

consider that under certain conditions could be common

Those responsible also contractually define the lead supervisory authority.213

We consider the wording there to be misleading and rely on European

technical level in the now newly established European Data Protection Board

(EDSA) for a correction.

For our testing procedures in matters of Facebook fan pages, this question is

However, not decisive, because the established conditions for a determination

tion of a lead supervisory authority by jointly responsible persons

are not present in any case. This would require that the

as a head office within the meaning of the regulations on the lead

branch of a jointly responsible authority applicable to the supervisory authority (here:

Facebook) would have the authority for all joint controllers (all)

to make and implement decisions about data processing. Facebook

however, is not entitled to decide whether the fan page operators use their

run the fan page at all, nor whether they (after recent changes)

changes by Facebook only minor) configuration options

or use the so-called page insights statistics, which provide more detailed statistical information

212 See Art 55, Art 56 Para 1, Art 4 No 16 lit b, Art 60 Para 10 GDPR

213 Article 29 Working Party, Working Paper 244, p. 8 f



provide information about the visitors of the fan page, and on which ones

Legal basis they base their actions on. Likewise, Facebook cannot be unilateral

decide on the scope of processing in joint responsibility

the. All of the fan page operators we contact remain in each

Case obliges the lawfulness of the processing of personal data

and to ensure that we, as the competent supervisory authority, also

assign.214

However, we are in a constructive relationship with most fan page operators

active dialogue. True, they could meet their legal obligations

ultimately consistently fail to comply and, in particular, the legality

not be able to prove the processing, mainly because the data provided by Facebook

provided agreement on joint responsibility is not sufficient

was. However, at the end of October 2019, Facebook had a significantly revised one
Version of the "Page Insights Supplement regarding the person responsible"215
provided. This addresses a large number of the points of criticism that the DSK and we
have expressed, so that some of our questions have been settled. In
However, this addition remains insufficient in relation to the most crucial points:
special are the data processing under joint responsibility
not exhaustive, but only described as an example. So that fan page
examine the lawfulness of the processing and their accountability
However, it is imperative that they understand the scope
conclusively know of the processing and it is ensured that there are no them
unknown processing in joint responsibility. In addition
there are doubts as to whether the agreement actually includes all processing in common
mer accountability, and there are other deficiencies in the area of information
information of the persons concerned. The latter should, however, without further
fix difficulties.
Considerable reservations about data processing in the context of
ment of Facebook fan pages, including doubts as to whether the von
Agreement provided to Facebook all processing steps in common

214 Art 5 Para 2 GDPR

215
Information from Facebook on page insights (https://de-de facebook com/legal/
terms/page_controller_addendum)



mer responsibility covers. In addition, it is conceivable that fan page
driving also subject to sanctions for a possible data protection violation
Facebook are jointly responsible. It can be assumed that these questions

will be busy for a while and for further tests and measures

can lead to

At present, fan page operators can fulfill their legal obligations to

we do not comply with the lawfulness of the processing. A legal one

Operating a Facebook fan page is currently hardly possible. fanpa

ge operators who do not accept the associated legal risks

want to take should ask Facebook to remedy the defects.

13.7 Social Plugins and Shared

responsibility

s

i

x

a

right

P

right

e

i.e

s

and

A

With a judgment of July 29, 2019, the ECJ determined that even when using

Social plug-ins such as Facebook's Like button share responsibility

of website operators and social media services.216 Basically

legendary ECJ ruling on Facebook fan pages217 was the fact that fan

page operators through the operation of their Facebook fan page processing

of data from fan page visitors in the first place, only one of

several justifications for Facebook's joint responsibility

and fan page operators. With the ruling on the Like button, the ECJ has now

unequivocally stated that it is for joint responsibility

It is sufficient if website operators integrate third-party content such as social plug-ins into their

Integrate the website and thereby the processing of personal data

made possible by these third parties.

In addition to the li-

ke button from Facebook almost any type of foreign content that is on a web

page can be integrated. Examples include scripts, fonts,

216 CJEU, judgment of 29 July 2019 − C-40/17; in particular Rn 75f (Fashion ID)

217 ECJ, judgment of 5 June 2018 − C-210/16 (Wirtschaftsakademie Schleswig-Holstein)



Videos, city maps, audience measurement and advertising. Main exception is

the existence of order processing - but such is not to be assumed

men if the third parties also use the supposed order data for their own purposes

may process, as is the case with Google Analytics.218

In this case, the joint controllers must not only have a

26 DS-GVO, but also need one each

Legal basis for processing the data. As the legal basis for the

Disclosure of the personal data of visitors to the

Website towards third parties usually only a consent in terms of

costume.219

In practice, website operators in many cases impermissibly bind third parties

comply, especially with tracking services and advertising networks. often

but also thoughtlessly used standard functions that are inadmissible and also

usually unnecessarily integrate third-party content without the user necessarily doing so

is aware. However, those responsible must verify the legality of their data processing

work.220 This requires precise knowledge of which

data is processed for what purpose and the examination of the lawful

speed of processing. Again and again we find that website operators

cannot provide any information as to which data is generated through the use of third-party

hold for what purpose are processed. It is to be clearly pointed out that

that ignorance does not protect against responsibility.221

We have received a large number of complaints about inadmissible third-party content,

In some cases we examine this ex officio. The procedures are because of

often very expensive due to the large number of third-party content. Against the background of

associated gross violations of the personal rights of the visitors

In this area, users and visitors of the websites are sure to be fined.

expected to drive.

218 See 13 4

219 See 13 3 and 13 4

220 Art 5 Para 2 GDPR

221 ECJ, judgment of 5 June 2018 − C-210/16 (Wirtschaftsakademie Schleswig-Holstein)



189

Anyone who integrates third-party content on their own website processes in most

ten cases personal data in joint responsibility

the provider of this third-party content and must communicate with it

or conclude an agreement with them in accordance with Art. 26 GDPR. Besides that

is consent for the integration of third-party content in most cases

of the visitors of the websites is required. website description

in Berlin should integrate their websites with suitable tools.

review the third-party content. Third party content must either be removed or

be made legally compliant.

13.8 Berlin.de - service portal with problems

s

i

x

a

right

P

right

e

i.e

s

and

A

The city portal Berlin.de is operated as a public-private partnership between the

State of Berlin and a private provider; the advertisements are

outsourced to another provider. The responsibilities are intrans-

parent. However, the visitors of the are all the more transparent

Website: Berlin.de integrates third-party content on a large scale, which

dig the transmission of personal data to the providers of the third-party content

connected is. In any case, the intensive tracking did not go through to the content

the country responsible sides means that also sensitive data of themselves

people who inform about the Berlin offers to various third parties

are given.

Even just accessing the Berlin.de home page is automatically linked to a

enormous number of third parties reported: Our tests showed that over 400 elements of

up to 149 different servers were loaded. Even if our exam

not yet complete, it appears that most of these will be services

to act that create usage profiles for advertising purposes. For inclusion

Such services require the consent of the website visitor

required, such as the DSK in the orientation guide for providers of telemedia

worked out in detail.222 In addition, according to case law,

ment of the ECJ a joint responsibility of website operators

222 See 13 3



and advertising companies, which among other things have an agreement according to Art. 26 DS-GVO

requires.223

On the pages for which the State of Berlin is responsible for content, it looks better

because there is no advertising involved. But even those who use a search

maschine the direct route to the service portal of the state (service.berlin.de)

has found must not feel safe from surveillance: There is also here

Usage tracking - and because of the non-transparent linking of those responsible

areas of land and private providers, it can quickly happen that the

"public" part of the offer is left unnoticed.

For example, if you search the state’s service portal in the “Security and emergency

lay" after the term "AIDS test", there are no results, although there are various

Information from the state on this topic is available - but not in the service

valley. Instead, it is offered to expand the search to Berlin.de as a whole -

which anyone who needs an AIDS test will certainly be happy to do. Without reference to the
Consequences for data protection, the further search then takes place in private
area of responsibility. The search term – sensitive information that
falls under the special legal protection of the DS-GVO224 - is used without consent
of the searchers passed on to a large number of third parties (in our test: 73
third party server). This is partly done in a very targeted manner, partly through technical means
Layout. This is without express and on the specifically sensitive data
related consent of the website visitor inadmissible.
We are conducting an ex officio review procedure for Berlin.de. Further lie
us various notices and complaints about impermissible tracking and impermissible
significant integration of third-party content. The exam will be canceled due to the large
wands still need some time for such tests. However, it is
already noticed that the topic of data protection at Berlin.de is neglected
terically and cannot even be found out internally at our request
the was which personal usage data by whom and to which
purposes are processed. The case law of the ECJ on the question
My responsibility seems despite all information from us or
223 See 13 7
224 See Art 9 GDPR

the various press releases on the subject to those responsible
to have attended. Although we are the Senate in this case about our
have informed you of interim findings, the situation has not yet
bar improved.
The Berlin.de case should be a warning example for website operators and
Reason for critically reviewing their websites. Who Third-Party Content

on your own website usually requires the consent of the

website visitor. Third-party content is particularly critical if the third party

Find out inputs such as search terms for the website operators

may contain uncontrollably sensitive data within the meaning of Art. 9 DS-GVO,

or if from the contents of the website on sensitive information about

Health or political settings can be closed. In the

explicit and specific consent is required in such cases

can hardly be obtained in practice. Third party content must be removed either

or made legally compliant.

13.9 Customer Account Deletion Routine

A citizen complained about an e-mail from a contact exchange in which he

was shared that his profile had been viewed by someone else.

The complainant had initially joined the platform six years previously

Register for free and create a profile. Shortly afterwards he also had a

applies for compulsory membership, which allows him to make contact with others

allowed members. However, he ended it shortly thereafter. There-

after the complainant was no longer active on the platform. his customer

However, denkonto and his profile remained saved. The complainant re-

only realized this when, six years later, he received an email saying

someone looked at his profile.

