Activity report of

Saxon data protection officer

Reporting period: January 1 to December 31, 2020

activity report

of

Saxon data protection officer

2020

Reporting period: January 1 to December 31, 2020

Legal status: December 31, 2020

foreword

Dear readers,

maybe you feel the same way: there are years that guess

quickly forgotten. Others literally burn themselves

into memory. The year 2020 is probably the most order

from us to the category "unforgettable". I conclude that

me in particular with regard to data protection.

2020 - that was the year in which analog life ended

was slowed down and the digital rapidly picked up speed.

In line with this, a large number of questions about data

protect me. Suddenly video conferences, streaming platforms and online

shopping. Home office and home schooling found their way into everyday life; Corona warning apps

should stop the pandemic.

In the middle of the year, a court decision caused uncertainty among those responsible.

Because on July 16, 2020, the European Court of Justice had the Privacy Shield Agreement between

Agreements between the EU and the USA were declared invalid ("Schrems II"). Consequently, it is US company

men no longer possible on the previous basis personal data of EU citizens

to process. This decision forces a variety of economic, political and
social actors to act. Companies in particular are likely to face the impending fine
have in mind when setting up their processes when processing personal data
do not adapt to case law. In this respect, too, the European data
General Protection Regulation (GDPR) their effect.

The conference of independent data protection authorities had to deal with the judgment just as quickly
the supervisory authorities of the federal and state governments. The data protection conference
(DSK), which I chaired in 2020, dealt intensively with the consequences of “Schrems
II”, for example with the transmission of Windows 10 telemetry data to Microsoft or
the legally compliant use of Office 365. Furthermore, the task force “Schrems
II" set up. It deals with the consequences of the judgment and serves the supervisory authorities
to vote on how to proceed.

In addition to questions about data protection-compliant digitization and the fight against pandemics,
In 2020 I had many more concerns. The need for advice in Saxony continued
high. Data protection affects more or less almost all areas of life. And so un-
no matter how different the individual practical cases may be, one aspect persists
famous common thread: the right to informational self-determination. It is an electronic
essential characteristic of our free democratic basic order and therefore
inalienable. The GDPR also follows this guiding principle, the structure of which is based on the
Article 59 activity report to be prepared annually.

Finally, I would like to thank the members of the Saxon state parliament and
would like to thank all partners who, not only in the reporting period, thanked for data protection and the
equipment have made my authority strong. I especially thank my co-workers
and employees. You've done a great job over the past year. I think so

not only to the Corona-related challenges, but also to coping with the

many requests for advice, the DSK chair, the preparation for the European data

protection day and much more.

You can find out details about all these events, dear readers, on the following

ing pages. With this in mind, I wish you lots of new insights!

Her

Andrew Schurig

Saxon data protection officer

6

7

Table of Contents

Table of Contents

2

2.1

Data protection in the Free State of Saxony

Data protection in times of the coronavirus pandemic

Survey on data protection in municipalities

Chair of the data protection conference

Supervision focus on video surveillance

Application of the General Data Protection Regulation to the parliamentary

task

The Saxon Data Protection Implementation Act in relation to

General Data Protection Regulation and the Federal Data Protection Act -

consent in employment

Consultation on government legislative projects

Act on the 23rd Broadcasting Amendment State Treaty

“Self-initiated” public relations work by authorities

Principles of data processing

Data processing principles, definitions

2.1.1

Company doctor as his own responsibility within the meaning of Art. 4 No. 7

GDPR

2.1.2

Data protection officer as the person responsible

2.1.3

MDK reform law – medical service as its own responsible person

2.1.4

Covert collection of vehicle number plates - transparency

Data minimization in the social field: scope of the

Where-used check of the integration aid to be checked

documents

2.2

Legality of data processing

2.2.1

What happens to my personal data at a

corona test?

2.2.2

Management of visitor lists at Saxon courts

2.2.3

Corona registration form in the town hall

2.2.4

Contact data collection for hairdresser visits in the coronavirus pandemic

2.2.5

2.2.6

disclosure of personal data, respectively

Health data from the health authorities to the police

Certificates of exemption from the obligation to wear a mouth mask

nose covering in schools

2.2.7

Health certificates for school attendance

2.2.8

Inspection of an authorized district chimney sweep

2.2.9

Proof of adequate vaccination protection against measles

Video surveillance causes neighborhood disputes

2.2.24

Videography: The valuable sculpture in the front yard

2.2.25

Doorbell cameras as digital door viewers

2.2.26

Video surveillance of the entrance area of a block of flats –

exceptions prove the rule

2.2.27

Video surveillance in a dental practice

2.2.28

Video camera in Thai massage studio

2.2.29

Video surveillance of the employee areas at a truck stop

2.2.30

Dash cams and helmet cams

2.3

Consent Questions

2.3.1

Revocation of consent given to municipalities

2.3.2

LernSax - the Saxon school cloud

2.3.3

Collection of health data from employees in the coronavirus

Pandemic

2.3.4

Table of Contents

2.3.6

Insurance broker consent forms

2.4

Sensitive data, special categories of personal data

2.4.1

Privacy-friendly collection of health data

employees

2.4.2

Reimbursement of union dues by the employer

3

3.1

3.1.1

data subject rights

Specific Obligations of the Controller

Data protection information according to Art. 13 GDPR – one-fits-all solution

allowed?

3.1.2

Information obligations of lawyers as persons subject to professional secrecy

3.2

right of providing information

3.2.1

Request for information to the school in a service law

matter

3.2.2

Refused information on the address reference for the letter shop model

3.2.3

Table of Contents

GDPR

6.1.2

Factual incompetence in an online encyclopedia

6.1.3

Change in supervisory authority for federal motorways

and federal roads

6.1.4

Collection area: minimum requirements for complaints

6.2

Figures and data on activities in 2020

6.2.1

Overview of the main areas of work

6.2.2

complaints and notices

6.2.3

consultations

6.2.4

data breaches

6.2.5

European procedures

6.2.6

Register of designated data protection officers

6.3

6.4

resources

Fines and sanctions, criminal charges

Table of Contents

6.4.1

Administrative offense proceedings in the public sector

Judgment of November 11, 2020 – 29 OWi 1/20

Information according to Art. 15 GDPR by free (electronic)

Transmission of the treatment file

9.7

On the storage period of account statements in social service files

171

172

173

174

175

177

15

List of Figures

List of Figures

List of abbreviations

List of abbreviations

Below are laws and other regulations in alphabetical order

the official, in exceptional cases also non-official abbreviation, alternatively the official one

abbreviation listed.

regulations

oh

tax code

Residence G

Residence Act

BDSG

Civil Code

BMG

BZRG

Federal Data Protection Act

Civil Code

Federal Registration Act

Federal Central Register Act

GDPR

General Data Protection Regulation

HGB

JI RL

OWiG

commercial code

Directive (EU) 2016/680 (Justice and Home Affairs)

Administrative Offenses Act

Saxon DSG

Saxon Data Protection Act

Saxony PolG

Police Act of the Free State of Saxony

SächsPresseG

Saxon law on the press

Saxon SchoolG

Saxon school law

Saxon author

Constitution of the Free State of Saxony

SächsVwVfZG

Law on the Regulation of Administrative Procedures and

Administrative service right for the Free State of Saxony and for

Changing Other Laws

SchfHwG

Chimney Sweep Crafts Act

SGB

StPO

TMG

UWG

social code

Code of Criminal Procedure

Telemedia Act

Unfair Competition Law

VwVfG

Administrative Procedures Act

ZPO

Code of Civil Procedure

17

List of abbreviations

Miscellaneous

Section.

kind

Inc

ASD

Az.

BfDI

Unit volume

article

working group

General Social Service

File number

The Federal Commissioner for Data Protection and Information

freedom

Federal Law Gazette

Federal Law Gazette

BGH

BKA

BMI

Federal Court of Justice

Federal Criminal Police Office

Federal Ministry of the Interior, Building and Community

BR-Drs.

Federal Council printed matter

ESR

BSGE

BSI

BT-Drs.

letter

BVerfG

Federal Social Court

Federal Social Court decision

Federal Office for Security in Information Technology

Bundestag printed matter

Letter

Federal Constitutional Court

BVerfGE

Federal Constitutional Court decision

BVerwG

Federal Administrative Court

Federal Administrative Court

Federal Administrative Court decision

DSK

Conference of the independent federal data protection officers

of the countries – data protection conference

ECtHR

European Court of Human Rights

EU

IVO

prison

KSV

European Union

Integrated transaction processing system for the state police

correctional facility

Municipal Social Association of Saxony

LaSuB

State Office for Schools and Education

LfV

LG

18

State Office for the Protection of the Constitution of the Free State of Saxony

district Court

List of abbreviations

LKA

LT Drs.

OLG

OVG

item no.

Saxony State Criminal Police Office

State Parliament printed matter

Higher Regional Court

Higher Administrative Court

marginal number

Saxon OJ

Saxon Official Journal

SächsGVBl.

Saxon Law and Ordinance Gazette

Saxon Constitutional Court

Saxon Constitutional Court

SID

SMF

SMI

State enterprise Saxon IT services

Saxon State Ministry of Finance

Saxon State Ministry of the Interior

SMJusDEG

State Ministry of Justice and Democracy, Europe and

equality

SMK

SMS

SMUL

SMWA

SMWK

StA

SVN

VVT

VwV

AWAY

Saxon State Ministry for Culture

Saxon State Ministry for Social Affairs and Society

cohesion

Saxon State Ministry for Energy, Climate Protection, Environment and

Agriculture

Saxon State Ministry for Economics, Labor and Transport

Saxon State Ministry for Science, Culture and Tourism

Public prosecutor

Saxon administration network

Directory of processing activities

administrative regulation

homeowners association

19

subject register

subject register

with * | only public area

without * | non-public area or public and non-public area

General Data Protection Regulation (EU) 2016/679

reference

archiving*

order processing

encumbrance*

Employee data protection (incl. service law*, personnel

representatives*, works councils, other representatives and

officers); see also videography, employees

Company data protection officer, see data protection officer

Rights of data subjects (information, information, deletion etc.)

et cetera)

education and Science

4.3

2.2.8

1.6, 2.1.1, 2.3.3, 2.4.1,

2.4.2 3.2.1, 3.4, 4.5.2

3; 2.1.2, cf. 2.2.10, cf.

also 8.3, 9.6, 9.7

 Universities, research institutes

 Schools, school authorities*, educational institutions 2.2.6, 2.2.7, 2.3.2, 2.4.1,

4.6.3

 Miscellaneous, general

Corona, SARS-CoV-2, pandemic measures and

with associated data processing

Data Protection Officer

Data Protection Impact Assessment

Dashcam, drones, see videography

eGovernment*

consent

Specialist administration* (e.g. building administration, immigration

den), see if applicable registration authorities*

Financial, tax and subsidy management*

(incl. municipal offices)

Liberal professions, see also health care if necessary

 Lawyers

 Notaries

 Tax consultants, auditors

 Architects, engineers

 Miscellaneous, general

Jointly Responsible

court administration*

Bailiff*

3.2.1

1.1, 2.2.1 to 2.2.7,

2.3.2, 2.3.3; cf. also

8.1

see 1.2, 2.1.2, 6.2.6

2.3; 1.6, 2.2.3, 2.2.16,

2.2.18, 3.3.4, 9.4

2.2.8, 2.2.13, 6.1.3

2.4.1

3.1.2

4.2

2.2.2

20

subject register

General Data Protection Regulation (EU) 2016/679

reference

healthcare

 Official supervision and monitoring*

 Hospitals

 Nursing Services

 Pharmacist

 Doctors

 Healthcare professions

 Miscellaneous, general

Trade, services, commerce, industry

2.2.1, 2.2.4, 2.2.5, 2.2.9,

2.2.15

9.6

2.1.1, 2.2.1, 2.2.27,

2.2.9

4.5.1

 Credit agencies, debt collection service providers, detective agencies

2.2.21, 6.1.4

 Banks, finance

 Trade, see also internet/e-commerce

 Craft, trade, industry

2.1.5, 3.2.3, 3.3.4

4.1.5

2.2.28, 2.2.4

 Hotel and gastronomy, leisure, tourism,

2.2.4; see also 8.1

Sports

 insurance; see if applicable social affairs,

2.3.6

service provider

 Advertising, market and opinion research

 Miscellaneous, general

infrastructural sector

2.2.18 to 2.2.20, 2.3.4,

2.3.5, 3.2.2, 3.3.2, 3.3.3,

4.2.3, 9.4,

2.1.4, 2.1.5, 2.2.4

 Energy, water and utilities

2.2.10, 2.2.11, 4.1.4

 Traffic and transportation

6.1.3

 Housing industry, property management

 Data centers

 Miscellaneous, general

Internet, media, communication

 E-mail, telecommunications processes, post

 Ecommerce

 Social media, telemedia

 Miscellaneous, general

Chambers, professional bodies d. ö.R.*

2/2/14, 2/2/16, 2/2/17,

2.2.26, 3.1.1, 4.2.2

see 4.6

2.2.18 to 2.2.20, 3.3.2,

3.3.3, 4.1.4, see 4.6

2.2.20, 2.3.4, 3.3.3,

Preliminary note on the use of language

Directive (EU) 2016/680

Police*

Administrative offense authorities*

Prosecution*

correctional system*

Other areas (outside Regulation 2016/679

and Directive EU 2016/680)

Saxon state parliament as parliament

defense of Constitution

Other data processing bodies

reference

8.1, 8.2; see also 1.9,

2.2.5, 4.2.1, 6.4.1

8.3; see 6.4.3, 9.5

8.1; 1.9, 9.2

1.5, cf. 1.7, 1.8

Preliminary note on the use of language

In this activity report, the generic masculine is used below to denote the

to facilitate reading and understanding. However, all genders are self-evident

meant. For reasons of grammatical correctness and correct application of the par-

In the tizip present tense, substitute forms such as users or users are not used.

1

Data protection in the Free State of Saxony

1.1

Data protection in times of the coronavirus pandemic

In the reporting period, the corona pandemic from March 2020 also led to a large number in Saxony
data protection issues. In addition to my other ongoing business, I was
therefore, like other Saxon public bodies, also with important and frequent
also deals with urgent corona-related processes.

There were essentially three areas: On the one hand, I was
State government, in particular the Saxon State Ministry for Social Affairs and
social cohesion, consulted. The main focus was on the respective
Austrian corona protection regulations. According to Art. 36 Para. 4 General Data Protection Regulation
(GDPR) I am to be consulted when drafting legislation. I have this
Involvement used to influence the concrete wording of the legislation
and have them designed as data protection compliant as possible. I hope so too
will be involved in the future, as required by Art. 36 Para. 4 GDPR (cf. also 1.7). On the other hand
I took up a large number of currently discussed issues and
ligten or even publicly expressed about it. This concerned contact tracing, for example
by health authorities, data processing in connection with the Saxon learning
platform LernSax, health confirmations for school attendance, data collection
through registration forms when entering courthouses or town halls, the contact
tracking with the help of data stored with the hairdresser, the legality of the request
gens a pharmacy for copies of ID and, if necessary, further explanations for
the issue of free FFP2 masks or the distribution of lists with positive test results
dead and quarantined persons to the police. Finally there was - guess-
at times several hundred – individual inquiries from citizens, petitions or mere references
facts relevant to data protection law in the fight against corona. As an example, they like
labor law questions about the powers of employers and employers at the

collection of data on corona test results. As mentioned, all this has to

led to a considerable amount of work in my authority, which with the existing personal

could not be managed with the available resources (cf. 6.3).

In all of this, I have always made sure that important statements are published immediately

were published on my website. Among other things, I informed myself there about the permitted

measures taken by employers or employers in the interest of

on protection, on data protection during (tele) home work or in the home office,

on the basic concept of the Corona-Warn-App or on the required content of mask

issued exemption certificates.

24

1.2

I also saw an important aspect of my job in being transparent

data protection assessment of the measures to combat the corona pandemic

Countering myths and conspiracy theories.

In the contributions 2.2.1 to 2.2.7, 2.3.2, 2.3.3 and 8.1 I present my activity and concrete

problem situations in connection with the pandemic in detail.

1.2

Survey on data protection in municipalities

The General Data Protection Regulation (GDPR) has been in effect since May 25th, 2018. she is the one

Basis for a uniform data protection law in the European Union. Consequently

At the beginning of 2020 we conducted a survey on the status of the implementation of the GDPR at selected

th municipalities. We wanted to find out to what extent the municipalities

already implemented in Saxony and the respective data processing processes

the regulations of the GDPR have been adjusted. A similar survey was already carried out in

their states. Thus we were able to respond to the questionnaire of the state representatives for the

Set up data protection Lower Saxony for our query.