The storage of personal data in free customer accounts that

not be used for a long period of time is not permitted indefinitely.

Businesses are committed to data minimization. You may

only process gene data to the extent that this is appropriate for the purpose and to the necessary

i

x

a

right

P

right

e

i.e

s

and

A

Chapter 13 Telecommunications and Media 13 9 Deletion routine for customer accounts

agile measure is limited. As soon as the processing is no longer necessary,

personal data must also be processed without the request of the person concerned

then be deleted. For this, companies need personal data

process, provide appropriate internal regulations and measures. She

must check at regular intervals which personal data

are no longer necessary and must be deleted. For this it is necessary

necessary to create a deletion concept, which data will be deleted after which period

and when the deadline calculation begins - information that, by the way, too

to be specified in the privacy statement.225

How long data in inactive customer accounts may still be stored,

cannot be answered in general. This depends on many factors of

on a case-by-case basis, e.g. what purpose the customer account serves, how sensitive the

Data is whether third parties have access to it and much more. m. Here every company must

first make an assessment and regulation for yourself, which we then

can be checked.

In our case, highly sensitive data was stored in the profile, e.g. photos

and information about sexual orientation and preferences. Besides, that was

Profile also visible to other members of the platform. So the data became

made accessible to a wide range of people. This represents a special

invasion of the complainant's privacy.

After six years in which the complainant did not use his customer account

in any case, the company could no longer easily get away with it

assume that he still has an interest in the storage and disclosure of

good information about him. The company would have at least

least need to regularly ensure that a maintenance of the profile

is still desired.

Companies that offer their customers (free of charge) the installation of a

offer customer accounts must be regularly checked, particularly in the case of inactive

frequently check whether the customers are still interested in the

have the right to maintain those accounts and otherwise delete those accounts.

225 See Art 13 Para 2 lit a or Art 14 Para 2 lit a GDPR



14 Europe

14.1 Adaptation of the Berlin state law

the General Data Protection Regulation

s

i

x

a

right

P

right

e

i.e

s

and

A

The General Data Protection Regulation (GDPR) is like any other EU regulation

directly applicable, so that in principle there is no implementation act

the Berlin legislature needed. Nevertheless, the GDPR contains in certain

ten parts of exceptional areas in which the state legislature authorizes and

is obliged to issue supplementary regulations. This concerns in particular

the creation of a legal basis for data processing by public authorities

len. Under certain conditions, the legislature can also

restrict rights. Actually, these adjustments would have the state law

to the DS-GVO by May 25, 2018 at the latest. The current

The timetable provides for the legislative project to be completed by mid-2020

is completed.

Almost two years after the deadline, the legislator is finally on target

cycle The Senate has drafted an article law that contains the necessary

summarize the changes in the Berlin state law and send them to the

netenhaus of Berlin is to be submitted for resolution. in charge

The Senate Administration is responsible for preparing a draft bill

for home and sport. The respective senate administrations responsible for content

work for the Senate Department for the Interior and Sport.

The draft bill provides that a total of approx. 80 Berlin laws and regulations

regulations are changed. Our authority was involved in the drafting of the

involved at least to some extent in the draft and has both the Senate administration

for interior affairs and sport as well as other individual Senate administrations for specific

cal questions.

In our statements, we particularly complained that the referee

design has overshot the mark at various points and the

Administration grants more processing powers than for task fulfillment



would be required.226 In addition, we have opposed restrictions on the

citizens' rights, which also only in very

narrow limits are permissible, some of which have been exceeded.227 Unfortunately,

in the draft bill, not all of our proposals

considers. This is not only a data protection policy problem, but

also goes against higher-ranking European law, since the opening clauses of the DS-

GMOs are inadmissibly overstretched. This also applies in a special way

in relation to sensitive data, the processing of which is particularly important under the GDPR

demands because it involves a particularly deep intervention in the personality

human rights.228

On the other hand, it is positive that the draft law includes a right to be heard

rer authority before the House of Representatives is provided again, which in the first

legislative processes after the GDPR came into effect. All-

However, this only applies in our capacity as data protection officer. In the

In the area of freedom of information, such a right is lacking, as is e.g.

right of appeal229. Here should also the support obligation of the public

bodies are standardized accordingly. Without these authorizations, an appropriate

proper fulfillment of the tasks under the Freedom of Information Act not possible

lich.

Another important area that is completely covered in the current legislative project

lig left out is the area of police and justice. area specific

Technical regulations for the implementation of the so-called JI guideline230 are missing. This also

Reich-specific regulations - in particular the general security and

Regulatory Law (ASOG) - urgently need to be integrated into the European legal framework

be adjusted.

226 See Art 6 Para 1 lit c, e Para 2, Para 3 GDPR

227 See Art 23 GDPR

228 Art 9 GDPR

229 See Section 13 (2) sentences 1-3 BlnDSG

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

2016 on the protection of individuals with regard to the processing of personal data

by the competent authorities for the purpose of prevention, investigation, detection

or prosecution of criminal offenses or the execution of sentences as well as for free data transfer

and repealing Council Framework Decision 2008/977/JHA



The Senate of Berlin has launched a bill. we will

which we continue to use in the legislative process to ensure that data

protection rights of citizens also in data processing

maintained by the public administration of the State of Berlin. It's closed

hope that the draft will be revised accordingly and then as soon as possible

is passed because it contains important regulations for the adjustment of the Berliner

State law on the DS-GVO contains. This also applies to the police sector

and justice and freedom of information.

14.2 How does a guideline of the European

data protection board?

s

i

x

a

right

P

right

e

i.e

s

and

A

With the entry into force of the GDPR, the so-called European data protection

Committee (EDSA) started its work. In this committee are data

safety supervisory authorities of all European member states as well as the European

nical data protection officers.231 An important task is to

to issue general guidelines for the interpretation of the GDPR. With that

Clarity regarding the uniform interpretation of vague legal terms

created in the data protection laws of the EU member states. One

Such a guideline, which our authority has been responsible for, is the guideline for

video surveillance.

Anyone who travels a lot in Europe and pays attention to it quickly realizes that - although we

With the DS-GVO there is now a directly applicable uniform data protection law

have - video surveillance is handled very differently in many places.

In some places, cameras seem to be following our every move and

in other EU member states you can move around freely and unobserved

move. The measures, such as video surveillance made transparent

power seem to vary widely.

This is less due to the cost of such cameras, which are now everywhere

are cheap to get, but rather because data protection laws are very

231 See 14 3





be interpreted differently. First of all, it should be noted that the GDPR

does not contain any special rules on video surveillance. Rather, the video

monitoring are measured against the general clause of Article 6 (1) (f) GDPR

the. This provision provides for a balance between the interests of the

responsible for monitoring and the interests and fundamental rights of the

respected. This balancing of interests is carried out by the responsible

carried out differently by supervisory authorities. For uniform handling

in the field of video surveillance, the EDPB has decided to launch a

to issue guidelines in this regard.

Since we have the freedom to be able to move around in public without being observed

s, for a particularly high and worthy of protection good, has our

was announced as the main rapporteur on this matter. Our

The aim was to achieve the highest possible level of data protection for those affected

reach or maintain and at the same time provide clear guidelines for the companies

so that they can adapt better to the new legal situation.

As the main rapporteur, we initially had the task of developing a concept

wrap and present in a working group of the committee. have after that

together with the co-rapporteurs from France, Sweden, Czech
Chien, Poland and the Federal Commissioner for Data Protection and Information
created a first draft, which was shared with the rest of Europe
data protection supervisory authorities was discussed in said working group. After
The working group has gone through many meetings and tedious negotiations
finally agreed on a draft that was presented on 9 July 2019 in the EDPB plenary session
was accepted.
During the entire process we were supported again and again by
supervisory authorities in other federal states. The integration of the other Germans
Supervisory authorities is not only important for reasons of division of labour. Since the
German supervisory authorities in the EDPB - like all other member states - only
have a voice, a corresponding opinion-forming process must be carried out in advance on national
take place at the onal level. In this case it was helpful to have one of your own
Working group on questions of video surveillance at the level of the conference
Federal and state data protection supervisory authorities (DSK). In this way
interim results were repeatedly presented to the working group, so that the ex-

certise of the members from the federal and state governments could be called up optimally
and close feedback between the European and national levels
was easily possible.
After the adoption by the EDPB, the process of creating the guideline was over
for video surveillance but not yet finished. Subsequently, a so-called
Public consultation carried out. With this form of public participation
have representatives from business, politics and civil society
society, but also interested private individuals the opportunity to express their views
issues and concerns in writing and to make suggestions for changes. To

We received about 100 comments on this guideline. Most came
from companies and business associations from all over Europe, but also from
Asia. We share these opinions with the co-rapporteurs
evaluated and the results submitted to the other European supervisory authorities
presented and discussed by the EDPB working group. At the end of this laborious
gene process is the approval of the proposed changes by the EDPB and
the final approval of the guidelines, which took place shortly after the end of the
period end of January 2020.
The development of guidelines at European level is in each individual case
a long and tedious process that requires a lot of coordination and coordination
national and EU level. Nevertheless, there is no alternative, since the DS-GVO
contains many general clauses that require interpretation. The Berlin representative
for data protection and freedom of information is actively committed to a high level
Level of data protection for citizens and at the same time for clear
and manageable rules for operators of video cameras
speed up



## 14.3 News from Europe - Overview of the work of the European data protection committee

At the latest since the GDPR came into effect, data protection law has become a
European joint project by all EU member states. That requires
a greater willingness to communicate and cooperate about the application
of the data protection regulations under the German supervisory authorities.
on the one hand and among the European supervisory authorities on the other.