In order to achieve a survey result that is as meaningful as possible, in addition to all
free cities and districts, various municipalities of different sizes for the
question randomly selected by us. The questionnaire with a total of four topics
plexen was sent to 118 places. We received feedback from 61 positions
in 2020 a. Few of the bodies responded within the six deadline set
weeks. With the beginning of the Corona Pandemic, however, we were unable to accept any further inboxes
register. Fortunately, we also have 27 completed forms from individuals
Specialist offices received from authorities.
Ultimately, all ten districts, the three urban districts (Dres-
den, Leipzig, Chemnitz) and another 48 cities and municipalities. Many thanks to all
who took part in the survey!
The 39 questions included topics from the GDPR on data protection organization, such as the
Appointment of an official data protection officer (Art. 37) and questions about the directory
of processing activities (Article 30). There were also questions about the specific data protection
compliant processing, for example on the basis of consent (Art. 7), for
contract processing (Art. 28 and 29), for data protection impact assessment (Art. 35 and 36) as well as
on the information obligations (Articles 12, 13 and 14) and requests for information from a data subject
person (Article 15). Finally, on the subject of reporting data breaches (Article 33)
asked.

Summary of the main results

The GDPR came into force in 2016 and has been in force since May 25, 2018 in all
Member States of the European Union directly. The evaluation showed that unfortunately
only 23 percent of the municipalities contacted by the end of 2017 with the
settlement work had begun and, as a result, the two-year transitional period up to

effective date of the GDPR. The majority (77 percent) of the

Written municipalities did not start implementation until 2018 or - even later - only

started in 2019. As a result, half of the municipalities surveyed were planning to implement the GDPR

necessary adjustments to legal provisions, forms, contracts and so on

to be completed by the end of 2020. Another twelve municipalities (about 20 percent) will

only in the course of 2021 or even later the data protection regulations under European law

have implemented compliantly.

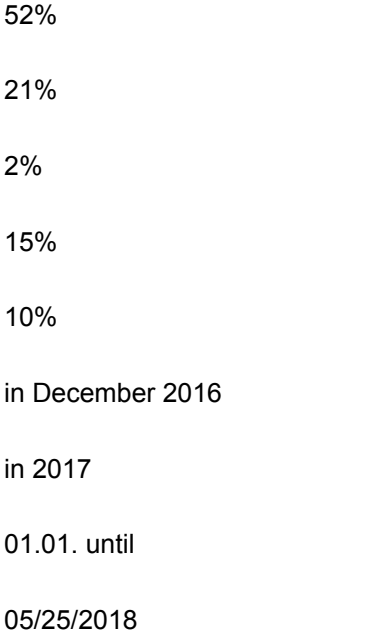

Figure 1: Beginning of the implementation of the GDPR in Saxon municipalities

It should be positively emphasized that almost all municipalities have individual employees as responsible

or project teams for the strategic and operational implementation tasks for the data

have named tenschutz in their house. In almost all municipalities (95 percent) were also

the employees involved in the processing operations about the new data protection law

informed. 54 municipalities (89 percent) stated that at the time of the

Query training measures have already been offered.

An authority or public body has
according to Art. 37 Para. 1 Letter a) GDPR
a data protection officer (DSB).
to name. Almost all municipalities in property
sen meet this requirement. 36 each
Municipalities (59 percent) have a
employees on data protection
ordered. 20 (33 percent) – mostly-
tens smaller municipalities – commissioned
an external service provider with this
Task. According to Art. 37 Para. 3, for
several such authorities or bodies
taking into account their organizational
structure and size have a common
named data protection officer
will. made of this possibility
four smaller communities (7 percent)
need. In most municipalities (89
percent) the DSB already has the
required specialist knowledge or there are
further training measures are already planned.
According to Art. 30 GDPR, the responsible
lichen obliged to keep a list of all
Processing activities (VVT) to create
len. 43 municipalities (70 percent) gave
indicates that you have created a VVT. A

full VVT was only two

Municipalities (3 percent) created and 16

Municipalities (26 percent) have this

at least to the extent of 75 to 99

created by the hundred. It is worrying that

21 municipalities surveyed (34 percent) on

Time of survey still at the beginning of the

required work.

Either they had with the creation

of the VVT has not yet started or

Less than half of the hundred done.

Only every second person responsible used it

electronic processing procedures

Does your administration have a

appointed data protection officer?

1 %

7%

33%

1.2

59%

internal DPO

external DPO

DSB with other municipality(s).

no DPO

Figure 2: DSB appointment in municipalities

Occur in dealing with consent

explain difficulties?

no information 8 %

no 18%

yes 74 %

Figure 3: Difficulties in handling

with declarations of consent

Does your administration have organizational

precautions have been taken to

request to issue electronically?

yes 13 %

in planning

39%

no 48%

Figure 4: Arrangements for granting

electronic requests for information

Was the privacy policy on your

Website adapted to the GDPR?

no 5%

yes 95 %

Figure 5: Adaptation of data protection

statement on the site

of the VVT. 25 municipalities (41 percent)

indicate that when creating the VVT

still have difficulties and that the

associated with the implementation of the GDPR

the effort in the municipalities

was estimated. In addition to time and resource

cenproblems were also, for example

Difficulties in assigning

Legal bases or the determination of

appropriate and appropriate to the purpose

corresponding storage and deletion

called deadlines. Some municipalities shared

in the query with that trouble

in state or federal proceedings

appear. For the creation of the VVT and

the data protection check

these central processes, which in all

administrations are used, would be the

Development of specifications or mus-

ter recommended. This could lead to a

Reduction of the effort in the municipalities

and the implementation of the GDPR

possibly improve.

Almost all of the municipalities surveyed (89 percent

cent) have those attached to the processing

the employees involved

Obligation to report data breaches in accordance with Art.

33 GDPR informed. At the time of

Query had only about half of

surveyed administrations organizational

Provisions for the information of

agreed according to Art. 34 GDPR.

Another 25 municipalities (41 percent) have

at least until the end of 2020

terminated.

23 municipalities (38 percent) stated that in

their administration video surveillance

put. Four of the 23 municipalities that

use monitoring, do not yet have o-

1.3

which did not have adequate signage attached to all video cameras. Furthermore, we asked

whether the information on video surveillance has been adapted to the GDPR. In the-

Information obligations of the person responsible for video surveillance are based on Art. 13

Paragraph 1 GDPR. At six responsible bodies, this information from the responsible

literal for video surveillance according to GDPR not yet adapted.

Overall, the survey results give a good impression of how the provisions of the

DSGVO had been implemented in the Saxon municipalities by the beginning of 2020. The evaluation

revealed not only which challenges were mastered. At the same time they stepped

Deficits came to light that still existed one and a half years after the GDPR came into effect.

These findings have already flowed into my consulting work in 2020 in order to

to further improve the level of data protection in the communities.

1.3

Chair of the data protection conference

After 2003, Saxony took over the presidency in 2020 for the second time since the authority was founded

the Data Protection Conference (DSK). The body of 18 independent data protection supervisory

Federal and state authorities have the task of protecting the basic data protection rights

and protect, uniform application of European and national data protection

right and to work together for its further development. This happens after

mentally through resolutions, resolutions, guidance, standardization,

ments, press releases and determinations.

The DSK meets annually under rotating presidency in rotation of two main and presiding

conferences and three interim conferences. There is also a session with the so-called

ten specific supervisory authorities, including the church data protection

or the broadcasting data protection officer for public service broadcasting

Listen.

The DSK chairmanship usually entails a high workload. Numerous voting

ments and circulation procedures are to be organised. In addition, the chairman represents the

medium to the outside. Against this background, the coronavirus pandemic presented an additional

challenge with new design options. With the exception of the first

th interim conference, all meetings were held via video conference for the first time. In this

In this respect, Saxony was a pioneer. Admittedly, on the anniversary of the 100th data

On November 25th and 26th we would like to have the participants personally in Dresden

welcomed. But the events of the pandemic only made it possible to meet via video

tion. Nevertheless, the results were impressive – also in a figurative sense.

An overview of all DSK documents published in 2020 can be found in Chapter 7.

At the beginning of 2021, the DSK chair changed as planned to the state commissioner for data protection

and freedom of information in Saarland. However, the planning and implementation of the

European Data Protection Day on January 28, 2021 is still my responsibility (cf. 7.7).

1.4

Supervision focus on video surveillance

Almost every day I receive submissions and information about supposedly impermissible video cameras

fast The videography remains unchanged - especially in the non-public area

one of the focal points of my authority. The enormous fall in the price of video surveillance

engineering technology as well as the wide availability via numerous internet providers as well as on site in the

Specialist shops, in hardware stores and even discounters as part of special campaigns

an ever-increasing spread of technology and new types of surveillance. the

Cameras often have a WLAN function and can therefore also be used for technical

Uncomplicated integration of niche non-professionals into the home network. About appropriate application

tion software, live images can be viewed from any location using mobile devices such as

Look at smartphones and tablets.

As a rule, video surveillance technology is used for security purposes

not only associated with individual concrete business models or purposes,

but distributed across all sectors and thus for both public and non-public

common jobs to the same extent and are also increasingly interesting for private individuals. in

to a greater extent, the camera operators cite the subjectively increased need for security as

motivation for using video surveillance technology, which in my opinion is a

essential reason for the ever-increasing penetration of all areas of economic and

social life with video surveillance technology.

The facts presented as examples in my activity report are symbolic for

the diverse areas of application of video surveillance (cf. 2.2.3 to 2.2.30, 3.1.1, 3.3.5,

4.2.1).

It often turns out that camera operators escape from what appears to be omnipresent video surveillance

also derive the right to operate a video surveillance system. she

all too often overlook the (lack of) sense of such an investment.

If I then use camera operators with alternative, equally effective or even effective
When I confront more tive measures, I regularly find that these are becoming more and more common in the
background and those responsible are increasingly less aware of such measures
include safety considerations. Sufficient illumination is given as an example
endangered areas or alarm systems with optical or acoustic signals that are
If necessary, raise an alarm with the police.

1.4

My admissibility statements in earlier activity reports have also been taken under the
since May 25, 2018 applicable General Data Protection Regulation (GDPR) essentially
nothing changed. The one to be applied when observing publicly accessible spaces
Provision of § 6b Federal Data Protection Act old version has been replaced. The Federal
enacted by the legislator with Section 4 (1) of the Federal Data Protection Act as a successor regulation
However, the Federal Administrative Court issued a verdict on video surveillance requirements
of March 27, 2019 (6 C 2-18) classified as contrary to European law (see activity report 2019,
9.1, page 161 ff.). Thus, the actually intended provision for video surveillance
no application in the non-public area. In the case of private positions, there is only one
Assessment based on the standards of Art. 6 Para. 1 Letter f GDPR by means of a comprehensive
send a weighing of interests into consideration, insofar as there is video surveillance on areas
beyond the private sphere, i.e. one's own apartment or one's own
property extends.
A video surveillance that extends to the public space cannot be considered as one
exclusively personal or family activities are considered to which the data protection
legal regulations would not apply (cf. Art. 2 Para. 2 Letter c GDPR). the
related decision of the European Court of Justice of December 11, 2014
(Case C-212/13) is still valid (cf. also 7th activity report for

the non-public area (04/2013 to 03/2015), page 33 ff.

The already mentioned provision of Art. 6 Para. 1 Letter f GDPR writes a legitimate one
Interest on the part of the camera operator or a third party with the
to weigh conflicting legitimate interests of data subjects
is. An extension of video surveillance to public traffic areas (walking or cycling
paths, streets, squares) will generally only be considered at all if
these traffic areas are directly adjacent to the building to be protected. It has to
also be an absolutely exceptional case, i.e. serious impairments
violating the rights of the camera operator, such as attacks on his person and family or his
immediate living sphere cannot reasonably be met in any other way. In each
In this case, a comprehensive examination in individual cases is required.

The Federal Court of Justice has already made clear in its judgment of April 25, 1995 (VI ZR 272/94)
states that private individuals, apart from situations similar to self-defense, do not have the right
to capture passers-by on public paths through video recordings. private individuals
do not expect from other private persons during your stay in public
room to be filmed. The right to information recognized by the Federal Constitutional
functional self-determination guarantees the right of the individual to express himself, especially in public
possibility of being able to move freely and without having to worry about unintentionally moving
to be made the subject of video surveillance. The resulting
legitimate interests of those affected regularly outweigh the interests of the operator

a preventive monitoring of property and the preservation of evidence in the case of criminal law
relevant incidents of theft, burglary or damage to property.

There is no case relevant to data protection law, if at all with video surveillance
no processing of personal data is involved, see Article 2 (1) GDPR. So

there are often dummy cameras to be found, or they only serve as such, but actually
functioning cameras are not subject to data protection law. In these cases I can
refer affected persons only to the general civil law. Through dummies,
no data is collected at all, and there are not even any signals for observation purposes
forwarded. If there is a lack of applicability of the data protection regulations
because of the control responsibility of my authority, it can only be pointed out that
that camera dummies from the jurisprudence in the application of common civil law
are regularly evaluated like functional cameras and therefore at least one
loge application of the GDPR should be considered. Because for those affected, the one
pass the "apparently" monitored area, the external image appears when the mere presence
the presence of a dummy is no different than operating a functioning video camera.
mera. This applies all the more as the sole purpose of a dummy camera is to deter
the effect lies. Alone in what is caused in the persons supposedly affected
Impression of the live observation as well as the making of a video recording and the
resulting and especially in the case of dummies, purposeful and consciously intended surveillance
judiciary already sees a considerable intervention in the general
personal rights. It speaks to those affected to cease and desist, eliminate or even
claims for damages. With this in mind, I recommend regularly for dummies
their dismantling or at least a change of orientation in such a way that for external
the impression of surveillance can no longer arise at all.
Additional clarity for both those responsible and those affected was provided with the
Data protection supervisory authorities nationwide coordinated "guidance video surveillance
inspection by non-public bodies" of July 17, 2020 (cf. 7.3). In it are found
Information on numerous cases in which video cameras are used.
The procedure for the practical
fair design of the information obligations of Art. 13 GDPR is repeated therein

explained (cf. activity report 2019, 3.1.1, page 71 ff.).

More and more disputes between neighbors are crystallizing as a main input

from (cf. 2.2.23 to 2.2.25). As reasons for this I see both the ignorance of the legal

Prerequisites as well as a lack of awareness of data protection

Long. In addition, a certain habituation effect seems to set in, it is today

but almost impossible, after leaving one's own living area, in view of the

Observation density for public transport, bus stops, train stations, gas stations

move unobserved in public space.

32

1.5

This prompted me to bring this to my attention before my authority dealt with it

Provide the parties involved with a brief, two-page notice sheet for a

Video surveillance to provide essential information. The ones available to me

existing human resources already do not allow everyone from the neighborhood

adequately follow up on any tip or complaint originating in this area. The note-

sheet is used if the facts presented to me still

there are no reliable indications that - in addition to the surveillance of neighboring

Plots actually also beyond public transport areas of the

suspected video surveillance. With a letter to the parties involved

With all parts to which I enclose the information sheet mentioned, I hope that

this contributes to a reduction in complaints in this regard, especially since I have purely private ones

neighborly disputes only limited investigative powers

and I am therefore entitled to the correctness of the information provided or to voluntary

timely revelations must be trusted. Especially in the case of broken neighborhood relationships

this does not contribute to pacification in the majority of cases. So I specifically do not dispose

about a right of access to private land and apartments. The provisions in Art. 58

Paragraph 1 letter f GDPR and Section 40 Paragraph 5 of the Federal Data Protection Act open up a

Speaking authority only for business premises.

1.5

Application of the General Data Protection Regulation to the

parliamentary activity

The rules of procedure of the Saxon state parliament of the 7th electoral period contain

instruction in § 11 as Appendix 3 the data protection regulations of the Saxon state parliament. She should

Processing of personal data when performing parliamentary tasks

regulate.

So far, the setting of standards has corresponded to my previous legal assessment and the

version of the conference of the independent data protection supervisory authorities of the federal government and the

Countries. After that, the General Data Protection Regulation (GDPR) should not apply

Parliaments and their organs as well as the activities of the members of parliament in relation to the

find mental core activities. Data protection regulations and supervision of

The supervisory authority should only act on the condition that there are clear legal provisions

results (see the wording of the decision in the Activity Report 2017/2018 Part 2,

7.2.6). In this respect, the independent regulation of the Saxon state parliament would also be necessary

been. In this respect, the conference had expressly recommended a

own "data protection regulations". Congruent with this is the regulation of the Saxon Da-

Data Protection Implementation Act, which stipulates that to the extent that the state parliament, its bodies,

its members, the parliamentary groups and their employees as well as the state parliament administration

processing personal data in the performance of parliamentary tasks

a data protection regulation of the parliament regulations are to be created (see § 2

Paragraph 1 sentence 4 of the Saxon Data Protection Implementation Act and also sentence 3 of the regulation).

With the decision of the European Court of Justice of July 9, 2020 in the case C-
272/19 was under a preliminary ruling on the scope
the GDPR, however, contrary decisions have been made. The legal dispute was one of
verwaltungsgericht Wiesbaden based on a request for information from a petitioner who
after submitting a petition, information about the processing of his personal data
data coveted. This was rejected by the Hessian state parliament because the
area of the GDPR, which provides for a corresponding right to information in accordance with Art. 15, denied
became.
The European Court of Justice, on the other hand, decided that the GDPR also applies to the petition
committee of the state parliament applies. Could you give the Petitions Committee
still assign the sphere of activity to an executive activity, the court ruled on the
specific focus of the dispute going beyond that controller within the meaning of the GDPR
not just authorities, but all bodies that alone or together with others
decide the purposes and means of data processing. Defined specific activities
of states or bodies are excluded from the scope of the GDPR,
but this does not apply to parliamentary activities.
The previous resolution of the data protection conference of September 5, 2018 on the application
application of the GDPR in the area of parliaments, parliamentary groups, members of parliament and political par-
parts was then suspended by the data protection supervisory authorities (see overview
on the resolution materials of the data protection conference under 7.3).
With regard to the political parties, which are also to be classified as non-public bodies,
there are no changes compared to the previous conference resolution of 2018
gen. On the one hand, they continue to be addressees of the GDPR, on the other hand, they are subject to it
indisputably subject to the supervision of the data protection supervisory authorities.
I will the Saxon State Parliament in the matter - after consultation with the other
ren data protection supervisory authorities – further advice.

1.6

1.6

The Saxon Data Protection Implementation Act

Relationship to the General Data Protection Regulation and the Federal Data Protection Act – Consent im Employment Type

During the reporting period, I was also faced with questions about the form of effective consent after the General Data Protection Regulation (GDPR).

The Saxon Data Protection Implementation Act does not contain any further provisions Consent. According to the Saxon legislator, the regulations of the GDPR are sufficient. As in the 18th activity report (04/2015 to 03/2017) under 1.6, page 26 ff. already shown, the GDPR only allows national and state legislatures to Reich-specific specifications and supplements regarding the consent.

Section 11 of the Saxon Data Protection Implementation Act regulates the processing of employee data from public Saxon authorities. A consent regulation as in the previous Script of § 37 of the Saxon Data Protection Act does not contain § 11. Nevertheless it should not lead to misunderstandings. Consent in the employment relationship is also Area of application of Section 11 of the Saxon Data Protection Implementation Act permitted. Included the consent in the employment relationship, also because of the in the service and employment relatively even data processing tends to remain the exception. The voluntariness must also be guaranteed despite the dependency relationship.

In contrast, the Federal Data Protection Act (BDSG) in Section 26 (2) sentences 1 and 2 set rules for voluntariness. About the provisions of the GDPR on consent Based on § 26 paragraph 2 sentence 3 BDSG the written form or electronic form of consent, unless another form is appropriate due to special circumstances

be sen. Sentence 4 also includes the obligation to provide information in text form about the purpose of the data processing and the right of withdrawal according to Art. 7 Para. 3 GDPR. In addition, in Para. 3 also in the case of consent to the processing of special categories of personal 2 (cf. § 26 Para. 3 Sentence 2 BDSG).

Occasionally, considerations are given in the literature on the supplementary applicability of the federal data protection regulations also for those responsible and bodies under state law represent. The wording speaks against it: The BDSG only applies to public bodies of the federal states apply insofar as data protection is not regulated by a state law and - cumulatively - to the extent federal law is carried out, which applies to the processing of employment date is not to be affirmed.

The state legislature simply did not provide for such regulations. supplementary I am convinced that the BDSG cannot be applied.

As a result, one becomes what the presumptions of interpretation and what, in particular, the written form As far as the consent is concerned, that according to the Saxon Data Protection Implementation Act is not is required to often come to the same or comparable results in practice but also an obligation to provide evidence of consent (cf. Art. 7 para. 1 GDPR and recital 42 sentence 1 GDPR). For the processing of special categories This applies in particular to categories of personal data, since in this case an "express che" consent is required. In my previous activity report I had already to the expediency of a written declaration by the consenting party for the responsible verbatim (see 18th activity report for the public sector (04/2015 to 03/2017), 1.6, page 26 ff.). The written or electronic form of the consent Saxon public bodies are independent of a corresponding formal requirement. to recommend.

Consultation on government legislative projects

In the reporting period, I was assisted in various legislative projects

tend to be involved. These were, for example, statements on the Saxon

E-Government Law Implementation Ordinance, on the Saxon School Law and the

Saxon Corona Protection Ordinances and the Saxon Implementation Act on the

State Treaty on Gambling. I also took a stand with the other members of the data

protection conference with regard to federal legislation, for example in the evaluation of the federal

data protection law or the draft of the register modernization law.

Art. 36 Para. 4 General Data Protection Regulation (GDPR) stipulates that state legal

legislative bodies, both in formal legislation and in regulations that

concerning personal data processing, the supervisory authority has to be consulted

ben. It applies – of course – also to the level of the national states.

Recital 96 of the regulation under European law states that the consultation of the

supervisory authority during the drafting of laws or regulations

to ensure the compatibility of the planned processing with the GDPR. To that extent

It should be emphasized that my department regularly has to be involved in a timely manner

strive is.

The obligation to consult my authority applies to projects of substantive legal

of any kind. This also includes mere changes that perpetuate individual legal

subject to son-related data processing. In my opinion

are also included for state treaties that the Free State of Saxony is also signing. she binds

the state government, but also the Saxon state parliament and its organs, if

legislative projects are to be initiated by the state parliament (see 1.5).

The rules of procedure of the Saxon state government contain a provision on the participation
of the Saxon Data Protection Officer (see § 12 Para. 3 Sentence 2). the material
legal provision of Art. 36 Para. 4 GDPR and the considerations presented
could the determination contained in the rules of procedure of the Saxon state government
in § 12 para. 3 sentence 1 only correspond to a limited extent, they are also referred to sentence 2 and so far
the Saxon data protection officer regularly after the completion of a referee
should be involved. According to the wording, “draft laws, draft legal
State government regulations, draft bills and state government letters
[...] only after the state government has passed a resolution on the release for the hearing
state parliament, other bodies, associations or other organizations"
the. It should be kept in mind that according to the ideas of the European regulation
the participation of the supervisory authority (consultation) "during the preparation"
and to ensure compliance with data protection law. at
more complex legal texts related to data processing is also recommended for the
lead department of government an early involvement of my
hear. Submitting the text of the Rules of Procedure, not necessarily related to the
the preceding sentence must be read and the wording simply states that so far
the right to informational self-determination is affected, the Saxon Data Protection
commissioned to participate is such that a prior consultation of my
authority is not excluded, one could and should get the best possible advice
participation of my authority into account.
Beyond the appeal for an early consultation, it remains for me to comply with Art. 36
Para. 4 GDPR to be warned in principle. Failure to comply is of course a violation of
the GDPR.
Finally, I would like to point out Section 20 of the Saxon Data Protection Implementation Act.
According to this, public authorities have informed my authority about the intended enactment of

administrative regulations – insofar as they relate to the right to informational self-determination –

to inform. This is a supplementary provision for sub-statutory

Legislation, which I did not have to consider further in the above context.

37

Chapter 1 Data protection in the Free State of Saxony

1.8

Act on the 23rd Broadcasting Amendment State Treaty

The Saxon Committee for Science, University, Media, Culture and Tourism

In spring 2020, the state parliament passed the state government's draft law into law

on the 23rd Amendment to the Interstate Treaty on Broadcasting (Printed Paper 7/679). I

took this as an opportunity to inform the committee of my position on data protection

to share. The conference of the independent data protection supervisory authorities of the federal and

Länder (DSK) already discussed the planned changes to the circular in spring 2019

radio amendment state treaty concerned. The privacy concerns were resolved

the then conference chairman Prof. Dr. Dieter Kugelmann, State Commissioner for

data protection and freedom of information Rhineland-Palatinate, in the meeting of the broadcasting

presented to the commission of the countries. In April 2019, the data protection conference

tion as a resolution "Planned introduction of a regular complete transfer of registration data

stop the same for the purpose of collecting the license fee" approved – published

as a PDF file on datenschutzkonferenz-online.de.

Irrespective of this, on June 6, 2019, the heads of government of the federal states approved the draft of the

23rd Amendment to the Interstate Treaty on Broadcasting adopted. The Saxon State Parliament was

President of the Free State of Saxony on June 21, 2019 (printed paper 6/18143)

informed.

The present draft itself was unchanged with regard to the comparison of reporting data. He was

but "to maintain the proportionality between contribution justice and protection

personal data” has been supplemented by a regulation according to which a comparison is not carried out should, insofar as the commission for determining the financial needs of broadcasters (KEF) determines that the database is sufficiently up-to-date. The assessment should be made by the Commission taking into account the development of contribution revenue "and other factors" make. In addition, the draft contained restrictions on the rights of those affected Persons for information in accordance with Art. 13 General Data Protection Regulation (GDPR) and future (Article 15 GDPR).

The data protection conference has already approved the first data collection carried out in 2013 immediately classified as highly questionable in terms of data protection law. The concerns raised at the time With reference to the necessary survey as part of the conversion of the fee renmodells on the housing principle and the uniqueness of the survey.

The now planned regular repetition of the complete comparison of reporting data in a four-year cycle represents a disproportionate interference in the informational constitutes self-determination and conflicts with the principles set out in the GDPR of data minimization and necessity (Art. 5 para. 1 letters a and c, Art. 6 para. 1 GDPR). In the case of a complete comparison of reporting data, data from

1.8

Persons are processed who are either not liable to pay contributions (other residents or the resident next to the contributor in an apartment or general fee paid) or are already properly recorded as paying contributions. In addition, includes the registration data comparison more data, for example doctoral degree and marital status, than for one contributions are required.

Incidentally, the broadcasters themselves assume that a complete de-registration ultimately leads to an additional, permanent attachment in less than one percent of cases registration of contributors (see evaluation report of the federal states according to § 14 para.

9a Broadcasting Contribution State Agreement of March 20, 2019). The needs of broadcasters after a legitimate safeguarding of their income would be the same with targeted measures realizable, for which special transmission powers could be created. Instead of-

sen should be a transmission of the complete database of the residents' registration offices in be made permanent for all adult citizens.

The regulations do not sufficiently take into account the standards of the GDPR.

Due to the priority of application of European regulations, national data protection regulations can be based on an opening clause of the GDPR. In case of rain

ments based on the opening clause according to Art. 6 Para. 2 and Para. 3 in conjunction with Art. 6 Para. 1 letter e GDPR are supported, the principles of data minimization and to be observed. According to this, Member State regulations for the fulfillment of Tasks are introduced that are in the public interest if they do not comply with the GDPR specify, but not exceed their limits. Regulations relating to this opening clause must therefore remain within the framework specified by the GDPR. at of the new regulation there are considerable concerns in this regard with regard to the Principles of data minimization and necessity.

The provision for the waiver provided on the basis of the statements made by the data protection conference on the comparison of reporting data is also problematic. The law leaves specifications for Determination of the up-to-dateness of the reporting data to the KEF with the vague formulation "un-

ter consideration of the development of contribution revenue and other factors".

However, the data protection concerns are not sufficiently taken into account.

Rather, the supplement creates an additional constitutional problem in that the Decision on the implementation of a complete comparison of registration data to the KEF de-

is alloyed without providing clear criteria for this decision. Such significant decisions related to the processing of personal data of all

However, the legislature must

meet themselves (provided by law).

The law continues to provide for restrictions on the rights of data subjects. so can

Information rights of the persons concerned are limited according to Art. 15 DSGVO. That there-

principle provided for in data protection law that information is complete or with legal information

stipulated exceptions is grossly disregarded in the law, in that an

Future disclosure is limited to an exhaustive list of dates. This planned loading

Restriction of the right to information is not compatible with the provisions of the GDPR: Art.

23 para. 1 GDPR contains a final list of the reasons for which the national

National legislators have rights that go beyond the scope provided for in the GDPR itself

can restrict. The legislature relies on the “protection of other important

Objectives of general public interest”. The justification states that the re-

success is intended to 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

don't endanger resses". This justification is in view of the information to be expected

absurd and disregards the fundamental rights of data subjects enshrined in the GDPR

to.

The additional restriction of the right to information for data "which is only stored for this reason

are because they are not due to legal or statutory retention requirements

may be deleted or exclusively for the purposes of data backup or data

serve as a protection control" is also not permitted under data protection law.

ber has the failure to provide information in accordance with Article 15 GDPR in the Saxon Data Protection

Implementing Act (SächsDSDG) conclusively regulated. The current regulation

the information rights of the persons concerned about the otherwise for public bodies

of the Free State is further restricted, without there being a need for this

is evident.

The Saxon state parliament passed the law for the twenty-third broadcast amendment state

contract on April 29, 2020.

1.9

“Self-initiated” public relations work by authorities

Occasionally I receive complaints from people who refer to police publications

addressed because the information in the reports makes it possible to identify their

allowed. The persons addressed are mostly victims

of crimes. So last year I received a petition from a doctor whose practice

had become the target of a burglary. Published in the media information that has been issued

on the website of the responsible police department, was from a burglary in a doctor's office

on the specifically named street. The report also contained information on the amount of

Theft and damage to property as well as the information that a safe with an exactly designated

A total of cash, blank prescriptions, various medicines and data carriers have been stolen

be. On the basis of the local information, it was possible to draw conclusions about the specific practice

be sen. On the day the police published the report, the doctor was from

a tabloid and acquaintances have been contacted and questioned about the burglary, under

among other things, whether patient data had been stolen.

40

1.9

The case highlights the risks involved in publishing information that is too precise

concrete occurrences. Is based on the information in the police information

reference to a person can be established, there is an encroachment on the fundamental right of the person concerned to

formal self-determination. A legal basis required for this

something is missing. In the - constructive - discussion of the incident with the police department turned out

It turned out that no guidelines or comparable regulations existed to date that would

Describe the evaluation process for the publication of facts relevant to the police

ben. I have therefore submitted to the Saxon State Ministry of the Interior (SMI)

prompted to encourage the police departments in the Free State to formulate data protection

the production and publication of police reports and media information

support by providing information on avoiding personal references in corresponding reports

be given.

In September 2020, the communication guidelines of the Saxony police came into force, which

framework for communication by the Saxony police with regard to objectives, structure,

gifts, content and processes are in force.

In addition, based on my suggestion, the revision of the joint administration

regulation of the Saxon State Ministry of Justice and the Saxon State

Ministry of the Interior on informing the public in law enforcement matters

of January 29, 1992 under the leadership of the Saxon State Ministry of Justice

and for Democracy, Europe and Equality (SMJusDEG). As part of the

I was contacted by the SMI for the necessary coordination of the SMI with the SMJusDEG

Opinion requested to what extent § 4 Saxon law on the press

(SächsPresseG) as the legal basis for “self-initiated” public relations work by state

Authorities - in the context of which personal or -related

raw data can be disclosed - can be used.

I have always been of the opinion that information from authorities that is self-initiated, i.e. without

underlying press request, on the website of the authority or in another

be published and which are therefore not (only) aimed at the press, but

are indirectly intended for a broad public, due to a lack of suitable authorization

impermissibly interfere with fundamental rights if they involve personal or personal

contain draggable data. According to § 4 paragraph 1 sentence 1 SächsPresseG all authorities are obligated

tet, the representatives of the press and radio, who identify themselves as such, who

to provide information serving the fulfillment of their public task, unless special

succeeded in the Saxon law on the press itself or general legal

ten to oppose it. According to the legislative will, not everyone is

or "the public" entitled to claim. In what way the authority

("How") answered the specific request of one or more press representatives (general

service information by press release or singular provision of information) is fundamental

at their discretion. However, the authority must, as part of its comprehensive assessment

between the interest of the press in the disclosure of the information and the opposite

Interests of those affected in the omission of information also take this point into account (§ 4

Para. 2 SächsPresseG). Thereafter, the authority may provide information to the press representatives

tern, among other things, refuse if and to the extent that they cause an overriding protection worthy of protection

private interest would be violated or the scope would exceed what is reasonable.

So it would hardly be necessary and proportionate to respond to a request from a single press

representative by means of a general press release accessible to all.

In any case, the requirement for the provision of information is at least one request

authorized representative of the press.