A

and

s

i.e

e

right

P

right

a

x

i

s

Particular importance is attached to the diverse coordination requirements

ties to the EDPB, which is an independent European institution and its

based in Brussels. The EDPB ensures the uniform application of the GDPR

of the European Union and promotes the cooperation of the European

data protection supervisory authorities among themselves. It consists of the European

data protection officers and the heads of the EU supervisory

authorities or their representatives. The German data protection

according to the will of the German legislator in the EDSA, only one voting

authorized representative and a deputy

Deputy, although in Germany it is due to our federal system

there are several data protection supervisory authorities.232 Voting representative in the

EDSA is the Federal Commissioner for Data Protection and Freedom of Information

A state data protection officer is entitled to act as a representative

to bring the country's perspective directly to the European level

can. This is of particular importance because the

between federal and state governments are clearly separated and just the area

the economy, which makes up a large part of the cases advised by the EDPB, countries

the thing is. Unfortunately, the Federal Council also more than two years after the entry into force

no person from the ranks of the state data

nominated by data protection authorities. The Hamburg Da-

data protection officer continues to perform this function.

232 Section 17 of the Federal Data Protection Act (BDSG)



One of the tasks of the EDPB is to provide general instructions in the sense of

measures, guidelines, recommendations or even specific handouts such as

e.g. on so-called "best practices"233, in which data protection

terms are clarified. The EDPB also advises the European Com-

mission in all matters related to the protection of personal data and the

change in data protection regulations. Further promote

the EDPB encourages cooperation and the effective exchange of information

information and experiences on best practices between supervisors

hear. Also in disputes between the European supervisory authorities

the EDPB to take action and issue a binding decision. In cases in

where a matter of general application is at stake, he can

publish statement. The EDPB reports every year in an annual report

about his activities.

The committee has several sub-working groups in which women

and employees of the supervisory authorities of the EU member states and the Euro

European data protection officers in Brussels to meet

develop the same guidelines and other documents. In the working groups too

Topics such as enforcement proceedings, cooperation, technology

logy, social media or fine proceedings, the work on the content takes place on the

based on problem cases and key questions. In these working groups

discussed in a compromise-oriented manner and argued productively in order to

concrete and application-oriented questions in connection with the implementation

tion of data protection in the EU. The results of the expert consultations

are then discussed and approved in the plenary session of the EDPB.

The Berlin Commissioner for Data Protection and Freedom of Information represents the

supervisory authorities of the countries in a number of EU working groups and has

thus contributed to numerous guidelines. However, since our authority is not in all

Working groups can be represented, we work closely with the supervisory authorities

other federal states and the federal government together. This means that we

these positions via the respective representatives in the working

bring in groups if we are not represented there ourselves.

233 Engl "Best practice" The term describes proven, optimal or exemplary

Methods, practices or procedures





The most important guidelines, which were developed in working groups of the EDPB and

plenary, one guideline deals with treaties

online services.234 In addition, a guideline on so-called behavioral

rules (codes of conduct) and monitoring bodies in accordance with the regulation

2016/679, which provides practical guidance on interpretation

and in the application of Art. 40 and 41 GDPR.235 This guideline aims

aims to establish procedures and rules for submission, approval and publication

clarification of codes of conduct for specific economic sectors at national and

explained at European level. Already accepted – but still subject

public participation – are the guidelines for video surveillance236

Data protection through technology design and through data protection-friendly pre-

and the "right to be forgotten" in connection with in-

internet search engines.237

The Berlin Commissioner for Data Protection and Freedom of Information acts on the

Guidelines, recommendations and other documents of the European data

protection committee. Through our participation in many of the working groups

of the committee, we are committed to a high level of data protection throughout the EU.

234 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the

context of the provision of online services to data subjects of 8 October 2019

235 Guidelines 1/2009 on codes of conduct and monitoring bodies in accordance with the

Regulation (EU) 2016/679 of 4 June 2019, p. 6

236 See 14 2 Note: This guideline was updated after completion of public

at the EDPB immediately after the end of the reporting period on 29 January 2020

adopted

237 All guidelines can be found at: https://edpb europa eu/our-work-tools/ge-

neral-guidance/gdpr-guidelines-recommendations-best-practices_de and - as far as in

German language available - also at https://www datenschutz-berlin de/info-

library-and-service/publications/guidelines/



14.4 General Data Protection Regulation vs.

Berlin Constitution

s

i

x

a

right

P

right

e

i.e

s

and

A

With the entry into force of the GDPR, the complete

Independence of the data protection supervisory authorities established. The Constitution

von Berlin (VvB) has not yet understood this development.

Art. 47 Para. 1 of the Constitution of Berlin (VvB) currently reads as follows:

"In order to protect the right of informational self-determination, the

a data protection officer. He is appointed by the President of the

appointed by the House of Representatives and is subject to its supervision."

In contrast, Art. 52 Para. 1 DS-GVO regulates that every supervisory authority at the

fully independent in the performance of their duties and in the exercise of their powers

acts gigantic. This is governed by Art. 52 Para. 2 GDPR, which stipulates freedom from instructions

expressly and comprehensively constituted, concretized.

The requirement for the independence of the data protection authorities from Art. 52 Para. 1

DS-GVO is anchored in primary law238 in the contract on employment

wise of the European Union (TFEU)239 and in the Charter of Fundamental Rights of the

European Union (GRCh)240, which provide that compliance with data protection

is to be monitored by independent authorities or bodies.

In its judgment against Germany241 the ECJ specified the requirements

to "complete independence" by making it clear that the decision-making

walt of the data protection supervisory authorities of any external influence

it must be withdrawn, directly or indirectly, “by the questioned

could be that the control bodies mentioned are doing their job of protecting the

Right to privacy and free movement of personal data

238 Primary law is the highest-ranking law in the EU

239 Article 16 (2) sentence 2 TFEU

240 Art 8 para 3 GRCh

241 ECJ, judgment of 9 March 2010 – C-518/07





To bring balance, to fulfill”.242 State supervision “no matter what

Art" allows such influence. Even if the supervision of a

In practice, the higher authority regularly does not issue specific instructions

the supervisory authorities, the mere danger of exerting political influence is enough

to impair their independent performance of duties.243

The official supervision of Berliners, which is still regulated in the Berlin constitution

Commissioner for Data Protection and Freedom of Information by the President of the

House of Representatives violates Art. 52 Para. 1 and 2 GDPR. Another

The decision of the ECJ in its judgment against Austria244 leaves room for interpretation

not to.

In this he evaluated the civil service supervision of the business

leading member of the Austrian Data Protection Commission despite the

strongly secured freedom from instructions and functional independence

Commission as a violation of Art. 28 para. 1 subpara. 2 Data Protection Directive

(old)245. In this respect, it is sufficient to point out that it cannot be ruled out that

that the assessment of the executive member of the Data Protection Commission

sion by the superior, with the official advancement of this official

should be promoted, in this to a form of "anticipatory obedience"

could lead.246 The Data Protection Commission was so due to the ties of its

res executive member to the political entity under their control

Organ not above any suspicion of partisanship.247 Against this background

For this reason, the majority of the literature also assumes that supervisory supervision

242 ECJ, judgment of 9 March 2010 – C-518/07, paragraph 30

243 CJEU, judgment of 9 March 2010 – C-518/07, paragraphs 32-36

244 CJEU, judgment of 16 October 2012 – C-614/10

245 Directive 95/46/EC of the European Parliament and of the Council of 24 October

1995 on the protection of natural persons with regard to the processing of personal data

ten and to free data traffic, out of effect since the beginning of the GDPR

246 ECJ, judgment of 16 October 2012 – C-614/10, paragraph 51

247 ECJ, judgment of 16 October 2012 – C-614/10, para. 52, ZD 2012, 563



about members of the supervisory authority not with the requirement "complete independence

pendency" from Art. 52 Para. 1 DS-GVO is to be agreed.248

The opinion of the Commission in the

breach of contract proceedings against Germany (No. 2003/4820).249 Accordingly

the supervision existing in the administrations to the requirement of a "complete

gene independence" in contradiction, since not with certainty bordering on certainty

possibility can be ruled out that the respective employer on this way

could attempt to unduly influence the decisions of the control body

gain weight. The German legislature made similar considerations in its

Explanatory memorandum to the second amendment to the then Federal Data Protection Act

set, with which from a service supervision for the Federal Commissioner or
the Federal Commissioner for Data Protection and Freedom of Information
would see. A waiver of the supervision is therefore necessary, "to the
formal appearance of an indirect influence on the official performance of
to prevent from the outset", even if a supervision neither the possibility
bility opened, direct influence on decisions of the data protection authority
exercise, nor the possibility to overrule or enforce these decisions
set.250 Something else can therefore not for the data protection officer
apply at state level.

Art. 52 DS-GVO only opens up limited leeway for the member states
ten. In particular, paragraphs 1 to 3 are directly applicable at the national level.
Bares EU law251 and thus national law takes precedence.252 In the case of
Violations of the member states against Art. 52 DS-GVO can prevent the supervisory
Authorities directly refer to the GDPR and judicial legal protection

248 Gola DS-GVO/Nguyen, 2 Auf 2018, DS-GVO Art 52, para. 12, 13; Ehmann/Selmayr/
Selmayr, 2 Auf 2018, DS-GVO Art 52, para. 17; Kühling/Buchner/Boehm, 2 on 2018,
DS-GVO Art 52, para. 25; Taeger/Gabel/Grittmann, 3 Auf 2019, DS-GVO Art 52, Rn 15;
Paal/Pauly/Körffer, 2 Auf 2018, DS-GVO Art 52, para. 3; Simitis/Hornung/Spiecker
gen Döhmann, data protection law, DS-GVO Art 52, para. 8

249 Opinion COM infringement proceedings against Germany No. 2003/4820, p. 5

250 Draft law for the second law amending the Federal Data Protection Act -
Strengthening the independence of data protection supervision in the federal government through establishment
a supreme federal authority, BT-Drs 18/2848, p. 13

251 Paal/Pauly/Körffer, 2 Auf 2018, DS-GVO Art 52, para. 2; BeckOK data protection R/
Schneider, 29 Ed 1 August 2019, DS-GVO Art 52, para. 1

252 ECJ judgment of 15 July 1964, Rs 6/64, Costa/ENEL

search.253 If Art. 47 VvB does not meet the data protection requirements

be changed accordingly, a renewed breach of contract

threaten proceedings against Germany.

A wording of Art. 47 Para. 1 VvB that conforms to European law could look something like this

are as follows:

"To protect the right to informational self-determination, the

liner House of Representatives a data protection officer or a data

applied. She or he will be appointed by the President of the

appointed house. The Berlin representative for data protection and

Freedom of information acts in the performance of her or his duties or at

completely independent of the exercise of his or her powers and not subject to instructions."

Art. 47 Para. 1 VvB is contrary to European law and should be changed.

253 BeckOK data protection R/Schneider, 29 Ed 1 August 2019, DS-GVO Art 52 marginal number 1

205

15 information obligation

data breaches

15.1 General Developments

Last year we talked about the new requirements for data

General Protection Regulation (GDPR) with regard to reporting and information obligations

of those responsible for data breaches254 reported.255 Were there in 2018

a total of 357 reports, which is already a sharp increase compared to

Last year meant 256, so the reporting period was another sharp increase

of the reports to be recorded on 1017.257

We are often asked by those responsible who have reported a data breach and

met (possibly as a precautionary measure) whether they were informed as a result of the report

could expect a sanction. In accordance with Section 43 (4) of the Federal Data Protection Act

(BDSG) may report a data breach in a procedure under the law

about administrative offenses against the reporting person or notification

the or his relatives only with the consent of the person required to report or

information.258 This provision in the BDSG serves to

safeguarding the principle that no one may be forced to

254 See Art 33, 34 GDPR

255 JB 2018, 1 3

256 It should be noted that the figures will not be available until the end of May when the GDPR takes effect

increased

257,874 reports in the non-public area, 143 reports in the public area

(Status: 31 December 2019)

258 According to the explanatory memorandum to § 43 Para. 4 BDSG (BT-Drs 18/11325, S 109).

the regulation is based on the opening clause of Art. 83 Para. 8 DS-GVO, where

according to which appropriate procedural guarantees must be created





in criminal or administrative offense proceedings.259 That's how it should be

Tensions in which those responsible are located are resolved,

because they are either due to a data protection violation that is subject to sanctions

accuse yourself or - to avoid this - against the reporting and notification

breach the obligation to correct, which in turn can be sanctioned.260 The

means that based on the information in the report alone, no fine will be imposed

may be imposed.261

However, it is questionable whether this also applies if the supervisory authority is still

finds out about the data breach in another way, e.g. through a complaint

affected person. The decisive factor here is whether the complaint as a direct di-

Direct reaction to the notification of those affected by the person responsible

done. However, even in these cases, a warning262 due to

the substantive data protection breach underlying the breakdown,

to be pronounced.

15.2 Individual Cases

Several day care centers have reported to us that digital cameras take photos

stolen from excursions with children and educators. All responsible

both the affected employees (as a precaution) and the

affected parents either with an information letter or by posting it in

informed the day care center about the incident - rightly so, because the risk that the child

259

"Nemo tenetur se ipsum accusare"; This principle is one of the recognized ones

Principles of a rule of law procedure and is by Art 2 Para 1 in conjunction with Art 1

Paragraph 1 of the Basic Law (GG) constitutionally guaranteed ("freedom from self-incrimination

obligation", see BVerfG, decision of April 27, 2010 - 2 BvL 13/07) The basic

Incidentally, the sentence is an expression of the fair trial principle in Article 6 of the European

shen rights convention (right to a fair trial)

260 Art 83 para 4 lit a GDPR

261 According to another view, the ban on use in Section 43 (4) BDSG is

contrary because there is no "reasonable" procedural guarantee in the sense of the opening clause of the

Art 83 Para. 8 DS-GVO, but beyond those procedural guarantees

emanates, which are required under European law Sun Kühling/Buchner/Bergt, 2 Auf 2018,

Section 43, margin no. 13; similar to the State Commissioner for Data Protection and Freedom of Information Ba-

den-Württemberg, 33 activity report, p. 17

262 Art 58 Para 2 lit b GDPR

207

Sharing photos through shady channels on the internet is sadly a thing these days

high.

The State Office for Health and Social Affairs (LaGeSo) reported to us that it

Apparently a total of 18 dictation machines at three district offices, a district court and

a tax office have submitted the personal dictations via public health officers

included investigations. After the LaGeSo had identified the error,

immediately asked the administrations to delete the dictations without reading them.

Nevertheless, we have demanded from LaGesSo that all dictation machines be

returned to the LaGeSo and they were examined by a person with IT expertise

and the official data protection officer to check whether

all dictations are completely and irretrievably deleted. The LaGeSo followed

our demand.

We received a message from the company that organizes the annual Berlin Mara

organized. There was a technical error in the database in one

time window of approx. 15 hours meant that marathon participants

could look at the emergency contact details of other runners,

whereby they are assigned the emergency contacts to the respective runners

runners was not possible. The total number of emergency

case contacts (each with name, date of birth and telephone number) amounted to

to 5,242 and affected people from across Europe. That's why it was

a "cross-border processing".263 As the lead in Europe, we have

competent supervisory authority is processing the case. The person responsible has affected all

Do not inform your emergency contacts directly if you do not have an e-mail or postal address

but has a notification letter for the runners

ben with a request to inform their emergency contacts.

A decrease in reports of data breaches is still not to be expected,

currently the numbers are still rising and it is about to level off

start at a high level.

263 See Art 4 No. 23 lit b GDPR





lungs in data protection

16.1 Brexit – consequences of a (no) deal

The withdrawal of the United Kingdom of Great Britain and Northern Ireland (UK).

of the European Union, commonly known as Brexit, was originally intended for

Scheduled for March 29, 2019. At their special summit on April 10, 2019, the

EU states have been granted a Brexit delay until October 31, 2019 at the latest.

is correct. Just before that deadline they have another UK application

to extend the deadline by January 31, 2020 at the latest.264

The conference of the independent federal data protection supervisory authorities

and the countries (DSK) has companies, authorities and other institutions

in Germany information regarding the legal situation regarding the data

ten protection after Brexit.265 In the process, between a

exit regulated on the basis of the exit agreement ("Deal-Brexit") and a

a no-deal Brexit. In the first case applies

EU law, including the GDPR, for a transitional period that is unique

can be extended by a maximum of two years until the end of 2020. While

this time, personal data could enter the UK under the same conditions

regulations are transmitted as before. In the second case, the UK becomes one

Third country within the meaning of the GDPR. Persons responsible for the personal data

If you want to transfer jobs in the UK, you would then have to include the data transfers

secure the special measures according to Chapter 5 of the GDPR.266 As long as it

no determination as to the adequacy of the level of data protection in the UK,

264 European Council Decision of 28 October 2019 – EUCO XT 20024/2/19, REV 2

265 DSK resolution of March 8, 2019, available at www data protection conference

online de/beschluesse-dsk html

266 See EDPB information of 12 February 2019 on data transfers in the framework

of the GDPR in the event of a no-deal Brexit (available as a German working translation

at https://www bfdi bund de/SharedDocs/Publikationen/DocumentsArt29Group_

EDSA/Other papers/EDSA_Info_NoDealBrexit_Arbeits%C3%BCbersetzung htm-

l?nn=5217120)



would there be data transfer instruments such as the standard data protection clauses or

binding corporate data protection regulations. Also

a code of conduct267 or a certification mechanism268 could be appropriate

provide these guarantees for the transfer of personal data to the UK.

What are the requirements for these new instruments according to the GDPR

are, will result from the guidelines that the European data protection

schuss (EDSA) intends to say goodbye in the coming year.

All bodies that want to transfer personal data to the UK are

well advised to take all necessary precautions for lawful data flows

meet.

16.2 Report from the Berlin Group

In 2019, the international working group on data protection met in the

Telecommunications (IWGDPT) as chaired twice for many years

the Berlin Commissioner for Data Protection and Freedom of Information.

16.2.1 Spring Meeting

s

i

x

a

right

P

right

e

i.e

s

and

A

At the spring conference on April 9th and 10th in Bled, Slovenia, protection stood

of children at the center of the deliberations. Two working papers were agreed

be divorced: On the one hand, on data protection for online services that (also)

aimed at children and on the other hand at smart devices with which they play

or learn.

Children are particularly at risk when using online services. you ver-

spend considerable time with online services: with websites and those there

content provided, with social networks and similar services

people, with apps on their smartphones that many have been using since they were

sit, with communication services running on these smartphones

267 Art 46 Para 2 lit e GDPR

268 Art 46 Para 2 lit f GDPR

Chapter 16 International developments in data protection 16 2 Report from the Berlin Group

Play on smartphones, PCs and game consoles and with voice-controlled assistants

assistance systems. Also, their ability is only emerging, informed about the

decide to disclose data that affects them or those around them. The

Intentions of the companies providing the Services or those involved in them

involved in provision, as well as many risks associated with the use

they are not yet aware of. The Consequences of Unintentional Revelation

and use of data concerning them can range from minor annoyances to

far more serious impairments, up to and including sexual exploitation

by other users of the services they visit.

The paper published by the working group focuses on the risk

ken of the improper processing of data about children by the

Operators of the services and the service providers integrated by them.