Of the opinion that § 4 SächsPresseG is not a suitable legal basis for "self-initiated"

official public relations work with the disclosure of personal and related data

ten is also not inconsistent with the fact that the provision of information to representatives of the press is purely factual

- in the event of later publication of the information by the press - in their effects

to the protected right to informational self-determination of the data subject of the direct

Informing the public often equals. When publishing these personal

The data collected or related to persons by the press are not

State interference in the constitutionally protected legal sphere of citizens, but, at least

if, in the activities of press representatives, an activity that is also protected by fundamental rights

ability. However, an authority is not active as a journalist. Even if they do public relations

drives, it cannot invoke freedom of the press.

These principles and in particular the finding that the state law determined

Right to information of the press no legal basis for self-initiated information

public with disclosure of personal data by authorities, were

recently by a decision of the Higher Administrative Court of Münster on an (illegal) internet publication

Investigation of a district court about the indictment against a celebrity confirmed (OVG Münster,

Resolution of February 4, 2021 - 4 B 1380/20).

The basic considerations on Saxon press law and the authority to

The ability or the media to disclose information does not only apply to the police and

prosecutor; they can be transferred to other areas of administration.

42

2.1

2

Principles of data processing

2.1

Data processing principles, definitions

2.1.1

Company doctor as his own responsibility within the meaning of

Art. 4 No. 7 GDPR

I occasionally had to deal with the question of whether company doctors were

responsible within the meaning of the General Data Protection Regulation. internal operating

I am convinced that doctors are functional positions within the responsible body

to watch. However, they belong to the person responsible and are not responsible for their own

chen. This also applies if the company doctors act as persons subject to professional secrecy. Although subject

You are subject to a special obligation of confidentiality, which means that you are within the data processing body act informationally isolated and they are also subject within no obligation to issue instructions regarding their area of activity, which is subject to secrecy, yet they remain part of the entity. Affected rights, such as not uncommon occurring information, are independent from internal company doctors without violating to fulfill confidentiality obligations. However, the person responsible has the technical and organizational to create technical possibilities and prerequisites for procedural implementation (cf. also activity report 2019, 9.3, page 165 ff. and activity report 2017/2018, 2.11.1, page 103 f.).

The activities of external company doctors should be viewed differently. These are about own responsible persons who process data on behalf of the personnel administration tend to be active, but they themselves are aware of the purpose and means of processing the personal gene data.

2.1.2

Data protection officer as the person responsible

In the last reporting period, I was confronted with a complaint in which affected persons contacted me because they wanted information from an external data protection officer coveted. The persons concerned had previously contacted the person responsible, who actual data processing office, with a request for information, whereupon the external data protection officer had become involved.

My authority treats the internal data protection officer as one of the responsible to be assigned to officials, even if they act independently – Art. 38 Para. 3 Sentence 1 of the General Data Protection Regulation (GDPR) - and a person subject to professional secrecy is provided (cf. 3.1.2 at the end and the wording of Art. 38 Para. 5 GDPR, cf. also Activity Report 2019, 9.3, page 165 ff. and Activity Report 2017/2018, 2.11.1, page 103 f.).

It is to be judged differently in the case of a commercially active – external – data protection commissioned. This operates the personal data processing processes and determines the purpose and means of processing.

The contents of the processed data are also not incorporated. That means the data processing tion is outsourced and with the processing of the person responsible for the external data named data protection officer, only partially identical. In this way, even with external data protection officer in practice Complaints and deviating content of the complaints are processed to which the naming person responsible does not have access or which has been withheld from him not only for reasons of secrecy but also procedurally be held (cf. 2.1.1).

In this respect, data subjects also have a fundamental right to information in accordance with Art. 15 DSGVO towards external data protection officers. Request for information to inter-
A data protection officer, on the other hand, is intended as information to the person responsible to evaluate. In the case of confidentiality obligations in question, the internal data protection officer but may also be active in providing information themselves.

2.1.3 MDK Reform Law – Medical Service as its own Responsible

With the MDK Reform Act (BT-DS 19/13397), which came into force on January 1, 2020 the medical services of the health insurance (MDK) no working groups of Health insurance companies no longer constitute but are considered a separate public body Legally uniform under the designation "Medical Service" (MD).

In the course of this is in paragraph 276 paragraph 2 fifth book of the Social Code (SGB V) - he is for the MD a central legal basis for data processing - the provision of § 35 SGB I expressly included. This ensures that the MD is also in its new Legal form as an independent corporation under public law as a body according to § 35 of the

First book (SGB I) subject to social data protection. This was previously the case because the

MDK as a working group of the health insurance companies is covered by § 35 paragraph 1 sentence 4 SGB I

were. In order to lower the level of protection for the data processed by the MD

prevent, it is appropriate to continue the MD to the strict area-specific

To bind regulations of social data protection according to the SGB.

2.1.4

Covert collection of vehicle number plates - transparency

A customer of a company that rents high-quality equipment to casual customers had

complains that an employee of the company has lost the license plate number of their im

yard of a motor vehicle parked in a customer parking lot is noted on a piece of paper

would have.

When asked, the company admitted that it cleaned up vehicle registration number data in individual cases

non-automated way (paper note), unless there are other suitable options

ability to identify (usually by presenting the personal document) is possible. Firmly-

However, the affected customers should then be informed immediately about this

to have. After the rented device has been returned without any complaints, the data will be sent immediately

deleted again.

The contradiction between the facts that are not disputed in this respect and the Compli-

I did not follow the ance rule any further. It was also questionable whether the objective application

had been opened up under the General Data Protection Regulation (GDPR) (Art. 2 Para. 1

GDPR). However, I have made it clear to the company that communicative trans-

parenz with regard to the protection of legitimate interests helps to avoid complaints (cf.

Art. 5 letter a GDPR). This statement applies universally.

2.1.5 Redacted ID card copies according to the Money Laundering Act -

data minimization

According to Sections 8, 10, 12 of the Money Laundering Act (GwG), those responsible under money laundering law must check the identity of the beneficial owner of a transaction (to be initiated) and document this. In principle, a copy of the identity document presented is to be negligent, since a corresponding legal obligation is obeyed (cf. Art. 6 para. 1 letter c GDPR).

However, the exact scope of this mandatory copy of the identity document is disputed ten. Since the underlying provision of section 8 (2) sentence 2 of the GwG has been recent changes in the law, most recently at the beginning of the reporting period conflicting information here.

I regularly receive complaints and requests for advice on this topic. Besides was the question of the possibility of a partial blackening of corresponding copies or Restriction of electronic copies, for example through copy masks, is also a subject of the Working Group on the Banking Industry of the Data Protection Conference (DSK).

In my well-established opinion, for a number of reasons, the identification subject to the right to include information not required for the purposes of the GwG in the copy of the to make the identity document unrecognizable or, in the case of the optoelectronic to partially cover the frame, in particular body size, eye color, photo and gear numbers; see details below.

The underlying anti-money laundering registration of those responsible and transactions is regularly expanded, so that smaller entrepreneurs such as brokers and Goods traders are affected. From the multiplication of affected transactions and corresponding systems for data processing is followed by a considerable increase in data intellectual property risks. This means that there are no longer just a few, central and extensive

responsible persons equipped with compliance systems for documentation according to AMLA

obliges. Rather, corresponding copies over a seven-digit number are sometimes small

secured IT and filing systems. In addition, the increasing digital

ized recording of copies of ID cards, which has resulted in a massive increase in the risk of misuse

to limit sam. Because such high-resolution electronic copies (scans) typically

a substantially higher quality and further use compared to photocopies

ability to. They can also be lost much more easily, leading to identity theft and

Document falsification are misused.

The right of the data subject to blackening or partial coverage mirror-image

The legal obligation for those subject to documentation follows from the requirement of data minimization (Art. 5

Paragraph 1 letter c GDPR). This applies in particular to electronic copies or scans,

whose data protection risk is significantly increased compared to paper copies.

Because even with the collection and processing of ID card copies, the updated word

according to Section 8 (2) sentence 2 GWG and higher-ranking law. only for

the video identification can apply that the complete recording of the ID document

mentes is permissible, insofar as this is covered by the consent and for the purpose of identification

cation is required. This data, which is increasingly susceptible to misuse (cf. e.g

"deepfakes") have increased again in line with the risks they pose.

subject to protection obligations.

In all cases in which responsible persons based in the Free State of Saxony make copies

wanted or made, I was able to black out or partially

obtain cover during the copying process. In cases where (also) by other authorities

supervised persons responsible make copies, I can only do this within the scope of my

performance mandate on my legal opinion and, if applicable, the legal clarification

durfnis and refer the procedure to the competent authority.

In order to counteract the inconsistency of legal interpretation and those responsible such as

affected persons to make their own decision within the scope of their responsibility or

to enable wise rights, the main arguments are presented below:

For the completeness of the copy to be made and thus the exclusion of blackening

tongues it is stated that conceptually every copy has to be complete. Also be the

of the Ministry of Finance of this opinion - of course without recognizable for the concrete

Money laundering tracking and investigation competent authorities would have been involved. a con-

46

2.1

concrete content-related reason for this view, despite detailed discussions, is neither pre-

worn can still be seen. However, according to this view, the earlier qualification of the

copy to be made in the law to implement the Fourth Money Laundering Directive, to

management of the EU money transfer regulation and the reorganization of the central office for financial

transaction investigations as “complete” would at least have been superfluous.

It is true that from the legislative materials of the Act on the Implementation of the Amending Directive

line to the Fourth EU Money Laundering Directive is not immediately apparent for what reasons

legislator has removed the qualification “complete” from the provision of Section 8 (2) GwG.

However, there are no indications of a legislative error: The 2020 in § 8

Paragraph 2 of the GWG carries the express specifications of the implemented

the Fifth Money Laundering Directive bill (Directive (EU) 2018/843 of the European

Parliament and Council of May 30, 2018 amending Directive (EU) 2015/849 on

Preventing the use of the financial system for the purpose of money laundering and terrorism

mus funding and amending Directives 2009/138/EC and 2013/36/EU). Art. 1 No.

25 explicitly emphasizes the limitation of the copy to what is necessary. After that is "a copy

of the documents and information received that are required for the fulfillment of the due diligence

are required for customers in accordance with Chapter II".

There is also no reason why the data protection principle of the data mini-

5 Para. 1 Letter c GDPR could be inapplicable here. Already the club

availability of the earlier version of Section 8 (2) GwG (2017: "complete copies of this documentation

ments or documents or to record them completely optically digitized")

higher-ranking law seemed quite doubtful. Because the requirement of data minimization

wise data economy does not arise from simple law, but is persuasive

considered a direct result of the constitutional right to informational

Self-determination (see BVerfG, judgment of December 15, 1983 - 1 BvR 209/83).

The corresponding justification in the legislative process of the GWG 2017 is at best

misleading and can hardly justify the "completeness" of copies introduced in 2017.

gene:

“Section 8 serves to implement Article 40 of the Fourth Money Laundering Directive. The rule

essentially corresponds to Section 8 of the previous Money Laundering Act. Because Art. 40 para. 1

Letter a of the Fourth Money Laundering Directive more than the Third Money Laundering Directive

copies, paragraph 2 sentence 2 provides for the production of complete copies of the documents

and documents required to verify the identity of the natural or legal person

serve.” BT printed matter 18/11555, page 114 f. = BR printed matter 182/17, page 130 f.

The Fourth Anti-Money Laundering Directive (Directive (EU) 2015/849 of the European Parliament and

Council of May 20, 2015 to prevent the use of the financial system for the purpose

money laundering and terrorist financing, amending Regulation (EU) No.

648/2012 of the European Parliament and of the Council and repealing the directive

2005/60/EC of the European Parliament and of the Council and Directive 2006/70/EC of

Commission) itself, however, does not provide for completeness of the copy at any point, but

rather requires data minimization: "Personal data should be

data are only collected and processed to the extent necessary to fulfill the

requirements of this directive" (recital 43, page 3).

Such as the storage of body heights (stored in ID documents), eye color

information, photographs or access numbers for combating money laundering or implementing

could serve the directive is not evident. While the explanatory memorandum of the

GWG 2017 thus stipulates, with Section 8 GWG 2017 essentially the Fourth Money Laundering Directive

implement, the law blatantly violated their express requirements and higher

senior right. The Fifth Money Laundering Directive implemented with the GWG 2020

further reinforces the importance of the principle of proportionality under data protection law

(cf. recital 5, page 2) and data protection in general (cf. recital 21,

38, 51). In this respect, it seems extremely obvious that the German legislature with the new

version of Section 8 Para. 2 GwG union, constitutional and data protection-compliant

wanted to ask.

In my opinion, it follows fundamentally from the right to informational self-

Provision and the corresponding Union and human rights requirements that the

Collection and processing of data not required for the purpose of the law to

has to stay. This probably applies regardless of the fact that the Fourth and Fifth Money Laundering Directive

should be able to grant sufficient concrete individual rights in this respect, and thus the data mini-

nification is also mandatory due to a guideline-compliant interpretation of the Money Laundering Act

seems.

A binding clarification of this question by the courts seems desirable and

tually the only way to have uniform interpretations throughout Europe or Germany

bring about gene.

2.1.6

Data minimization in the social field: scope of the

Where-used check of the integration aid

documents to be checked

A petitioner had asked me to check which documents the district social welfare office had

from a data protection point of view to check the proof of use of the integration

request assistance.

The petitioner described the situation as follows: He is receiving integration assistance

the social welfare office and receives benefits in the form of a personal budget that

use of support services. In a contract between the social welfare office

2.2

and the petitioner was also regulated, among other things, as to how the proof of use

has taken place.

Referring to the proof of use specified in the contract, the pe

tent to me. On the one hand, he complained about the request for personal data for the

Checking the use of the services paid, for example presenting the account statements

trains of the budget account. On the other hand, he opposed the conduct of a detailed

care diary. In his opinion, an income and expenditure account is sufficient.

In my opinion, it is necessary to compare income and

Expenditure with the account statements of the budget account and the associated meaningful ones

Maintain and submit evidence/receipts for the billing period. The template of

Receipts are required to prove what income or expenses are actually

materially incurred.

Since these are public funds that are being used, I see the dated

The district office accepts the total amount of proof of use as required.

The stipulations made therein regarding the evidence were based on data protection law

View therefore not objectionable.

2.2

Legality of data processing

In the past year, I received a large number of inquiries and complaints about the

clock data collection in the coronavirus pandemic. A selection of cases can be found in the

Articles 2.2.1 to 2.2.7. In addition, there were events worth mentioning regarding the legality of the

Data processing from the public area (2.2.8 to 2.2.14) and in the non-public area

rich (2/2/15 to 2/2/22). The submissions for videography did not ebb in 2020 either. some

games are listed in 2.2.23 to 2.2.30 (see also 1.4, 3.1.1, 3.2.3, 4.2.1).

2.2.1 What happens to my personal data at a

corona test?

A person who tested positive for COVID-19 has

contacted me at the end of March 2020 and asked me to let me know what happened to his personal

related data or health data collected during the test

ted. He asked for information on who these will be passed on to.

Getting tested for COVID-19 usually requires going to your family doctor first

to go, as the Corona ambulances require a referral from the family doctor. With his

doctor, the person concerned concludes a treatment contract. § 630 f Civil Code

(BGB) regulates that patient documents are to be kept for ten years. These include the

example findings.

The sample taken from the patient during the corona test is not a personal

Personal data within the meaning of Art. 4 Para. 1 General Data Protection Regulation (GDPR). First

when it is analyzed and information concerning the patient is processed

– the laboratory determines that the patient has COVID-19 or suspects it

has not been confirmed - is this the case.

COVID-19 is a notifiable disease within the meaning of Section 6 Infection

Protection Act (IfSG). Should the doctor determine that the patient is ill with it, he has

according to § 8 Abs. 1 Nr. 1 IfSG. A commissioned laboratory has verified this finding

§ 8 Para. 1 No. 2 IfSG to report to the responsible health authority.

According to § 9 IfSG, it is a nominative report. § 9 para. 1 respectively

Para. 2 IfSG lists the other points that the report includes, for example address and

Contact details. The report must be sent immediately to the responsible health authority of the state

district or the district-free city.

The processed data to reportable data are according to § 11 IfSG by the health

heitsamt in whose district the patient has his main place of residence, via the competent state

authority - in Saxony the state investigation institute - to the Robert Koch Institute (RKI)

reported. This message is pseudonymised. This means that the RKI cannot relate to

Create person of patient.

I also informed the person concerned that the RKI on its website rki.de under the

Item "COVID-19" Answers to frequently asked questions about the coronavirus SARS-CoV-2/

disease COVID-19 has stopped. To the answers to the questions about what is notifiable

is how the reporting process works and what information is transmitted to the RKI

I pointed out.