It identifies the existing risks and makes recommendations, on the one hand

for authorities and for the regulation of the services by laws and other

on the other hand for the companies that provide the services. This recommendation

genes relate to the obtaining of valid consent by the legal guardian;

sufficient transparency about the planned data processing

Information both for the parents and - in a way adapted to the target audience -

appropriate language and form – for the children themselves; Data protection through technology

design and privacy-friendly defaults built into the Services

should be grated; the deletion of data necessary for the provision of the services

are no longer relevant and the granting of the right to information and the

Right to transfer of the data stored in a service to another

their, possibly more privacy-friendly.

Smart devices intended for children include electronically controlled and possibly
Internet-connected toys, "smart" electronic watches and
such as baby monitors and other child monitoring devices. These devices
use the connection to the Internet to determine their location (and thus the
to determine the whereabouts of the children), to transmit data with which the
Children's behavior can be monitored by parents, and linguistic
to enable communication. They record the names of the children and the
Sons in their environment, image data, data on whereabouts and behavior
and possibly even health data of the children. Unfortunately, international
national experience has shown that some manufacturers of such toys or

advises on the rights of consumers and the protection of their
have paid far too little attention to data. Some toys had to
withdrawn from the market by order of regulatory authorities.
Here, too, the working group analyzed the associated use of such devices and
Toys associated risks and formulated recommendations. The determined
The greatest risks extend to opaque and excessive data collection
and processing, excessive storage of the collected data and their
unauthorized secondary use, insufficient security of the devices and the
Communication with the service providers with whom they connect, as well as
otherwise unlawful processing operations.
Often manufacturers use highly vague general business terms
terms and privacy policy. From such deficient documents
it is regularly not clear to which other companies and institutions the
data recorded with the devices for which purposes are passed on
the. Storage periods are also not specified. As a rule, the

Manufacturers also reserve the right to change the provisions at any time. Due to the-

Art of defective information, informed consent is not possible and the

frequently carried out data processing that goes beyond the mere provision of the

go beyond the service associated with the devices remain without legal

basis. Devices and toys that provide a way to control the processing

instructions, make them misleading and misleading in the instructions

the parents and their children to adopt privacy-unfriendly practices that

they specify by default to accept. Often grant serious

and easy-to-exploit vulnerabilities give unauthorized third parties control

via data and recording devices (often microphones, sometimes also cameras). If

Update functions are not provided or updates are not provided

den, these gaps cannot be closed either.

The paper follows up on this analysis with a series of recommendations that

primarily to the manufacturers, but also to the parents and other custodial

to schools and teaching staff as well as to the data protection supervisory authorities

judge yourself.



16.2.2 Autumn Conference

The second meeting of the year focused on working on a paper

Tracking and profiling of people when using web offers,

which is to be completed and approved in the coming year. More the

were sensor networks and assistance systems that were activated by speech or gestures.

be controlled.

The working group also used this meeting to evaluate its activities

and the new work regulations that she had given herself two years ago. There

the range of topics worked on in the working group has spread over the years

tert, it was also decided to change the name. The new name is “In-

International Working Group on Data Protection in Technology”.

The Berlin Group enjoys great international recognition. The through her

adopted papers have the inestimable advantage that they are international

nal are coordinated on a broad basis and therefore as well as due to the in them

concrete recommendations for action that are usually contained, a technically reliable one

Offer orientation in difficult data protection issues.

213

# 17 Freedom of Information

## 17.1 International Developments

From March 10th to 13th, 2019 the International Conference of Information

commissioned (ICIC) in Johannesburg/Republic of South Africa. There was

lution decided to act as a permanent network in the future, and the so-called

ICIC Johannesburg Charter agreed as a first set of rules.269 The

conference a regulatory framework in favor of a more constant organization

received. Guidelines and regulations for admission and participation

ment formulated by members.

The Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI) has

took part in the conference and meanwhile the accreditation procedure

successfully completed. As a member of the ICIC270, she is entitled to attend the closed

attend meetings of the annual meetings.

For this conference, the BlnBDI together with the Federal Commissioner for

Data protection and freedom of information from the Conference of Information

Commissioner for Freedom in Germany (IFK) adopted positions last year

tion paper on the issue of administrative transparency when using algorithms

rithmen271 introduced in a slightly abbreviated version to this important

Topic to achieve an international positioning. The paper is

is circulating and is intended to be revised in this way and approved by the ICIC

be decided.

269 www information commissioners org

270 www information commissioners org/berlin

271 See JB 2018, 13 1



## 17.2 Developments in Germany

### 17.2.1 Freedom of Information Cooperation

commissioned

This year, the IFK took place under the chairmanship of the independent data protection

in the center of Saarland. With the position paper "Information

Easier access to information in the authorities through 'freedom of information by design'"

the conference called on the legislature to change the legal basis and

to create framework conditions so that the public administration

ments to freedom of information from the outset in the design of their

IT systems and organizational processes.272

In addition, the freedom of information officers have agreed in a resolution

sion for more transparency in political decision-making processes

chen.273 The legislator was asked to introduce a mandatory lobby register

to introduce, in which the interest groups at least stating their

must enter their job and activity in the respective decision-making process.

Such lobby registers already exist in other countries.274

17.2.2 New federal law

In April, the Law on the Protection of Trade Secrets (GeschGehG) came into force

entered into force.275 The European “Directive on the Protection of

confidential know-how and confidential business information (business

272 IFK position paper of June 12, 2019, available at www datenschutz-berlin

de/infothek-und-service/publications/decisions-freedom-of-information/

273 Resolution of the IFK of June 12, 2019: Transparency in the context of political

divorce processes – introduce mandatory lobby register, available at www

data protection-berlin de/infothek-und-service/publications/decisions-information-

freedom of mation/

274 For example in Denmark, France, Ireland, Lithuania, Slovenia, Canada and the USA

275 See Federal Law Gazette I 2019, p. 466 et seq



secrets) from illegal acquisition and illegal use and disclosure

lege”.276 In the new law, the term trade secret

defined differently than previously by the case law of the Federal Constitutional

concretized by the court. According to this case law, operating and

trade secret all facts, circumstances and

understood events that are not obvious, but only to a limited person

accessible to the public and the legal entity participates in their non-disclosure

has a legitimate interest.277 According to the legal definition in the new law, it comes

now also on the economic value of the information and on

appropriate confidentiality measures.278

This means that the hurdle for justifying a protection requirement for business

secrets higher than defined by the Federal Constitutional Court for years

predetermined. Because the rightful owner of the secret must

according to appropriate confidentiality measures" with regard to non-

known information. If such measures are missing, there is no

business secret and therefore no special need for protection

to the undesired use of the information.

Whether the legal definition of the new law will affect the

has trade and business secrets to be checked under the Freedom of Information Act,

is discussed, but against the background of the clear wording of the

Law and justification questionable: The GeschGehG expressly stipulates that

that public law regulations on secrecy, acquisition, use

or disclosure of trade secrets;279 beyond that

after the justification of the law, the application of the law, etc. for information

tion claims against government agencies are excluded.280 Accordingly

the Berlin Administrative Court (at least so far) also assumes that the

276 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June

2016, OJ L 157 of 15 June 2016, p. 1

277 BVerfG, decision of March 14, 2006 – 1 BvR 2087/03, 1 BvR 2111/03

278 § 2 No. 1 a), b) GeschGehG

279 Section 1 (2) GeschGehG

280 BT-Drs 19/4724, p. 23



Regulations of the GeschGehG in the area of freedom of information are not applicable

are.281

17.2.3 New State Laws

After the states of Bremen, Hamburg and Rhineland-Palatinate, Thü-

wrestle about a transparency law and thus about a more modern information

right to freedom, which grants people free access to state information

information via a transparency portal on the Internet. Still there

But there are three federal states that have neither a freedom of information nor a

have a transparency law: Bavaria, Lower Saxony and Saxony.

17.3 Developments in Berlin

Fortunately, the first steps towards transparency have also been taken in Berlin.

set recognizable. For example, the FDP parliamentary group has drafted a Berlin transparency

brought into the House of Representatives.282 A hearing of

Experts in the lead committee for communication technology and data

ten protection instead.283

Beside it has an alliance of 40 civil society organizations around

the Open Knowledge Foundation Germany e. V. and Mehr Demokratie e. V

initiated a “People’s Decree on Transparency Berlin”.284 It includes

its own draft law for a Berlin transparency law. In December

the more than 30,000 signatures were handed over to the Senate. heart

of both initiatives is the obligation of the State of Berlin to actively publish

of information on the Internet.

281 VG Berlin, judgment of June 26, 2019 - VG 2 K 179 18

282 Abghs -Drs 18/1595 of 16 January 2019

283 KTDat, meeting of 25 November 2019

284 https://volksentscheid-transparenz de/



Towards the end of the reporting period, the Senate Department for the Interior and

Sport, as the lead administration, drafted an initial key issues paper for a transparency

formulated. The fulfillment of the coalition agreement of 2016 is moving in

a little closer to that point.285

285 See already JB 2018, 13 2 1



18 From the office

18.1 Developments

Over the past year we have detailed about our first experiences

as the supervisory authority for data protection after the data protection

General Data Protection Regulation (GDPR) on May 25, 2018.286 As a result

we had to realize that the workload in the entire authority through

the immensely increased number of petitions, complaints and requests for advice

could hardly be managed. The development observed at that time has changed

continued dynamically in the reporting period.

When data breaches are reported by companies and other

verbatim, all of which were researched and provided solutions within tight deadlines

have to be supplied, there has been a seventeenfold increase in the processes

ben.

The number of complaints from citizens relating to their

Rights under the GDPR is consistently high. On average, mo-

Of course, we received almost 400 submissions from affected citizens. There-

with , citizen petitions have tripled permanently since May 2018.287 Through

the large number of processes was the service center for citizen submissions, in which the first

processing of complaints (e.g. examination of factual and local

quality, completeness of the documents, etc.) is carried out centrally, so overloaded that

that the timely processing of the cases could only take place to a limited extent.

All incoming complaints - but also all cases in which the Berlin

commissioned for data protection and freedom of information (BInBDI) ex officio

is active, as well as the data breaches reported by those responsible - must

after the GDPR has come into effect, it can now also be checked whether

there is cross-border data processing. To use this for us as a

286 JB 2018, 14 1

287 See 18 2 1



supervisory authority to be able to cope with a new task was already in the previous year

Service center for European affairs set up.288 The labour-intensive processing

processing of cross-border cases is carried out there by specialized service

forces under the highest legal and technical requirements, in addition

under great time pressure and largely in English. The required

Coordination with the other national and European supervisory authorities

takes place via the Electronic Internal Market Information System (IMI). Until now

were around 760 cases across Europe to determine the lead and the

concerned supervisory authorities in the IMI system. In over 360 cases

it was determined that the BlnBDI was affected, so that we can deal with the content

had to deal with the reported facts. A total of 35 cases were reported in

IMI processed under our leadership.

The sanction procedures to punish established data protection law

Sanctions are imposed centrally in our authority in the service center.

works.289 The vast majority of cases are now reported after the new

Fine regulations processed, which in several proceedings on fines in re-

levant height according to the new assessment criteria. To the one with the

Effective date of the new GDPR regulations, in particular for prosecution

of administrative offenses to be able to apply effectively and efficiently

the area of sanctions was reorganized and staffed during the reporting period

structured.

Our offers for teaching data protection and media competence in particular

In the period under review, we expanded our special focus on children.290 The very high

Demand in connection with the project days that we have on the subject of data

protection and media competence in schools shows the immense

allowed in this area. This can be done with the resources available to us

and resources are not nearly covered, which is why we are too

are increasingly looking for cooperation partnerships and networks. We have ours

Children's website www.data-kids.de fundamentally revised and redesigned.

The nomination of this site for the German children's software award TOMMI and

288 See 1 5

289 See 12 1 to 12 4

290 See 5 6



Reaching the finals in this year's competition shows us that we can

are on the right track.

Due to the implementation of the regulations of the DS-GVO, the agency is in all areas

are exposed to extremely high loads. That the tasks at least

rudimentary could be done is not least on the remarkable

commitment of the highly motivated employees.

Backlogs in processing could only be achieved through the performance of a large number

in overtime and partly in weekend work. This permanent

However, excessive workload on the part of the staff has also led to sick leave

falls and is not sustainable as a permanent condition.

Fortunately, the budget legislator has reacted to these abuses

and for the years 2020/2021 a noticeable improvement in staffing levels

decided by the BlnBDI. While this will not result in an immediate change in the

described situation, as the posts (spread over two years) initially

written and staffed, and so will the new employees

have to be incorporated first. With the provision of the new personnel

However, there is now a tangible prospect that the tense

situation will noticeably improve over the next two years.

The new European regulations of the GDPR have led to a permanent

multiplication of the tasks of the BlnBDI. It's very gratifying that

the Berlin legislature reacted to this and by strengthening the per-

for our authority in the budget 2020/2021 a strong sign for

set the importance of data protection in Berlin.



18.2 From the Citizens' Submissions Service

18.2.1 Submission development, statistics, content

Trends, conceptual approaches

s

i

x

a

right

P

right

e

i.e

s

and

A

Even after the GDPR has taken effect, the processing of entries

gave one of our most important tasks. The service center for citizen submissions is

the first point of contact for incoming citizen submissions such as complaints,291

general information or requests for advice.

All receipts are first sighted in the service point, with a first

assessment is made. Both the factual and the local

consistency checked. In addition, it is checked whether the entries are complete and

all necessary documents are available.

A complaint can only be processed by us if there is a violation

against data protection laws when processing personal data

is excluded. Some of the general inquiries can be

tests can already be answered in full at the service point. The

remaining inquiries and the (completed) complaints will be

then forwarded to the relevant specialist departments for processing

ben. Should citizens contact us with concerns, where

we cannot help you further due to a lack of responsibility,

we send these to the responsible authorities such as the supervisory authorities of others

Federal states, the Federal Network Agency, to consumer protection organizations or

also to the law enforcement authorities.

After the emergence of complaints with the entry into force of the GDPR

initially quadrupled, the number of submissions has been at a high level ever since

remained constant. On average, almost 400 citizen petitions have been submitted every month since then

what is a tripling compared to the input figures from the time before

GDPR means.

291 Art 77 GDPR



A large number of the complaints are complaints regarding

data information that was not or not fully provided or because it was not provided

Deletion of personal data. Very often it is also about the receipt of

unsolicited emails and newsletters.

A large part of the incoming citizen petitions concern companies from the

rich economy such as online shops, delivery services or social networks. There-

In addition, there are also subject areas such as the housing industry, health, finance

nancial services and employee data protection are strongly represented.

On the one hand, we consider the increase in the number of complaints to be a

ches sign, because it shows that the citizens their

Know your rights and make use of them. However, the number of

Unfortunately, at the same time, complaints that the data protection laws

The rights of citizens are too often disregarded by companies

become.

The number of complaints is also in the second year of the effectiveness of the DS

GMOs remained consistently high. This shows that the GDPR has been in place from the start

and has had a lasting effect on those affected changing their data protection

Know your rights and assert them.

### 18.2.2 My Perfect Complaint - Notes on

### Complaints Procedure

Complaints from citizens about violations of

rights are the main source for proceedings conducted by us. To those affected

To make your input easier, we offer an electronic

cal complaint form.

In order to be able to act as a service point for citizen submissions of the BInBDI for the person concerned

In order to be able to take action, we need in particular information about the data

responsible for data processing. Due to the complexity of the data

property right is an abstract evaluation of the process without specifying the

responsible body usually not possible. The service center also requires

223

A

and

s

i.e

e

right

P

right

a

x

i

s

citizen submissions for the processing of the respective complaint, a precise description

Description of the facts relevant to data protection law and, of course, address

stated what the violation of data protection rights actually consisted of.

The submission of suitable evidence (e.g. e-mail or correspondence

with the responsible body or other documents that prove the violation

may) be helpful. This saves the person concerned from having to ask our

and thus also serves to process the complaint more quickly. Generally

should the supervisory authority be informed of measures that

have seized themselves.

The aim of most complaints procedures is to enforce an existing,

but not granted claim from the so-called data subject rights292; this against

about the person responsible for data processing

first of all the data subjects themselves. Data subjects can, for example, write to

Liable to contact authorities or private bodies and for information about the

ask them stored data. There is also the possibility of processing

to object to their data or to have the data corrected or deleted

request if the relevant conditions are met. Unless one

such concerns of the data subject on the part of the body addressed

is not met or not met in a timely manner, it has the right to contact a

to complain to the data protection supervisory authority.

The submission of documents that support the facts described can

for better assessment of the process and faster completion of the

contribute to the procedure. Especially if a violation of data protection regulations

writings due to conflicting statements from the person concerned and responsible

literal passage cannot be determined beyond doubt, the template may be more suitable

Evidence for examining the alleged data protection violation very much

be helpful and contribute to clarifying the facts and a ascertained

th infringement then, if necessary, to be punished.

292

Specifically, the rights to self-disclosure (Article 15 GDPR), rectification (Article 16

DS-GVO) or deletion of your own data (Art. 17 DS-GVO); also the rights to

Restriction of processing (Article 18 GDPR) or objection to it (Article 21

DS-GVO) and the right to data portability (Article 20 DS-GVO)

Our complaint form293 lists exactly what information the

Service center for citizen submissions from the person concerned and, if necessary, other

share needed. These details can either be sent by post or also

can be sent digitally directly to the Citizens' Entries service point. a

coding also ensures data protection-compliant transmission in the latter case.

lung.

As soon as the Citizens' Entries Service Center has all the required information and

there is local jurisdiction on our part, the complaint will be

assigned to the relevant department. The specialist departments process the complaint

closing under their own responsibility, provide regular information on the status

of the procedure and grant after the end or discontinuation of the procedure

a closing message.

Thanks to the many submissions from citizens, numerous

rich data protection violations uncovered and those responsible for accounting

to be pulled. These inputs are an important tool to

ensure long-term compliance with data protection laws and

to prevent data protection violations.

## 18.3 Cooperation with the Berlin House of Representatives

The Committee for Communication Technology and Data Protection (KTDat) met

in 10 meetings in which the BlnBDI comment on various topics

and could make recommendations. Subject of consideration in committee

were a Berlin transparency law,294 Jelbi – the so-called mobility app of the

BVG,295 the malware infestation at the Berlin Court of Appeal296 and the so-called

Digital Pact Schools297.

293 https://kontakt datenschutz-berlin de/

294 See 17 3

295 See 4 1

296 See 2 4

297 See 5 4



On the occasion of the one-year anniversary of the GDPR, the BlnBDI invited MPs

of all parties represented in parliament in the Berlin House of Representatives

24 May to a parliamentary breakfast at your office. The aim was

it to present the working methods of the authority to the parliamentarians and in particular

or the procedures changed by the new European regulations

to illustrate. In a lecture, employees presented

the individual work steps for data protection complaints with cross-border

future reference, which is carried out in close cooperation with other European supervisory

authorities are processed. In another keynote speech, the

worked on and supplemented the media-pedagogical offer of our authority, www.

data-kids.de. Afterwards there was time for the participating MPs

neten, with the data protection officer and their employees

to come and ask more questions. As the format proved to be successful

proved, further events of this kind are planned.