Since the IfSG regulates who has to report which data and to whom the report is made

Transmission of personal data within the meaning of Art. 4 No. 1 GDPR by the doctor

or the laboratory to the health department and then to the RKI according to Art. 6 Para. 1

Letters c and e and paragraph 3 DSGVO lawful, since the processing is necessary for the fulfillment of a

task is required which is in the public interest. As far as the transmission is concerned

of the patient's health data within the meaning of Art. 9 Para. 1 GDPR, this is after

Art. 9 para. 2 letters g and i as well as para. 3 DSGVO permissible.

50

2.2

2.2.2

Management of visitor lists at Saxon courts

In the spring of 2020, I received a series of inquiries about keeping visitor lists
contained in Saxon courts. In an effort to narrow it down
of the infection process in the emerging pandemic, the courts laid
aisle area lists. Visitors to the court should register in it in order to
to enable contact tracing that may be necessary. Uniform specifications are
tens of the State Ministry of Justice, for Democracy, Europe and Gender Equality
(SMJusDEG) for the procedure of the court administrations did not exist.
After contacting various jurisdictions and locations due to the impact
that SMJusDEG had contacted, our houses quickly agreed that
that due to the lack of a legal basis for the collection and storage at the time
processing of visitor data for infection protection purposes
with the consent of the person concerned (Article 6 (1) (a) GDPR).
A legal basis for collecting the contact details of visitors to the courts was found
neither in the Infection Protection Act (IfSG) nor in the then valid Saxon Corona
Protection Ordinance (SächsCoronaSchVO). On the house-
right the presidents and directors of the courts could the collection and storage of the
Data also do not base, since such an interference with the fundamental right to informational
Self-determination – at least for non-domestic purposes such as protection against infection – one
norm-clear legal basis and not in exercise merely habitual
legal powers (Art. 6 Para. 3 GDPR; Federal Constitutional Court decision
divorce 65, 1, para. 151; Art. 33 Constitution of the Free State of Saxony).
As a result of our exchange, the State Ministry agreed with the Presidents of the
sian higher courts and the Attorney General of the Free State of Saxony "Action
Recommendations for the courts and public prosecutors of the Free State of Saxony for the
Duration of the coronavirus (SARS-CoV-2) pandemic". After that, visitors should

Visitors to courts and public prosecutor's offices as part of access control when

entering the building will be asked to fill in the visitor cards. The visitor cards

should be collected on a daily basis - but in any case under lock and key - and after three weeks

be destroyed. At the same time, the visitor should be in appropriate clothing during access control

How the instructions are given that the collection of your data serves to

to be able to inform possible contact persons of the possible infections, to extract this data

finally used in case of infection and destroyed after three weeks

and that the information you provide is voluntary.

The legal situation changed at the end of the year. With the entry into force on December 11

They were expressly subject to the Saxon Corona Protection Ordinance passed in 2020

also authorities and courts of legal obligation (Art. 6 Para. 1 Letter c DSGVO), name, tele-

phone number or e-mail address and zip code of the visitors as well as the period and location of the

to record visits and for a limited time only for the purpose of contact tracing

ment, i.e. to keep a possible request from the health department. With the

thus created legal basis - § 5 Abs. 6 SächsCoronaSchVO of 11. De-

December 2020 in conjunction with Section 32 Clause 1 in conjunction with Section 28 Paragraph 1 Clause 1 and 2 as well

with § 28a paragraph 1, paragraph 2 sentence 1 and paragraph 3 IfSG - a collection of visitor data was carried out

Courts also permissible without the consent of those affected, more precisely: mandatory. for po-

prospective visitors who want their data to be collected for the purpose of contact tracing

wanted to avoid, the option remained to forgo their visit to the court.

Compare also entry 2.2.3 on visitor lists in the town hall.

2.2.3

Corona registration form in the town hall

A city councilor approached me for a City Hall visit registration form. In

this should be declared in lieu of an oath that in the past 14 days you have been in

did not stop in any corona risk area designated by the Robert Koch Institute, to

had been in contact with someone who was proven to be infected with the virus and feel healthy overall.

I asked the city administration to comment at short notice. I pointed it out

point out that I do not meet the requirement of an affidavit according to § 294 civil procedure

see order. Furthermore, I could not provide any information on the form used in accordance with Art.

13 General Data Protection Regulation (GDPR), such as the retention period,

remove. In addition, it was not pointed out whether the information was mandatory (on

what legal basis?) or are voluntary. Should the latter be the case, of which I

next, the consent would not have met the requirements of Art. 7 GDPR.

The designated municipal data protection officer then informed me that my concerns

ken would be shared. Passed against the revised and sent registration form

no data protection concerns.

See also 2.2.2 on visitor lists in court.

2.2.4

Collection of contact data when visiting a hairdresser in the

coronavirus pandemic

At the end of April 2020, I received an inquiry from a customer who wanted to know whether it was legal

It is reasonable that when visiting the hairdresser, the contact details of the respective customer are collected and

if necessary, would also be forwarded to authorities.

52

2.2

With the general decree for the enforcement of the Saxon Infection Protection Act

Ministry of State for Social Affairs and Social Cohesion from March 22, 2020

On the occasion of the coronavirus pandemic, exit restrictions were imposed in Saxony for the first time

imposed (first lockdown). This resulted in drastic restrictions on fundamental rights and

the extensive shutdown of public life, in particular the closure of

barber shops and restaurants.

On March 31, 2020

Then the first Saxon Corona Protection Ordinance came into force

(SächsCoronaSchVO) came into force, which regulated these restrictions on an ordinance basis. the

SächsCoronaSchVO of April 30, 2020 initially saw the opening of certain commercial

Facilities subject to the collection of contact details from customers and

visitors.

I informed the customer that according to § 9 para. 2 SächsCoronaSchVO, as of April 30, 2020, the

Hairdressers from May 4, 2020 hairdressing services under the conditions of compliance

the SARS-CoV-2 occupational safety standards of the Federal Ministry of Labor and Social Affairs and

existing industry-specific implementation and that of the Ministry of Social Affairs and

Social cohesion laid down by general decree hygiene regulations

are allowed to provide. In accordance with point II, paragraph 12 (access of non-company persons to work

workplaces and company premises) of the SARS-CoV-2 occupational safety standard of the Federal Ministry

nisteriums for work and social affairs, the customer contact details should be documented as far as possible.

The trade association for the hairdressing trade has also included in its SARS-CoV-2 work

protection standards, as of April 30, 2020, stipulates that this measure of documentation

of the customer contact data in the operational concept of measures for occupational safety

take is. The background to this contact collection is that the hairdressing trade is one of the

belongs to occupational groups in which, due to direct customer contact, there is an increased

there is a risk, especially since the minimum distance of 1.5 meters is not safely maintained

can be. The aim should be to trace infection chains, e.g.

fection of an employee in the hairdressing salon. With this measure, the infectious

on chains are broken and thus further infections are avoided. aim of this

Contact collection is the health protection of the population and employees.

This data processing is permitted by Article 32 Clause 1 in conjunction with Article 28 Paragraph 1 Clause 1 and 2 Infection Protection Act, § 10 Para. 2 SächsCoronaSchVO in conjunction with Art. 6 Para. 1 Letter c and f General Data Protection Regulation justified.

Also in other areas, such as in the restaurant and hotel industry, the Contact data collection for customers and visitors by the applicable Saxon Corona Protection Ordinance introduced. Due to the large number of inquiries and complaints on the legality of the contact data collection, in particular which data for which purpose may be collected and used, how this data may be collected, how as long as they may be stored and much more, I have a "hand

- Data protection aspects of collecting contact data from customers and

Visitors during the Corona Pandemic" and corresponding sample forms light. These are adapted to the applicable regulation or continuously updated. tualized.

2.2.5 Disclosure of personal data respectively

Health data from the health authorities to the police

In connection with the coronavirus pandemic, I received various inquiries, under which conditions a transmission of personal data is permissible. In some cases it was about passing on the data of those who tested positive from the health officials to the police.

A collection of health data by the police enforcement service or by the rescue control center at the responsible health authorities and the transmission of the necessary In individual cases, I see such data as being sent to the police enforcement service/rescue control center permissible if there are indications of a specific danger.

I justify this as follows:

According to § 7 paragraph 1 sentence 3 law on the public health service in the Free State of Saxony (SächsGDG) in connection with § 6 paragraph 2 sentence 2 SächsGDG comes a transmission from Health data by the health authorities of the districts and district-free cities to Their bodies, such as the police enforcement service, are only considered if this is for defence a danger to the life or health of third parties is required. The person concerned should point this out be shown. Transmission of infection data by the health authorities to the Police enforcement service is permissible in this respect. The prerequisite is the existence of a (specific) Danger to the life or health of third parties and the suitability and necessity of the data transmission of data to avert danger.

However, the SächsGDG does not provide a legal basis for a precautionary (preventive), ad hoc independent transmission of sensitive health data to the rescue control center or wise to refer to the law enforcement service. The same applies to the regulations of the Infection Protection Act (IfSG). The transmission of sensitive health data is in In these cases, it is also inadmissible under data protection law. A general access of the rescue control center or the police enforcement service on data from the health department ill people who are stored in a database, for example, is also included not permitted.

If necessary, an inquiry can be made in individual cases with the health heitsamt by the rescue coordination center or the police for the self-protection of the rescue workers or the police.

54

2.2

A flat-rate transmission of data, especially sensitive health data the health authorities to the rescue control center or the police service, on the other hand not permitted.

2.2.6

Certificates of exemption from the obligation to wear a

Mouth and nose covering in schools

I received numerous inquiries from parents, some of whom even received

was threatened with denying their children access to the school building. background were

the certificate of exemption from the obligation to wear a mouth and nose cover. On the one hand

it was demanded that these must contain a justification, on the other hand they wanted that

In any case, keep a copy of the certificates in the school.

No version of the Saxon Corona Protection Ordinance contained requirements for the

Content of a medical certificate. Accordingly, the Saxon State Ministry for

Social and societal cohesion (SMS) from the beginning on the Internet: "Zur

The presentation of a medical certificate is sufficient for credibility. A separate justification

the doctor is not necessary."

Irrespective of this, the Saxon State Medical Association, which pursuant to Section 37 (1) of the Saxon

sische Heilberufekammergesetz is subject to the supervision of the SMS, in a press release

from November 9, 2020 …

"currently summarized the content requirements for an effective medical certificate. Around

for example, an appropriate decision on exemption from the so-called mask requirement

for medical reasons, the medical certificate must meet a certain minimum

requirements (Higher Administrative Court of North Rhine-Westphalia, decision of 24 September

September 2020 - 13 B 1368/20). […] In addition to the full name and date of birth

It must therefore be clear from the certificate which ones are to be specifically named

Health impairments are to be expected due to a mouth and nose cover

are and from what they result in detail. If there are relevant pre-existing conditions,

these must be specified. In addition, it must be recognizable as a rule

the basis on which the attesting physician came to his assessment."

The SMS probably took this as an opportunity in the justification for the Saxon version

Corona Protection Ordinance of December 11, 2020 (completely correct)

ren:

"[...] also clarifies that to prove the exemption from the obligation to wear the

Submission of a medical certificate issued by a licensed doctor

55

Chapter 2 Principles of data processing

issued by a licensed doctor is sufficient. A separate justification by the doctor

The doctor's consent is not required for data protection reasons.

The person concerned cannot be expected to disclose the diagnosis to strangers.

especially since these people are not medically trained personnel."

I am not aware that the SMS in this case relies on its supervisory rights over the

made use of the Saxon State Medical Association. The press release was over

of the reporting period can still be accessed without comment on slaek.de.

With regard to the admissibility of a copy of the certificate, the Saxon Corona Protection

Ordinance of September 29, 2020 in § 2 para. 7 the following wording: "For credibility

To request an exemption from the obligation according to sentence 1, it is sufficient to present a severely handicapped

tenancy card or medical certificate."

This did not seem to be understandable enough for a number of headmasters. So I turned to

the Saxon State Ministry for Culture (SMK) with the request to take action.

In the meantime, the version of the Saxon Corona Protection Ordinance of 21.

October 2020 even clearer: "To substantiate an exemption from the obligation according to sentence

1, granting access to a severely handicapped ID card or a

medical certificate."

The SMK then also announced in a letter from the headmaster on October 30, 2020:

"The copying of certificates, with which schoolchildren from wearing a mouth

No nose covering is permitted. Likewise, it is not permissible to use these certificates

to put in the student file. The Saxon data protection officer pointed this out.

However, it should be noted for the respective student

that a corresponding certificate has been submitted."

The SMS finally took a complete U-turn with the version of the Saxon Corona

Protection Ordinance of November 27, 2020. There it was now regulated in § 3 para. 3:

“Schools and child day care facilities are authorized to use the medical certificate

which an exemption from the obligation according to paragraph 1 is made credible, in an analogous or

digital copy or, with the consent of the presenter, the original."

In my opinion, this was still permissible under data protection law, since

has been regulated that the copy or the certificate is to be secured against unauthorized access and after

Delete or destroy it immediately at the end of the period for which the certificate is valid

is, but at the latest by the end of 2021.

56

2.2

What was not regulated, however, was the relationship between the still existing general

Restriction on Permission for Inspection and Permission for Schools to Permit Copies

create. The justification of the version of the Saxon Corona Protection Ordinance of

December 11, 2020 will lead to this (albeit with the wording of the

now § 3 paragraph 4) from: "It is now also made clear that the school or

childcare facility may make a copy of the certificate; the submitter has

to allow and tolerate this.”

2.2.7 Health Certificates for School Attendance

In the spring of 2020, numerous parents contacted me. It was about fulfilling the

long health confirmations. These had to be shown daily and belonged to the public

tion concept of day-care centers and elementary schools with fixed, separate groups. child

who are only allowed to take part in lessons if neither they themselves nor members of the

household showed symptoms of the disease Covid-19. Parents had to do this every day
certify signature. The Saxon State Ministry for Culture (SMK) presented in
clear to the press that no liability is associated with this. I have no data against this
had concerns about property rights; the case law of the last instance saw this as well.
However, the storage of these monthly forms as practiced by some schools was not permitted,
as the SMK confirmed to me on request. Some of these were provided by the schools
collected at the beginning of the lesson and distributed again after the end of the lesson, partly after
also permanently collected over the course of the respective month. However, all principals have
after my cover letter the data protection violations were stopped and already collected
health certificates issued again.

2.2.8

Inspection of an authorized district chimney sweep

An authorized district chimney sweep complained to me about the
separate district office. This has owners, in their property by a fireplace inspection
the complainant was subsequently sent in writing to answer a number of
asked questions about satisfaction with his job. This included, among other things,
whether the fireplace inspection was carried out in person.

The district office, which I asked for an opinion, first informed me that the
powerful district chimney sweep himself demanded in a letter: "If not for me
is believed, for my exoneration, write down some of the properties where I
was."

Irrespective of this, the questionnaires in question were sent out in
Fulfillment of the supervisory duties according to § 21 Section 1 of the Chimney Sweep Trades Act

can

competent authority

(SchfHwG). Therefore

authorized

District chimney sweeps with regard to the performance of the tasks assigned to them and

powers and compliance with their obligations at any time. To these so-called

Professional duties include, among other things, the personal implementation of the

Fireplace inspection by the authorized district chimney sweep (§ 14 SchfHwG).

I could therefore not identify a data protection violation.

the

2.2.9

Proof of adequate vaccination protection against measles

The entry into force of the Measles Protection Act on March 1, 2020 had numerous complaints

and inquiries at my office. On the one hand, these concerned the procedure

with proof of sufficient vaccination protection against measles and on the other hand the

Ask when the health department should be notified.

In their complaints, several parents complained that the day-care center was managed

or the kindergarten, proof of sufficient vaccination protection against

her child's measles were copied for record keeping.

The Measles Protection Act changed, among other things, the Infection Protection Act (IfSG). This

stipulates in § 20 para. 8 no. 1 that persons who work in community facilities according to § 33

Para. 1 Nos. 1 to 3 are cared for or work, have adequate vaccination protection against Ma-

must have. According to number 1, these include day-care centers and

After-school care centers and, according to number 3, schools and other training institutions.

According to § 20 paragraph 9 sentence 1 IfSG, proof is provided to the management of the facility

by presenting vaccination documentation or a medical certificate of immunity

against measles or a medical certificate confirming the existence of a medical contraindication

tion or confirmation from a government agency that proof has already been provided.

It is sufficient, for example, if the parents of the child to be cared for present the medical certificate

lay. In my opinion, the vaccination card and also a medical certificate are allowed

data protection reasons are not copied and filed, as these

contain data other than that required by law – principle of data minimization. the

The management of the facility can document, for example, with a note that the

proof has been submitted. The documentation should refer to the necessary information

limit

I asked the institution responsible for the institution, here the municipal administration, to comment on the

complaint requested. I informed them about the legal situation and asked them to

Inform the management of the facility accordingly. Should it be true that copies of the

58

2.2

Proofs were produced, these are to be replaced by a note and then

to destroy. In this case, the destruction of the evidence had to be confirmed to me.

A number of inquiries from the parents were also aimed at when by the management of the facility

Information to the responsible health department of the district office or the

District-free city are to be forwarded that contain personal data.

If the medical certificate shows that it is a permanent medical contact

IfSG

rendered.

Immediate notification of the health department and transmission of personal

According to § 20 paragraph 9 sentence 4 IfSG, the data obtained is provided for in two cases: If the proof

according to sentence 1 is not submitted or if it turns out that vaccination protection against measles is only possible

is possible or can be completed at a later date. According to § 20 paragraph 9

Clause 4 IfSG, the health department in whose district the facility is located must

to be notified and to transmit personal information to the health department.

2.2.10 Use of electronic water meters

In my activity report from April 1, 2017 to December 31, 2018 I had myself under

2.2.6 (page 175) already on the admissibility of data processing using electronic water

counter voiced. At that time I unfortunately had to report that the Saxon State Ministry

of the interior did not want to become active because it was difficult to assess "which specific

significance of the situation described on site".

Fortunately, that has changed. After a vote with my authority was

a detailed circular via the Saxony State Directorate to all municipal tasks

water supply agencies (municipalities and special-purpose associations).

The document states that it may be necessary for a municipal

ler authority within the scope of its responsibility for the task of drinking water

ment stipulates in its municipal (water supply) statute that it

uses a water meter or equips it with a radio module. It will be

aptly pointed out that for the use of electronic water meters in

of the public drinking water supply neither the Ordinance on General Conditions

ments for the supply of water (AVBWasserV) are still technically relevant

State laws, such as the Saxon Water Act, area-specific regulations

provide that the requirements of Art. 6 Para. 2 and 3 General Data Protection Regulation

(GDPR) would comply.

Such a statute should in particular contain details on the rights of those affected in accordance with Art.

12 to 17 GDPR are regulated, for example information obligations, rights to information,

Right to rectification and deletion of data, right of objection. In case of use

of radio modules is the principle of data saving standardized in Art. 5 Para. 1 Letter c GDPR.

(or data minimization requirement) must be observed. Depending on the technology used,

For example, regulations on the time intervals in which a radio module data

should be transferred to the water supplier.

2.2.11 Aerial photographs of properties by the public sector

or their agents

Various complaints and inquiries reached me during the reporting period

production and use of aerial photographs. Purpose of such recording

In these cases, the determination of sealed areas to determine the wastewater

subject to a fee and the determination of green spaces to consider a partial exemption from

Waste fees (organic bin obligation).

Although photographic recordings such as aerial photographs regularly represent personal

generative data when recognizing persons or personal identifiers such as license plates

are cash; such a fine resolution could, however, be excluded in the concrete cases

will. In this respect, the decisive factor is the granularity ("pixel resolution") of the prepared

took.

The identifiability of individual plots or houses make the recordings related

on owners and tenants or tenants personally, insofar as the responsibility

literally has the legal ability to sell the affected plots of land to an owner

or assigned to tenants or leaseholders.

for such overflights

I had already familiarized myself with the data protection requirements and

general conditions

(cf. 18.

Activity report for the public sector (04/2015 to 03/2017), 5.5.5., page 57 ff.).

The substantive legal requirements have essentially not changed. such

According to Art. 6 Para. 1 Letter c of the General Data Protection Regulation, recordings can be made

existing (statutory) law to fulfill legal obligations.

Specifically, in the proceedings of the reporting period, the sovereign duty in particular formed

on the fairness of charges, the waste law or (waste) water law

Access rights and the decentrally regulated powers for checking the information

the background. It is harmless if the person specifically responsible as a lien or

acts as an administrative assistant, uses existing databases or a processor

switched on as long as the relevant requirements are met. The data collection

by means of

cost-effective data collection

the possible

aerial photography

served

60

2.2

or verification of information. This was done in the interests of as much

proper relocation of

for waste or wastewater disposal

total costs incurred. On the other hand, property owners and others are – at

corresponding granularity of the recordings - touched only selectively in their social sphere.

The concrete procedures in the reporting period were partly due to the use of the geodata portals of the

corresponding district or the Free State, partly the use specifically

based on finished aerial photos. In all of these cases, the conditions were lawful

data processing. In this respect, it is gratifying that – as far as can be seen – the

general conditions drawn up by my authority in 2017 must also be complied with in the area

the.

2.2.12 Use of Population Register Data by Village Chiefs

A local mayor asked me for a data protection check for the following plans: He
intended to invite all new residents arriving in 2019 and 2020. In addition
should also include those who have bought land to build a dwelling house
erect The aim was to get into conversation with the residents and to ask for help and
to offer support. The voluntary fire brigade, clubs and groups are also trying
to attract new members.

For this purpose, the mayor turned to the municipal administration, which issued a corresponding
should be compared with the residents' registration data. He also asked the concerned
Write and invite residents. However, this was correctly rejected.

Even if the concern - new residents in this way in the village community
to be integrated - is comprehensible, the legal framework conditions must be complied with
become.

According to § 37 para. 1 Federal Registration Act (BMG) within the administrative unit, the
the registration authority belongs, under the conditions specified in § 34 para. 1 BMG
details are passed on. These requirements of Section 34 (1) BMG include
that this is to fulfill within their jurisdiction or within the jurisdiction of the recipient
underlying public tasks is required.

I could not see this in the intended information from new residents. dar
In addition, according to Section 50 (2) of the Federal Ministry of Health, the jubilee
data are made available. The legislator has refrained from further regulations
hen.

I have therefore recommended that the relevant information be provided when registering for the
to comply. Also distributing relevant information to all residents without

Use of the population register would of course be conceivable.

2.2.13 Neighbor participation in building projects

A petitioner asked whether all construction documents, in particular the floor plans

and the dimensions of the individual rooms of the planned house, to their neighbors

inspection would have to be presented.

First of all, § 70 of the Saxon Building Code must be observed. In addition, the

Administrative regulation of the Saxon State Ministry of the Interior on the Saxon Building Ordinance

tion. Section 70 regulates the involvement of neighbors in detail there.

According to Section 70.2.2, it is stipulated that the neighboring participation by the building inspectorate

authority takes place, insofar as it has not already been carried out by the client. The neighbors are out

For reasons of data protection, to only provide information on the building plans that are necessary for the assessment

treatment of their concern are necessary.

The scope of the documents to be submitted can therefore only be determined on the basis of the respective individual case

be determined.

2.2.14 Disclosure of Attachment and Confiscation Orders

to third parties

Because of the dispatch of garnishment and confiscation orders by a municipality

to the tenants of his apartment building and the associated disclosure of his data

a petitioner contacted me. I commented on this process as follows:

In Germany, the garnishment and confiscation order is a measure of compulsory

enforcement. The seizure and confiscation order is issued by the responsible enforcement

enacted by the insurance authority itself. This was the treasury (city treasury). income from

rental are, provided they are not subject to seizure protection, fundamentally

restricts attachable by creditors by way of enforcement of a claim. The tenant is

here so-called third-party debtor. The garnishment and confiscation order is with the

Service on the third-party debtor effective (see Section 309 (2) of the Fiscal Code). From this

At the moment he has to observe the garnishment. For this reason, the third-party debtor, so here the tenants of the residential and commercial building, also aware of the relevant decision admit.

62

2.2

Whether the garnishment and confiscation order was issued lawfully, i.e. the applicable made claims of the municipality against the petitioner actually existed, is in the Matter not a question of data protection law, so that this was beyond my control.

2.2.15 Address of the food manufacturer

A beekeeper contacted me about disclosing his contact details on honey jars me.

According to REGULATION (EU) No. 1169/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011 on consumer information on food medium and amending Regulations (EC) No. 1924/2006 and (EC) No. 1925/2006 of the European Parliament and Council and repealing Directive 87/250/EEC of Commission, Council Directive 90/496/EEC, Commission Directive 1999/10/EC sion, Directive 2000/13/EC of the European Parliament and of the Council, the Directives 2002/67/EG and 2008/5/EG of the Commission and Regulation (EG) No. 608/2004 of the Commission, the responsibilities are regulated accordingly in Article 8, that responsible responsible for information about a food is the food business operator, under whose Name or company the food is marketed or, if this entrepreneur is not in established in the Union, the importer who introduces the food into the Union. The food business operator responsible for the information about the food guarantees in accordance with the applicable food information law and requirements of the relevant national legislation, the existence and correctness of information about the food. Art. 9 contains the list of mandatory

indicate under letter h) the name or the company and the address of the food

according to Art. 8 Para. 1.

The regulation is binding in all EU member states. A deviation from the address

It is therefore not possible to state this.

2.2.16 Passing on tenant contact data to brokers and subsequent tenants

In the area of the housing industry, the transfer of personal contact data

(telephone number, e-mail address) as part of the termination of the tenancy

to complaints.

Petitioners regularly complain about unauthorized disclosure of their data to brokers,

prospective tenants or new tenants. This illustrates the widespread among tenants

Worry they are being deprived of control over who they reveal this data to. Did-

In fact, the risk of data misuse cannot be dismissed out of hand, especially since the

E-mail address is often used for identification in various internet services. in

In response to the disclosure of the telephone number, the people concerned complained about calls

at the wrong time, for example in the early morning or late evening hours.

Telephone number and e-mail address are personal data within the meaning of Art. 4 No. 1

General Data Protection Regulation (GDPR). Their disclosure falls under the concept of processing

(Art. 4 No. 2 GDPR). A legal basis according to Art. 6 is required for their legality

Paragraph 1 GDPR.

First of all, it must be made clear that the collection, storage and use of telephone numbers

mer and the e-mail address as contact details of the tenants regularly from the purpose

of the tenancy Art. 6 Para. 1 Letter b GDPR is covered. However, this only applies

with the restriction that this data is used exclusively for the lessor's own purposes

or the property management within the framework of the implementation of the rental agreement.

Landlords and also property managers are often subject to the erroneous view that with a
The countersigned data protection declaration provides a legal basis for data transfer
gift can be created. In fact, however, they only come from them
According to the law due to the obligation to provide information according to Art. 13 DSGVO. A privacy
declaration cannot justify data processing according to Art. 6 Para. 1 DSGVO, but
otherwise only represents a measure accompanying this.
drawing on tenant side nothing. Certainly not such a consent in the sense of
Art. 6 Para. 1 Letter a DSGVO to qualify. Consent must be voluntary, for a
specific case, after sufficient information and in an unambiguous manner
will. In addition, it must be bound to one or more expressly stated purposes
and, in addition, an express reference to the objection that exists at any time
call option included.
Can the contact details be used during the tenancy, e.g. for craftsmen
and representatives of the landlord or the property management in individual cases, if necessary
justified with necessities in the tenancy agreement, the passing on of telephone numbers
mer and e-mail address to the next tenant or agent, not even for the further fulfillment of the
rental agreement is required, so the admissibility of the
Article 6 paragraph 1 letter b GDPR. What is required to fulfill the rental agreement is
to be measured against the relevant provisions of the German Civil Code (§§ 535 ff. BGB).
The comprehensive weighing of interests according to Art. 6 Para. 1 Letter f GDPR does not apply either.
According to this, the processing of personal data is only lawful if it is used to protect
the legitimate interests of the person responsible or a third party, provided that
not the interests or fundamental rights and freedoms of the data subject who
require protection of personal data prevail. However, tenants do not have to
assume that personal data held by the landlord or administrator, un-
asked to third parties with whom they themselves do not want to enter into any relationship

2.2

will. A relevant information in the course of a corresponding notification

writing does not lead to the admissibility of an intended data transfer in this respect; one

Legally effective consent requires a clear action by the data subject.

A few example cases are presented below:

After terminating her rented apartment, a tenant received an on her private mobile phone

Call a real estate agency to arrange a viewing appointment. Except-

she was informed that the apartment she (still) lived in was on several

Internet portals for subletting had been discontinued.

As the property management confirmed to me, the tenant had her phone number before the state

The previous tenancy is reported to the broker in a tenant self-assessment

disclosed to. In addition, there was written advance information about the fact that

the agent will contact her to arrange a viewing. However

a self-disclosure issued to enter into the existing tenancy is suitable

not as a justification for a data transfer based on it, because after

the principle of the storage limitation of the broker after the conclusion of the rental agreement

should have had access to the personal data of the tenant (Art. 5 para. 1 lit.

e GDPR). The purpose of the data collection was achieved, so the broker's existing

which tenant data are immediately deleted or handed over to the landlord

the must.

Apart from that, (still) tenants - apart from an express consent (Art. 6

Paragraph 1 letter a GDPR) - a transfer of your contact details for preparation purposes

of course not accept subsequent new tenancies. A data transmission

Lending to brokerage companies to coordinate viewing appointments is neither of the

Purpose of the rental agreement (Article 6 (1) (b) of the General Data Protection Regulation)

includes, nor from a balancing of interests (Article 6 (1) (f) of the General Data Protection

order) derivable. Irrespective of the lack of a legitimate interest, the Hausver-

administration can also easily arrange appointments themselves. That would be one

Intrusion into the tenant's personal rights could have been effectively avoided.

The property management finally showed me that they had a further

has prevented further use of the data. He also pointed out to her that it had been deleted

the corresponding data.

In another case, a tenant registered with a homeowners' association

me and complained about daily calls during working hours. After one from his landlord

outgoing disclosure of his telephone number to three companies, which in turn

around brokers, he was constantly on the phone to make appointments

contacted. Before submitting a petition to my authority, he had contacted the landlord

contacted in this regard. However, he had only succinctly referred to the

confirmation of delivery, which contains a written reference to the data transfer (name, telephone

number and email address) to three companies. The manager made me

against his justification in addition to the

In accordance with Art. 13 GDPR, information about data processing was provided.

Although I do not represent the legitimate interest of the landlord in a complete subletting

tion in question. A necessity to send the data to companies commissioned with the search for tenants

take it and pass it on to brokers commissioned by them, but I don't see it. The reference

on the data protection declaration also went wrong, since with this no legalization for an actual

unlawful processing of personal data can be achieved (see above).

Otherwise, this data protection declaration did not contain any general formulations

outgoing notices. She did not name any brokers or persons in charge of subletting

carried companies as (possible) recipients, nor did it contain statements on the scope

of data usage.

The inadmissible use of the tenant data was finally ended by the fact that the Ver-

tenant the company commissioned by him to delete and the waiver of a further

usage prompted.

In the third example, following an inspection appointment for the purpose of

renting, the prospective tenants still have to ask whether their previous kitchen is also in the new one

apartment fit. Therefore, they contacted the property management in order to contact the previous

to be able to contact the tenant. With the telephone number given by the administration

equipped, they contacted the tenants by telephone, which they took as an opportunity to

about complaining to my authority.

When questioned by the complainant, the property manager was not aware of any guilt.

She was unapologetic and argued that other tenants didn't either

would see bad.

In this case, too, there was no authorization for the release of the data. The tenants had to

Don't expect potential new tenants to contact you directly

would, especially since the visit came about at the instigation of the property management

was. The management should either have contacted the tenant itself and

sharing the kitchen dimensions or contacting them independently or

if necessary, have to coordinate a (further) inspection appointment.

The property management also arranged for the deletion of the name and telephone number

mer towards potential new tenants.

66

2.2

I advise property managers and affected tenants what the use of tenant data

going to make explicit and unambiguous agreements. E-mail and

However, the tenants concerned are also entitled to contact telephone contact data afterwards
limit Moreover, property management companies and landlords should, in cases of doubt or in individual cases,
with regard to disclosure to third parties or, if necessary,
obtain consent.