18.4 Cooperation with other entities

The 2019 conference of the independent data protection

Federal and state supervisory authorities (DSK) met on 3./4. April on the

Hambach Castle and on 6./7. November in Trier and made numerous

closures and resolutions on current issues of data protection.298 Three

Intermediate conferences took place on March 22 in Berlin and on June 25 and October in Mainz. The after the GDPR came into effect proved its worth revised rules of procedure of the DSK in several cases and proved to be constructive and purposeful.

The Conference of the Freedom of Information Officers in Germany (IFK) met on June 12 in Saarbrucken. She passed a resolution introducing a mandatory lobby register for more transparency in the context of political

298 All resolutions and resolutions of the DSK can be found on the DSK website. available: https://www datenschutzkonferenz-online de/entschlussen html https:// www datenschutzkonferenz-online de/beschluesse-dsk html



decision-making processes and a position paper on easier information passed in the authorities through "freedom of information by design".299

The Berlin Group (IWGDPT) met under our chairmanship on 9./10. April in Bled (Slovenia) and on 10./11. October in Brussels (Belgium).300

## 18.5 Public Relations

The media interest in the work of our authority is also in the year 2019 increased again compared to the previous year. This year we answered a total of 245 press inquiries. While in 2018 the general theme was the DS GMOs and their implementation in business and administration were in the foreground, the public was particularly interested in the specific ones this year Effects of the GDPR. The question always arose as to whether and to what extent we have already made use of our possibilities, to impose sanctions under the GDPR. Three known fines divorces301 resulted in a particularly large number of enquiries, including from the European

ic abroad.

Other topics that were of great interest to the media public

were test procedures carried out by us against the bike-sharing provider

Mobike and the video app TikTok. Also safety deficiencies in connection with the

Information systems of the Berlin police and their misuse

kept our press office busy. Our press team was

nalists and journalists are available on these and many other topics,

thus the sometimes difficult legal and data protection issues

Questions in media reporting are presented in a comprehensible and correct way

could.

299 Both documents are available on our website: https://www datenschutz-ber-

lin de/infothek-und-service/publications/decisions-freedom-of-information/

300 For the results see 16 2

301 See 12 1 to 12 3



On the occasion of the one-year anniversary of the GDPR, the BlnBDI invited journalists

journalists to a press breakfast at their office on May 23

a. In two short presentations we presented our work in the areas of

European cooperation and media education and offered the participants

This gives an insight into the tasks and working methods of our authority. At a

subsequent discussion round there was time with the data protection officer

and their employees to start a conversation and be open

to clarify questions. Since the format proved to be successful, further events

events of this kind are planned.

With a total of 16 press releases, the BlnBDI addressed its own

men to the public. So we made problematic legislative

plan, e.g. to introduce uniform cross-administrative personnel

identification code or the Data Protection Adaptation Act302, carefully and

informed the public about our media-pedagogical offer as well as

New releases from the Berlin Group303 on topics such as smart devices, online

Services for children and artificial intelligence.

We published the following press releases this year:

• Threatening letters from police circles - complete clarification demanded (February 6th

2019)

• Invitation to the Press Conference – Annual Report 2018 (March 22, 2019)

• Annual Report 2018 (March 28, 2019)

• Berlin data protection officer at the re:publica Netzfest (2 May 2019)

• Berlin Group publishes working paper on data protection and artificial intelligence

intelligence (May 9, 2019)

• Berlin Group publishes working paper on large-scale location tracking

(May 10, 2019)

• Maja Smoltczyk: Europe is the way - go vote! (May 23, 2019)

• Data Protection Adaptation Act – alleged reduction in bureaucracy is one

Milkmaid Bill (June 27, 2019)

302 See 14 1

303 For the results see 16 2



• Data protection for elementary schools - revised and expanded offer

(July 30, 2019)

• ECJ ruling on social media plugins – website operators have a duty

(July 31, 2019)

• Citizen-friendly administrative digitization is also possible without personal sign (September 13, 2019)

• Media-pedagogical offer of the BlnBDI for the software price TOMMI nominated (September 16, 2019)

• Delivery service and online bank – Berlin data protection officer imposed sensitive fines (September 19, 2019)

• Berlin Group publishes working paper on smart devices for children and children's privacy in online services (October 8, 2019)

• Berlin data protection officer imposes a fine on real estate companies (November 5, 2019)

• Data protection officer: Google Analytics and similar services only with Permission usable (November 14, 2019)

All press releases are available on our website.304 By email to the address presse@datenschutz-berlin.de is an entry in our press distributor possible.

18.6 Public Relations

On January 28, at the invitation of the DSK, on the occasion of the 13th European Datenschutztag a central event in the representation of the state of North Rhine-Westphalia at the federal government in Berlin. The theme was “European Data protection: opportunity or risk? Eight months DS-GVO - balance sheet and look after front".

For the second time, on May 4th and 5th, our authority took part in the Internet netkonferenz re:publica in Park am Gleisdreieck. In the program part “Politics & Society” of the digital folk festival, three employees of the authority presented their

304 https://www datenschutz-berlin de/infothek-und-service/pressemitteilungen/

work on. In addition to the long-running GDPR, this year the subject of

A special focus is dedicated to service pedagogy, e.g. as part of a

Workshops entitled “Digital Natives – Digital Professionals? Privacy for children

the and youth”. At the information stand, the employees answered

and employees of our authority numerous questions from citizens

gladly, accepted suggestions and distributed information material about

data protection and freedom of information.

On September 7th we were again with an information stand at the day of the

open door in the House of Representatives. This year the responsibility

event in connection with the 30th anniversary of the fall of the Wall in November 1989.

As in previous years, we took this opportunity to

Citizens to get into conversation, to answer questions and

to accept suggestions. In addition to the current annual report and the

most important legal texts, visitors to the information

onsstands guide to data protection in social networks, in image, sound and

Video recordings in the day care center or to protect privacy as tenants

and take tenants with you. The big and small visitors of the

Stands could also test their knowledge of data protection in the data protection quiz

and insights into our new media education offer www.data-kids.de

take.

The conversion process of the fully overhauled

The BlnBDI children's website www.data-kids.de is now designed

completed. However, the content should also be continuously supplemented

become. The children's website offers comprehensive media-educational information

information that can be used in many ways. elementary school

der, teachers and parents will find here in addition to a child-friendly glossary of terms

also games, explanatory videos, workbooks, handicraft templates and other materials,

to help you find your way around the world of data protection. As

In addition to the children's website, we offer project

days for schools to test the materials and sensitivity to the topic

Develop data protection.305

305 See 5 6

230

Chapter 18 From the Office 18 6 Public Relations

We receive a large number of requests for advice from both public and non-public bodies

Place. Numerous general inquiries from citizens,

companies, authorities, freelancers, clubs, associations etc.

on various topics come to us. Most of them are in

related to the implementation of the GDPR. Many of these individual

Unfortunately, we had to make inquiries again this year for capacity reasons

reject.

Nevertheless, both the BlnBDI and its employees

more than 40 lectures this year as part of training courses, work

shops, symposiums and lectures. However, the need was and is much greater.

For example, despite numerous inquiries, only a few seminars and

Training events for data protection officers or data protection lawyers

lawyers are offered. Also the Administrative Academy Berlin,

the urgent lecturers on various topics in the field of

If you are looking for training and further education, we unfortunately had to cancel it.

The GDPR was at the top of the list of topics for the lectures this year

Job. Just on the subject of "One year of the General Data Protection Regulation - experience

10 lectures were held:

volumes, non-profit organizations, independent sponsors, at congresses, in specialist

shots and as part of a lecture series at the Technical University of Berlin. But there was also

numerous specialist lectures on specific questions regarding the application of the regulations of the

DS-GVO and the resulting consequences or problems:

• Basic principles of the GDPR

• GDPR “perfect complaint” requirements

• Rules of conduct according to Art. 40 GDPR

• Role of the works council in the context of the GDPR

• The GDPR in practice and from the point of view of the BInBDI

• Problems of the Berlin economy with the implementation and application of the DS

GMOs; Suggestions for improvement and instructions for action

• European General Data Protection Regulation in child and youth welfare

For the 16th time, the University of Applied Sciences Berlin took place

(HTW) from November 2nd to 23rd the lecture series of the Children's University Lichtenberg



(KUL) - an annual offer for all inquisitive girls and boys

from the age of eight years. On Saturdays there is always the same time

Events for parents on issues of upbringing, family life and

School. We also regularly offer lectures there. On November 23, one

Information and discussion round on dealing with social media will take place, which will be great

has aroused interest. Lectures on the subject of "Data protection in social networks

ken", "Tips on data protection on the Internet" and "Check: WhatsApp - Possibility

opportunities, dangers, alternatives” are also distributed throughout the year in the

offered to interested schools as part of the KUL underway306.

Lectures and training courses on other

various data protection issues and the work of our authority. Here some

Examples:

• Data protection and information security in the work of courts and state

advocacy

• Consents in the context of employment

• Questions about employee data protection

• Data protection in the transport sector

• Structures, working methods and data protection regulations in

Genamt and in the Berlin Police – Opportunities and Limits of Cooperation

rations

• Current issues in data protection supervision

• Practice report – updates from the regulator

• Main features of the work, tasks and organization of the BlnBDI

• The enforcement practice of the supervisory authority – current affairs and prospects

We will continue our activities in the field of public relations and our me-

continue to expand the service-pedagogical offer in the coming years in order to

urgent need for data protection education, training and advice

to be able to comply.