2.2.17 On the question of the transfer of data provision after
Census law on property management

A population census to take place every ten years was originally planned for 2021
planned in the member states of the European Union, to which Germany on the basis of the
Census Act 2021 (ZensG 2021) should participate. The actual deadline was May 16th
2021, § 1 para. 1 ZensG 2021. The purpose of this statistical survey is to determine
Development of basic economic and socio-structural knowledge related to the
Population and their housing situation in Germany. The determined population figures
which is used, among other things, in the division of constituencies or the distribution of votes
of the states in the Bundesrat. But also the financial equalization of the federal states, the calculation for
The funds and the distribution of tax funds are based on the census data obtained.
As a result of the coronavirus pandemic, however, this census was changed from 2021 to 2022.
pushed the legal basis was changed from the 2021 Census Law to the 2022 Census Law
(ZensG 2022) changed. The new reference date is now May 15, 2022, Section 1 (1) ZensG 2022.
A central component of the census is the census of buildings and dwellings, Section 9 (1).
ZensG 2022. The owners and administrators are obliged to provide information in accordance with Section 24 (1).
ZensG 2022. Administrations that do not provide (housing-related) information according to § 10 ZensG 2022
are obliged to provide information on the owners instead, § 24
Para. 2 ZensG 2022.
The census actually planned for 2021 was the cause of a complaint from an owner
mers of a larger homeowners association. This complaint was directed
the implementation of the 2021 census and a related resolution in the

assembly. With the resolution, the property management against provisions
of data protection violated, according to the complainant. The decision stipulated that the
Administrator for the additional effort to fulfill the notifications resulting from the census
payment obligations receives a flat-rate special payment and the distribution of costs according to the
number of apartments should be made. Upon inspection of the minutes of the meeting, it was found in
In fact, at first the impression that the property management wanted to settle with a majority
conclusion of the owner not only the transmission of the building-related characteristics - § 10
Para. 1 No. 1 ZensG 2021 - but also the transmission of the housing
and personal characteristics (cf. Section 10 Paragraph 1 No. 2, Paragraph 2 ZensG 2021). However, these include

also personal data within the meaning of Art. 4 No. 1 General Data Protection Regulation
(DSGVO), such as net cold rent and names of the apartment users.
In the case of an obligation imposed by majority vote on all owners to provide
Distribution of this personal data to the property management would the individual owners
In this respect, however, they also have control over the personal data relating to them
then lose if they have not agreed to this resolution. A majority decision
does not constitute consent within the meaning of Art. 6 Para. 1 Letter a GDPR. In such a
case, the persons present at the owners' meeting or the
owners who voted in favor practically over the heads of those who voted against or
absent owners away decisions in solely the respective individual
owner or his personal data matters
met. However, this is subject to the constitutional right to informational self-
against determination. This regulates the rule of the individual over the disclosure and
use of his personal data and is therefore an individual and highly personal
human fundamental right. Such a majority decision could therefore have no binding effect

develop for the individual owners.

As it finally turned out, both the text of the decision and the accompanying

Explanation only formulated in a misleading way, which irritated the complainant

had taken care of. In fact, the property management service in this regard was merely

as a voluntary, but of course not free offer to the owners

ment to take over the overall transmission of information for them. In the first

phase, the property management should ensure that the data is transmitted as part of the building

Counting takes place with the simultaneous publication of the lists of owners, in the second phase

then, if necessary, the transmission of the apartment and personal characteristics. Whether the

process designed in its second stage as order processing or on the basis of consent

tion would be supported was not certain at the end of the supervisory procedure. This one

Matter on the part of the property management also from their external data protection officer

was accompanied, I was able to refrain from further involvement by my authority. inso

far I have only made sure that the property management to avoid further

inputs or inquiries, a written clarification to all owners of the

community makes.

2.2.18 The use of email and telephone contact details at

existing business relationship

A complainant had contacted me because he believed that his

tens of the person responsible with the intention of extending the contract with him

would have been inadmissible. For his part, the complainant had no express

consent given for this.

68

2.2

As the company plausibly explained to me in its statement, the call was made

in causal connection with the Customer's visit to the Controller's store and

has also made changes in terms of content as part of the contract initiation negotiations that he himself initiated lungs moved. In order to make a promotional call within the meaning of § 7 of the law against unfair betting competition (UWG) is therefore not involved in this respect. Under this condition, it is necessary in accordance with Art. 6 Para. 1 Sentence 1 Letter b General Data Protection Regulation for the relevant data Data processing also requires no (additional) consent from the data subject.

It goes without saying that the customer is willing to refrain from certain communication channels noted and (except in emergencies) respected.

2.2.19 Eligibility for Business-to-Business Marketing

In the case of so-called "business-to-business" advertising, any personal reference must be taken into account. ten. Appropriate documentation of the advertising mailing processes must also be implemented Allows data subjects to request information.

The ban on cold calling according to the law against unfair competition applies in absolute True, this is only true for the so-called “business-to-consumer” area. has been misjudged in In a case presented to me, however, the fact that company e-mail addresses contain a personal reference, insofar as it contains name components or - if - equally less burdensome - refer to partnerships. I am responsible literal reference to the legal situation. Associated with this was the instruction that data (temporarily) may not be deleted if requests for information are pending.

2.2.20 Delimitation of non-promotional customer information from Promotional speeches and reminder emails – “nudge emails”

In a complaints procedure, a portal operator has, in addition to the (so far inconspicuous) Newsletter creates non-deselectable reminder emails (“nudgemails”) which – according to the digital Paperwork, which was also made known to the person concerned at the time the contract was concluded - were "automated" and "could not be switched off" without the user to delete account. An advertising contradiction according to Art. 21 Para. 2 General Data Protection Regulation (DSGVO) by the person concerned was rejected with precisely this reasoning,

so that he was faced with the decision of either accepting the broadcasts

or cancel the account and contacted my authority.

When assessing such reminder e-mails, the first question that arises is whether or not

but advertising in the legal sense is to be disseminated. advertising could be affirmed

if a sales target in the direction of a chargeable alternative or additional product

would have stood. However, the process offered no evidence of this.

69

Chapter 2 Principles of data processing

The requirements according to the law against unfair competition for electronic

I therefore regarded the exercise as objectively not fulfilled. The question remained, however, whether

Legal basis according to Art. 6 GDPR existed. With the reminder email, dem

Customers informed that longer inactive profiles would be deactivated. With the statement of

responsible, he had specified this with the expiry of nine months. This leads to

Discontinuation of all e-mail contact, even if the contractual relationship

was not terminated by the user.

I consider the memory

E-mail contractually and measured against the expectations of the contractor as usual and

reasonable. In my opinion, however, the following conditions must be met

be: The shipments have a customer-related, contractually relevant information

content, in particular with regard to a warning of the consequences of further

re inactivity. Technically, no endless routine may be set up and the time

status of the reminder e-mails must be based on the purpose and presumed interest

ented to be appropriate.

Under these (narrow) conditions, I have the "Nudgemail" as a permissible form of

standing customer communication considered.

2.2.21

Claiming a Minor by a

collection service provider

In one case, a petitioner or his/her legal guardian led against a

Claims by a collection agency indicate that the person concerned is an alleged

Customer or debtor is a minor and therefore – according to the applicable Austrian

Reich law - is not legally competent. This assertion was supported by a corresponding

relevant official excerpt from the population register of the home country. The subject of

The alleged contract was the use of an erotic online dating site. man

In any case, there was no valid contract between the debt collection client and the person concerned when the payment was

made.

(cf. Section 110 of the Civil Code or Section 170 (3) of the General Civil

ugly law book). The person concerned was based in Austria, hence the contract

to be assessed according to Austrian civil law.

The debt collection company based in Saxony that was questioned stated irrefutably that

Corresponding direct response from the person concerned or their parenting authority

not to have received it. That was only said in the context of subsequent discussions

company finally agrees to enter the relevant data now in terms of time and

restricted to use, insofar as within the framework of permissible investigations into alleged fraud

actions required by using foreign identities, and then promptly

Clear.

70

2.2

The data protection supervisory procedure was completed without a warning

because intent by the debt collection company of the person responsible could not be proven

and the data protection violation has been resolved cooperatively. However, the company was

pointed out that the specific case had gaps in the age verification of the commissioned

existing company. Accordingly, the collection agency with regard to these

increased duty of care to check the plausibility of the

hung transferred claims and the right to data processing within the framework of

Debt collection (cf. detailed activity report 2019, 2.2.18, page 54 ff.).

2.2.22 Correction to “Requirements for websites of public

Place"

In the activity report 2019, 2.2.1, page 31 ff. I explained under what conditions

Gen public bodies User data for visitor statistics and similar purposes data protection

can process compliantly. In essence, it was about the interpretation of the legal basis

of the legitimate Art. 6 Para. 1 Letter f General Data Protection Regulation (GDPR), which for

applies to private bodies and is not applicable to public bodies. Therefore I have the appli-

6 Para. 1 Letter e GDPR in an analogous interpretation is recommended. The result was

It is thus possible for public authorities to also use cookies to recognize visitors

set, if doing so the data processing is in the exclusive sovereignty of the public body

is operated.

The Federal Court of Justice (BGH) ruled on May 28, 2020 in the proceedings of the Federal

Association of Consumer Centers (VZBV) against the address dealers and lottery

operator active Planet49 GmbH fundamental decisions in connection with the

data protection assessment of the use of cookies on websites. The GE-

Firstly, § 15 Para. 3 of the Telemedia Act (TMG) conforms to the guidelines

Specifications of Art. 5 Para. 3 ePrivacy Directive and determined that service providers

Cookies to create usage profiles for advertising purposes and marketing only with consent

allowed to use the user. Secondly, with this content § 15 paragraph 3 TMG in addition

of the GDPR applicable since May 25, 2018. Third, set a preset

Checkbox in a cookie window on a website does not provide an effective privacy

legal consent. With this third statement, the BGH unsurprisingly followed the

preliminary ruling from the European Court of Justice obtained in the referral procedure. This
had already ruled on October 1, 2019 that there was no effective consent if
the storage of information or access to information already in the terminal device
of the user of a website are stored by means of cookies through a preset
checkbox is allowed that the user can deselect to refuse their consent
got to.

This makes it clear that informed consent is required for cookies that are not technically required.
is required. Public authorities should therefore check their websites for compliance with the
check applicable regulations. I still get a lot of complaints
by citizens who need to check websites of public bodies and identify violations.
Not only the main website of the public body is to be considered, but also the
of the institutions of the public body that operate their own websites, for example
libraries and baths.
In general, I advise public bodies against storing data that requires consent on websites.
to carry out processing. The reasons are that the voluntariness of the
given declaration of intent is to be questioned, since a website of a public body in
is generally perceived as an authority and therefore does not require consent on the
can be assumed. In addition, Art. 8 GDPR must be observed and
appropriate mechanisms to ensure consent by the holder of parental authority
to establish a response for a child. Since public authorities are pursuing the claim
to be available for all citizens, this aspect must be observed and in the
Practice with numerous problems, such as suitable proof and a technically
plex implementation, fraught.
If consent is nevertheless to be obtained, this has all the claims to the

sufficient information. With regard to data processing, there is complete transparency

to produce and technically ensure that the data processing is actually only

after consent or not at all in the absence of consent. There in the

In practice, errors often occur, I would like to refer separately to my publication on

Indicate the use of consent layers on websites, available at datenschutz.sachsen.de.

A web analysis is still possible, which does not require cookies and otherwise

adheres to the requirements formulated in the 2019 activity report.

For private bodies it should be added that even before the decision of the Federal Court of Justice in the case of an application

the guidance of the supervisory authorities for providers of telemedia (OH Telemedien,

available at datenschutzkonferenz-online.de) as a result, most of the

set tracking and marketing services due to the transmission problem to third parties

and their processing of usage data for their own purposes requires informed consent

require.

2.2.23 Video surveillance causes neighborhood disputes

Almost regularly, I receive complaints about video surveillance (also)

neighboring plots of land where the property owners mutually share the video

accuse them of monitoring their property. In the majority of cases, the vi-

deodorant surveillance in the neighborhood is the result of a broken neighborhood relationship

opinion, which is often presented to me more or less extensively by those involved

is placed. It is usually about civil law issues that affect the jurisdiction

not affect my authority. In addition, a submission often serves as a

Valve to complain about other incidents or to the neighbor through "official channels"

to cause difficulties.

A property owner noticed one during tree felling work on his property

Video camera located on the neighboring property with alignment to his property.

He took this discovery as an opportunity to ask the city administration for the complete removal

or to demand permanent dismantling of the camera, from where he could contact my authorities

was reported. After questioning the camera operator, he in turn accused neighbors

the video surveillance of the public road in front of it, which he had to use,

to get to his property. His suspicions even went so far that after

barn believed capable of creating sound recordings, since the latter's verbal comments were immediately "in

the deed would implement. Background for the massive presence of surveillance cameras in

A series of burglaries were evident around the property owners.

How in the course of my investigations the "return coach" of the (initially) responsible

shown, two of the four cameras were also aimed at parts of the public traffic area

directs. All cameras were not in operation due to technical problems. also saw

the responsible person no need at that time on his property

active construction companies to monitor. However, a restart was after completion

of the property work aimed at. The person responsible believed himself to be in agreement with

the data protection law.

Property owners often do not realize that they are also outside of their property

areas located at least marginally, possibly because they are only

have an eye for your own property. Furthermore, I can only assume that they

also with the technical possibilities that a video surveillance system offers - with

for example to carry out blackening - not always sufficiently familiar with it.

In principle, there are no objections to video surveillance of one's own property

To ponder. In any case, in the case of plots of land used solely for one's own residential purposes

the budget exception of Art. 2 Para. 2 Letter c General Data Protection Regulation (GDPR)

covered with the result that the data protection regulations do not apply

come. However, if the detection area exceeds the sphere of your own property,

the admissibility under data protection law is based on the provisions set out in Art. 6 Para. 1 GDPR
the permitted circumstances listed below. With video surveillance, re-
only the comprehensive weighing of interests of Art. 6 Para.
costume.
73
Chapter 2 Principles of data processing
Burglary protection is recognized by case law as a legitimate interest.
However, for the monitoring of public transport running in front of the property, there is no
traffic areas and also neighboring properties at the need to reach the
pursued purposes. In addition, the interests of those on public areas outweigh
holding and moving people regularly the monitoring interest of the camera
operator. Therefore, video surveillance has always been on your own property
to restrict.
Those responsible occasionally also state that the video surveillance in
was successful in talking to the neighbors and they even expressed the wish
also to monitor their properties. As far as monitoring only on private
I can see in data-
from a legal point of view there is no reason to intervene. However, the one
willing neighbor must be aware that, depending on the design of the vi-
deo monitoring and the conditions on site the monitoring neighbor numerous
views into his private area. In addition, there is always a risk that
an initially good neighborly relationship turns into its opposite.
Again and again responsible camera operators confront me with the fact that they
received a tip or a recommendation from the police to install cameras
would hold. Under no circumstances can a statement to that effect by a police officer be so
be interpreted that the camera operator can also carry out surveillance practically at will

public traffic areas. I suspect that such general police

The information given by the property owner is often "reinterpreted" in this way.

Irrespective of this, of course, this cannot be used to legitimize a

carry out video surveillance that is not permitted under the General Protection Regulation, regardless of

that only my authority is responsible for the data protection assessment in such cases

and accordingly police statements have no binding effect on me.

Also compare the articles under 2.2.24 and 2.2.25.

2.2.24 Videography: The valuable sculpture in the front yard

Especially when the neighborly conditions are not in the best of shape,

the installation and commissioning of a video camera usually still requires an existing

confrontation. In the course of which the persons concerned promise themselves of my

I often hear a remedy (cf. 2.2.3). It was the same in one case in which the video surveillance

of a front yard and the adjoining public road. Of the

Responsible property owner had in the course of redesigning his front yard

removed the vegetation there and installed an allegedly valuable stone figure in its place.

which he intends to protect with video surveillance attached to the wall of the house.

sighted.

The screenshots presented to me by the camera operator showed that the fear of

neighbors was justified. With the camera attached to the wall of the house, actually

parts of the road along the property, including the pedestrian walkway, are also recorded. the

The entire monitored area, the front yard and the adjoining sidewalk, was shown as a live image

can be accessed on the property owner's smartphone at any time and from any location. One

However, the recording was only made when there was movement in a defined area of the

triggered around the stone figure. Also only from this room was ultimately after

triggering a video and sound recording.

I have assessed the operation of the video camera as inadmissible insofar as the recording

range of live monitoring also outside of the private operator's property.

lying areas had expanded. In this respect, the owner could not rely on the

exception of Art. 2 Para. 2 Letter c of the General Data Protection Regulation (GDPR).

The sole assessment standard was the comprehensive weighing of interests according to Art. 6 Para. 1

Letter f GDPR.

When monitoring areas that go beyond your own property, the approval fails

negligence already in the absence of a legitimate interest in monitoring. to

If video surveillance is to take place, the requirement of necessity must also be observed

the. According to this, video surveillance must be suitable for achieving the intended purpose

and there must be no milder means by which the end can be achieved to the same extent

can reach. Finally, the surveillance measure must also be proportionate.

The camera operator initially stated that the camera could not be rotated any further. To the

must be countered that a technical situation for which a camera operator is responsible

cal nature within the meaning of Art. 6 Para. 1 Letter f GDPR legitimate observation

performance requirement and consequently a justification of the encroachment on the fundamental right to domestic

formal self-determination of the persons concerned (passers-by, road users)

can be deduced. It would also fundamentally contradict the data protection requirement

principle if the need for data processing is due solely to the fact

det would be that the responsible person has purchased a technical system that is not

can be operated, although the fundamental rights encroachment on another system or a (with

cost-related) changing the mounting method or the camera location easily

could have been avoided.