306 KUL on the way is the children's university, which comes to the school - with lectures,

shops and ideas for excursions The free offer is aimed at various

which class or age groups and all schools in Lichtenberg and Treptow-Köpenick,

in Wuhletal and Berlin-Buch



Chapter 18 From the Glossary Service

2 factor

authentication

Proof of an individual's identity via two of the three

the following features:

1. Possession of a device exclusively for this

2. Knowledge of a secret (e.g. a password),

person has

that only she knows

Anonymous/Pseudonymous

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.

apartment

Application program for mobile phones

Article-29-

privacy group

Chief Information

Security Officer (CISO)

Group according to Art. 29 European Data Protection Directive,

made up of representatives from all European

ic data protection authorities. She has

advisory function; primarily against the euro

European Commission, but also towards others

data processors within the European Union.

Responsible for the development of security

guidelines for alignment, planning and coordination

tion of measures to ensure safety

of information processed by an organization

as well as for the evaluation of the implementation of these measures

taken and the remaining risks

233

Glossary Cookie

Cookie Banner

CRO

dashcam

Double opt-in procedure

GDPR

A cookie is a text file that is used to communicate with a

Website related information on the computer

to save the users locally and

to transmit back to the website server on request

tell This means that users can

recognized and visited websites as well as time

points of the visit are assigned.

Banners are graphic or animation files that are included in the

are integrated into the website and either appear at the edge

appear or lay across the webpage. in the

gel contain this advertisement. Cookie banner included

usually notes on the use of cookies and are

usually provided with a simple "OK" button.

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 or

medical products in the course of planning and implementation

supported by clinical studies.

A dashcam is a video camera that is

dashboard or on the wind

protective window of a vehicle is attached.

Double opt-in procedure refers to a process in which

the user after entering their contact data

th in a distributor this in a separate second

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



glossary. On the one hand, this is intended to protect

personal data within the European

Union ensured, on the other hand the free data transfer

traffic within the European single market

be achieved. The regulation replaces 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 25.
Effective May 2018. Since then it has been available in all member states
of the European Union directly applicable.
The data protection conference (DSK) consists of the
dependent federal data protection authorities and
the countries. It has the task of data protection
to uphold and protect fundamental rights, a unity
common application of the European and national
to achieve data protection law and together for
to enter into its further development. This happens after
mentally through resolutions, resolutions,
planning aids, standardization, statements,
Press Releases and Determinations.
The European Data Protection Board (EDPB) is a
independent European body that contributes to
common application of the data protection regulations in the
whole European Union contributes and the cooperation
work between the EU data protection authorities
that. The EDPB consists of representatives of the national
data protection authorities and the European Data
Protection Officer (EDPS).

Recitals are statements by the legislature

to the actual legal text, which this regular

to be attached to European legislation.

"Electronic Identity" - This is a

NEN electronic proof of identity (with chip), with

whose help electronic processes are carried out

can.

235

DSK

EDSA

EC / Recital

oath

Glossary end-to-end

encryption

fan page

firmware

common

federal committee

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

become; it will appear in the relevant search engines

NEN indexed, i. H. listed in the result list. In the

In contrast to the profile page, which is created by private

is used, it is not about "befriending", but

therefore, with the help of the page z. B. directly with customers in the

to communicate in the network or to collect "fans".

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.

The Federal Joint Committee (GBA) is

the four major self-governing organizations, the

National Association of Statutory Health Insurance Physicians, the Kassenzahn-

Medical Association, the German Health

hausgesellschaft and the central association Bund der

formed health insurance companies. He is the supreme decision-

body of joint self-government in Germany

schen health system and determined in the form of

Guidelines for quality assurance measures for

xen and hospitals.



Glossary geodata

GovData

Digital geological data, e.g. in navigation systems

be processed.

Data portal for Germany, which has a central and

Uniform content-related access to administrative data

from the federal, state and local governments that provide these

accessible in their respective open data portals

have power.

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.

This is a mathematical

arithmetic rule, which from any starting data

such as a document or just a

a unique word or telephone number

Fixed-length hash value calculated.

Informed consent "Informed consent" refers to an

declaration of consent, in which the users

detailed, complete information about the planned

processing of your data, its type, scope and purpose

have then clearly consented to the processing of these.

integrity

Understands the preservation of the integrity of data

to protect them from accidental loss or

unintentional falsification or the correct function

tion of systems.



Glossary IP address

IT architecture

coherence method

LABO

LaGeSo

link

Market place principle

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.

The State Office for Citizens and Regulatory Affairs

unite is one of the Senate Department for the Interior and

Sports Subordinate Authority. It's for citizens

and citizens, companies and authorities on the

offer reparation, civil status

and population and motor vehicle affairs

employed.

The State Office for Health and Social Affairs is one of the

Senate Department for Integration, Labor and Social Affairs

subordinate authority. It is in the task

chen health, social and supply.

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. 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



Glossary messenger service

metadata

microblogging

Neural Networks

One stop shop

Market location principle should be uniform

ments are created for all companies that

goods and services on the European market

offer gene.

Telecommunications service involving two or more

Participant text messages (possibly also audio or

video messages and other files) so exchange

ensure that the news is as immediate as possible

reach the recipients.

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.

Artificial neural networks are usually attached to the

organizational principles and the learning processes of

human brain oriented computer models.

The one-stop shop principle means that both

every citizen and every company

can contact the local supervisory authority.

This also applies in particular if personal

Genetic data are processed across borders, e.g.

B. through social networks or other international

operating companies. The supervisory authority at which a

complaint has been filed, the

guide about the status and the result of the

procedure. For companies with offices in

different Member States is the supervisory authority

 at the headquarters of the central contact

partner. All these supervisory authorities are on

involved in regulatory procedures and respect

together ensure that the rights of citizens

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 data

Open government

Opening of the state and administration to the citizens

citizens and the economy

Opt-in / Opt-out

opt-out model

pixel

PNR data

Pre-recording function

Opt-in means that data processing is only permitted

is when the data subject expressly consents to it

has decided, i.e. usually given their consent

gave. In the case of an opt-out procedure, on the other hand,

the data subject to expressly take action in order to

prevent data processing.

"Opt-Out Model" means a procedure that

consent if not within a

objected to within a predetermined period of time.

Small graphics on websites, which are usually only 1×1 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.

i.e. it is a recording function

which is already a few seconds before pressing the recording

drawing button, the data is saved.



Glossary Privacy by Default

Privacy by design

profiling

test value

pseudonymize

public consultation

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.

Pseudonymizing is replacing identifying

Information such as name, address, date of birth or other

re clear identifiers or characteristics by a

other designation (e.g. a consecutive number) of

art that an inference to the person without knowledge

the assignment rule or only with disproportionate

is possible with moderate effort.

dt. public consultation - before the adoption

of guidelines, the European data protection

schuss (EDSA) through public consultations in order to

views and concerns of all stakeholders,

Stakeholders, citizens to be heard.

Usually, guidelines are made prior to their final

Adoption published on the EDPB website

public. Then there is usually for six to eight

weeks the opportunity to comment on the guideline.

241

Glossary source code

ring memory

score value

sensitive data

Social Plugins

Mainly business associations and

take advantage of this opportunity. The ESDA

but also receives feedback from civil society

groups and citizens. After expiration

During the consultation phase, the EDPB decides which

Change requests are taken into account.

The program code (technical basis) of a software

goods

A ring memory stores data continuously in a

a certain period of time and overwrites them

expiry of a specified time again in order to

to free up some space for 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. for this purpose

hear information about the racial and ethnic origin

origin, political opinions, religious or philosophical

physical beliefs, union membership,

health or sex life.

Social plugins or social media plugins connect

the websites or apps with social networks.

Operators add a program

code into the source code of your website or app, the

automatically data on the operator of the social network

factory sends and retrieves data from this. The operator

About the social network learns what the

Visitors to the website are interested

and can create personality profiles by means of profiling

create and personalize ads. The operator

can indicate, for example, that acquaintances of the web

site visitor or the website visitor

Liked the website. Through social

telematics tariff

tracking

Plugins can cause network effects in particular

Significant visits to websites and in the

As a result, significant sales are regularly generated.

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. Be included

e.g. B. the number of night trips, trips in risky

Areas or on accident-prone roads and the

Compliance with maximum speeds and the

acceleration behavior. For this purpose, an intensive

electronic monitoring of vehicle activities

and transmission of the data to the insurance company. This

Tariffs are also referred to as “pay as you drive” tariffs

draws.

is

tracking

in understanding of the data protection

supervisory authorities the logging and evaluation of the

behavior of visitors

Websites or apps for generally website-wide

sweeping follow-up. The areas of application

range from a pure range measurement

statistical evaluation according to browser, operating

system, language settings and country of residence

and website usability tests

for detailed observation and recording of all

physical mouse movements and inputs as well as for web

cross-site and cross-device creation of user

Development and personality profiles for advertising purposes.

Tracking / cookie walls

Preventing the use of a website if you do not

accept cookies

behaviour rules

english Code of conduct - This is an in-

instrument of self-regulation. According to Art. 41 GDPR

Associations and other associations can behave

develop tens rules with which the application of the



wearable

WIFI base stations

WiFi tracking

DS-GVO is specified. task of the supervisory authorities

is to authorize the elaboration of such codes of conduct

promote and approve.

Technical information when using a

Telecommunications service incurred, such as a

Phone call calling and called phone number

mer, start and end of the connection and for telephone

also the location in the mobile network. Also as

called connection data.

Wearable computers, or wearables for short, are

computers that are so small that they don't have a room

still need a desk, but

e.g. B. worn as a bracelet and glasses or in clothing

can be incorporated. During the application

Are they attached to the user's body and often-

connected directly to the internet. So e.g. B.

a blood pressure monitor, which is permanent or over

worn on the arm for a longer period of time,

out as a device from the field of wearable computing

be designated.

device for wireless data transmission; will mostly

used for wired internet access

mobile devices nearby using the internet

allow without having to connect cables.

A technique with which the movement of people

can be tracked using location data that

using the smartphone of these people

are recorded.