75

Chapter 2 Principles of data processing

The operator was only able to name one single case of damage, that of the blasting of his
mailbox at the turn of the year. For me, however, there was no
to establish a connection to the stone sculpture (which did not yet exist at the time). Even
This incident does not allow the conclusion that there is a particular risk situation. In
In view of the stone figure to be protected, surveillance was restricted to
The private property of the camera operator is perfectly adequate. Just the presence
a video camera - whose detection range is exclusively on your own property
extends – usually already has a sufficiently large deterrent effect on people
who seek to impair property existing on private property. To-
the deterrent effect was further enhanced by the information sign attached to the courtyard gate
strengthened.
After I had pointed this out to the responsible person, he was suddenly able to
but make a realignment of the camera, so that it is now only your own
Front yard captured. Considering that only a motion-triggered vi-
deo recording also a (simultaneous) sound recording was made and just outdoors by the
mostly existing ambient noises (street noise, wind, birdsong) as well as
the distance to the speaker does not rule out the usability of corresponding recordings
I saw no data protection concerns in this regard.

2.2.25 doorbell cameras as digital door viewers

In a curious case, I received an entry for a digital door viewer in a larger
outer housing unit. The responsible person had the conventional door
spion replaced by a digital door viewer that is clearly visible from the outside. The Complainant-
in it, which lived on a floor above and the apartment of the responsible person and
also had to regularly pass through the digital door viewer installed there, saw her
privacy rights violated. She had previously applied for an "immediate disposal."
contacted the responsible property management, but obviously without success. That's why it was enough

She lodged a corresponding complaint with my authority and supported it with the

afraid that she will be constantly filmed.

In the end, however, the situation was to be completely different from what the house

resident had described. As it turned out after questioning the person responsible,

she had withheld essential information from me. It turned out that the roles actually

were actually swapped and the apartment owner as the alleged "perpetrator" actually

real "victims". Because the complainant had previously had the digital door viewer several times

taped up with newspaper and tape. Nor did she shy away from using snow

spray back, which ultimately led to irreparable damage to the door viewer, so that

this had to be replaced by the apartment owner.

76

2.2

After the camera integrated in the (original) digital door viewer only at

Pressing the bell that is also integrated there triggers an image recording (single image),

the only thing left to the owner of the apartment each time was to determine the incident and to remove

mitigation of the consequences of damage. However, he had no knowledge of who caused it. However

the resident of the house was apparently against one of the actions attributable to her

slipped off the peephole and inadvertently touched the integrated doorbell

pressed, which triggered an image recording. Although at this point they

had already sprayed the camera lens to such an extent that no usable image was recorded

had been taken, the apartment owner could at least determine the "time of the crime" based on the recording

determine. Therefore, on the following day, at the same time, he stood behind the apartment

door and was able to catch the petitioner in the act. However, this was inconsistent

and put the meaning of their act into perspective.

Even if this makes it clear that the submissions received by my authority - in particular

video surveillance – disagreements that often go back further

and even (verbal) arguments are the basis, my data protection

Legal assessment strictly based on the legal requirements. On the legal situation before the data protection

Basic Regulation, I already discussed the admissibility of digital door viewers in my 7th day

Activity report for data protection in the non-public area (04/2013 to 03/2015), 8.1.14,

Page 45 f. The criteria established there also have, taking into account the

General Data Protection Regulation inventory. Accordingly, there are against the use of digital

Door viewers have no objections if the following requirements are met:

•

•

•

•

•

The camera may only be activated when the doorbell rings

be able.

The camera may only be in the immediate entrance area (close-up area) in front of the door

capture.

The camera must be deactivated again automatically after a short time.

The live image must not be transmitted over the Internet.

It must not be possible to record the images.

If these requirements are met, I have against the use of digital door viewers - also

like from doorbell cameras – no objections. After in the present case through the newly

managed door viewer camera no more photos were saved, the door viewer only

triggered after manual operation of the bell integrated in it and the displayed image of the

The area in front of the door was only visible for ten seconds, I saw no evidence of

a data breach. Finally, I also told the complainant that

divided.

2.2.26 Video surveillance of the entrance area of a block of flats -

exceptions prove the rule

The starting point of my referral was the complaint of a person on the ground floor of a

resident commercial tenant. This was - after unauthorized access

had manually taken the automatic door in the entrance area out of operation

- been contacted by the landlord by telephone with the message that he was to be considered a

cause of the door manipulations using the video surveillance systems covering this area

system have been able to determine. The complainant explained to me that nothing about

of such video surveillance, in particular no relevant information

to have noticed signs and asked for an examination of the admissibility of the operation of the

video surveillance system. He looked around and in the overall very large

Residential area comparable video surveillance systems also in three other, from

high-rise buildings that are identical in design.

The admissibility of video surveillance in common areas of apartment buildings

sern is based on Art. 6 Para. 1 Letter f General Data Protection Regulation (GDPR)

to judge. According to this, video surveillance is permitted if the associated

Processing of personal data to protect the legitimate interests of the responsible

literal or a third party is required, unless the interests or fundamental rights and

Fundamental freedoms of the data subject, which require the protection of personal data,

prevail, especially when the data subject is a child.

This provision therefore initially requires that the landlord with the video surveillance

pursues legitimate interests and that the video surveillance is suitable for safeguarding them,

is necessary and insofar also proportionate. In addition, one may also take part in it

Subsequent weighing of interests not in favor of the persons concerned, so here in

primarily the tenants and their visitors.

The landlord has told me that the relevant video surveillance systems in the

four high-rise buildings to prevent vandalism on the one hand and also to educate and

On the other hand, they served as safeguards in the event of damage and criminal offences. The thus pursued

Objectives primarily of property protection but also the protection of tenants were without

Recognize more as legitimate interests. With an evaluation submitted to me

Insurance claims that have occurred in recent years have also been proven

it is not just an abstract danger situation, but that within the residential

area in particular the high-rise buildings that are the subject of the proceedings by Van

dalism damage were affected.

78

2.2

Video surveillance is suitable for achieving these goals, or at least supporting them,

because it works on the one hand - as far as a corresponding labeling or

recognizability is given - preventively, and on the other hand it enables - a sufficient

Assuming the quality of the recordings - undoubtedly a preservation of evidence and thus one

Contribution to the clarification of facts and identification of perpetrators. The required

cannot be called into question, because the additional measures taken, such as the

step control (automatic doors with access control system) as well as the nightly use of a

Security services in the residential area have obviously not proved to be sufficient,

to significantly reduce the number of claims. It was also necessary to consider

that some of the damage found can even be traced back to individual residents

was. In this respect, the tenants in the predominantly one-room apartments

high-rise buildings had a rather unfavorable social structure and thus an above-average one

potential for conflict. Milder measures that have the same effect as video surveillance

men were not recognizable. The video surveillance only recorded the particularly dangerous

the entrance areas and the elevators. The floors closer to the apartments

Corridors and the stairwell were not monitored. Incidentally, the video

actually monitoring these four skyscrapers; other buildings were not

wakes up

With regard to the necessary balancing of interests, the following was determined:

As a rule, with video surveillance of the immediate living environment, the

legitimate interests of the persons concerned, although the interest of the operators of vi-

deo surveillance systems especially if the cameras also provide regular access

(here the entrance area and the elevators) to the apartments, as the tenants

impossible to escape from such video surveillance. In any case, you must

cross the entrance area and are mostly dependent on using the elevator

senior The latter applies in any case to the numerous older and often health-impaired

residents of the high-rise buildings for whom alternative use of the stairwell is not an option

consideration. Already the possibility that the landlord can check at any time which

cher tenants, when, which visit receives, comes or goes, sets the apartment tenants

under considerable pressure to monitor and adapt. In an analogous way, albeit

weakened, this also applies to the few commercial tenants.

Nevertheless, in the individual case to be considered here, I have come to the conclusion that

the monitoring interest described by the landlord these data subjects worthy of protection

interests outweigh for once. On the one hand, the decisive factors were the

very high damage amounts, which have been in the six-figure range for the last six years;

on the other hand, it had to be taken into account that, in particular, functioning elevators for

the - to a considerable extent - older tenants of almost essential importance

are. In addition, the tenants are interested in a functioning letterbox system

as a mandatory prerequisite for the proper delivery of postal items. the

Surveillance therefore served to protect the landlord's property and was also part of the
interest of the tenants themselves. In addition, the entrance area is usually quickly
and the stay in the elevator is only for a short period of time. It found neither
constant monitoring via live monitoring nor a routine evaluation without
speaking reason instead. According to the submitted service instructions, access to the recording
Subscriptions only permitted for specific reasons. It was different from smaller residential properties
the majority of the tenants are not personally known to the landlord and therefore
evaluation (viewing the recordings to identify the perpetrator) not without further
res identifiable, so remained largely anonymous to him in this context.
The encroachment on the personal rights of the tenants and their visitors was therefore comparatively
way low; the threatening (health) disadvantages were much more serious
especially for the residents of the upper floors in the case of non-operational elevators. the
Video surveillance of the entrance area also served to implement a functional one
Access control (automatic doors with access authorization check) and more functional
mailbox systems. According to the statements of the landlord, these areas were always
again the target of wanton damage to property. In this regard, too, there was a considerable
interests of the (honest) tenants that the security of the property has a minimum level of security
is guaranteed.
As a result, I have video surveillance in the four high-rise buildings as permissible and therefore
lawfully assessed, but would like to expressly emphasize at this point that this is
dealt with an individual decision in a special exceptional case. the
The complainant did not agree with this assessment and, according to Art. 78 para.
1 DSGVO filed a lawsuit in this regard with the Dresden Administrative Court. On the
I will report the outcome of this lawsuit in due course.
With regard to the lack of sufficient information, which the complainant also addressed

point to the video surveillance, I have indeed had to identify corresponding deficiencies

senior While the landlord claimed that from the outset the video surveillance was

speaking stickers, the complainant informed me that

that camera pictograms were only attached for the first time after his complaint

the be. The truth will probably lie somewhere in between, in particular it can't

excluded that tenants or third parties have removed the pictograms. Clear

was, however, that new GDPR-related, but still deficient at the first attempt

signs had actually only been attached after the complainant had

deführer addressed both to the landlord and to me accordingly

would have.

Ultimately, however, a quick remedy of the defect was taken care of in this regard.

For this purpose, both the contents of the upstream information signs and the complete data

data protection information and the places where it is attached or deposited with me

80

2.2

been coordinated accordingly, so that since then a complete GDPR-compliant

it can be assumed that the video surveillance in these four high-rise buildings

the can. For the required labeling see Activity Report 2019, 3.1.1, page 71 ff.

2.2.27 Video surveillance in a dental practice

Two submissions reached me in connection with video surveillance in one

group dental practice. A total of four video cameras were in use there

both the entrance and reception area, especially the workplaces in the

Registration employees, as well as the corridors and thus the entrances to the consulting rooms

captured. The images from the cameras could be accessed if the corresponding access data was known

can be called up by the dentists from any Internet PC. The practice operator

stated that the video surveillance system serves to protect property and security

security of the staff and led to various burglaries (prescriptions, cash and other
medical device) and burglary attempts throughout the house. In addition, the
responsible also cases in which during ongoing operation of the practice suddenly strangers in
appeared in the consulting rooms.
For the data protection assessment of the admissibility of video surveillance was between
to differentiate between the opening and closing times of the practice. After being outside the
practice times, no people were allowed to stay there, there was only a data
property rights assessment of camera operation during opening hours.
In its judgment of March 27, 2019 - 6 C 2/18 - the Federal Administrative Court
dealing with the admissibility of video surveillance in a dental practice. That is
was the decision made before the introduction of the General Data Protection Regulation (GDPR)
applicable legal situation, but the Federal Administrative Court has
also respects the basic data protection regulations already applicable at the time of the decision
regulation and an admissibility assessment according to the from May 25, 2018
applicable data protection regulations.
With the (implicit) consent of the patient simply by entering the dental
xis and the associated knowledge of the video surveillance to be assumed
The practice rooms can be entered using the information sign attached to the entrance door
In any case, this does not justify the operation of the video cameras (Article 6 (1) (a) GDPR). This
also because the legal information obligations are independent of the data protection
legal admissibility of video surveillance and one that is illegal per se
Processing of personal data cannot help to make it permissible.
81
Chapter 2 Principles of data processing
Consequently, the data protection assessment based on Art. 6 Para. 1 Letter f
GDPR. This provision specifically regulates that the processing of personal

Generic data (video surveillance) is only permitted if it is used to protect the legitimate
best interests of the person responsible or a third party, unless the interests
sen or fundamental rights and freedoms of the data subject, which protect personal
related data require prevail, especially when it comes to the data subject
person is a child. These admissibility requirements were in the specific case
however not fulfilled.
On the one hand, there was already a lack of a legitimate observation
interest of the doctor. Although the protection of property and employees had preventive
cke, which were also to be recognized as justified. The CCTV was because of her
insofar undisputed preventive effect as well as the existing recording possibility
also suitable to achieve some of the stated purposes, i.e. protection against burglary and thieves
steel attempts and to make a contribution to clarification through the recordings
ten. However, such incidents during practice hours are unlikely
be lich. On the other hand, the principle of necessity was violated. There were a row
milder, but nevertheless equally effective, means of achieving the desired
the intended purpose, for example the permanent presence of the staff
the reception, staggered breaks, installation of an electric door opener combined with a
Doorbell camera, lockable cash box to be carried by the staff, safe
Storage places for prescriptions, medical equipment and so on.
In addition, the video observation also encountered the majority of things worthy of protection
interests of the affected patients. They are looking for a practice because of health issues
problems, which also manifests itself in their demeanor, occasionally even in their appearance
reflects. As a result, they have an interest in protecting their behavior
not observed or even recorded by video cameras during the stay in the practice
as well as subsequently for an indefinite period of time - from the patient's point of view - without
that they control the further use and deletion of the video recordings or

can influence. The interest of those affected weighs all the more heavily as the patients for the

purely preventive monitoring have given no cause. one at

dental practices

respectively

There is a risk of damage that stands out from the general abstract risk of life

objective view does not. (Dental) medical practices are also not areas for which a

there is actually an increased risk potential (such as with banks). burglaries or even

Attacks are a minor danger, especially since countermeasures can also be taken by means of

other measures that do not affect the interests of those affected that are worthy of protection

seize

at least none existed

clues. The balancing of interests to be carried out in the last test step also went well

therefore in favor of the patients.

to let. For a specific risk situation

special security

existing

maybe

82

2.2

For the video transmission aimed at patients or persons unfamiliar with the

monitoring at the same time associated employee monitoring, the admissibility of which is

ultimately would have been assessed according to Section 26 of the Federal Data Protection Act, there were also

no justification. Against the background that the inadmissibility of video surveillance

6 Para. 1 GDPR, this was no longer relevant.

As a result, video surveillance in the practice rooms was only outside of practice hours

allowed. Those responsible have followed my assessment and have the video surveillance

security system is now set in such a way that the cameras only work when the alarm system is switched on

are activated.

2.2.28 video camera in Thai massage studio

Imagine being a regular customer at a Thai massage parlor and noticing

when leaving the studio, suddenly an inside above the entrance door to the commercial

oriented camera. A visitor to the studio addressed this issue

my authority and asked for a review.

I then got my own impression of the local conditions.

According to my findings was actually inside on a shelf above the entrance

door hides a small video camera next to a flower arrangement. The massage studio

had shop windows that were easy to see from the outside without privacy screens and one that was unlocked

Entrance. A reference to video surveillance was not appropriate.

The owner was able to place the saved videos and a live image from the camera

hungwise on your smartphone at any time. Even if at check-

point the camera was not in operation due to technical problems, I was able to use the

of video recordings on the owner's smartphone an overview of the recording

the camera. This ranged from the entrance area to the reception

and the waiting area. Even some massage tables could be seen in the video; pi-

oddly enough, in the sequence shown to me, a scantily clad gentleman even walked through it

Picture. When asked, however, the owner stated that it was her son-in-law

acted.

From the permissions of Art. 6 Para. 1 General Data Protection Regulation (GDPR)

only letter f came into consideration here. According to this regulation is a video surveillance

permissible, insofar as the processing is to safeguard the legitimate interests of the person responsible

chen or a third party is required, unless the interests or fundamental rights and

Fundamental freedoms of the data subject, which require the protection of personal data,

predominate.

83

Chapter 2 Principles of data processing

The protection of the employees was named as a monitoring interest, since these

are occasionally in the studio until 9 p.m. and it is always closed, especially in the evening hours

Harassment in the form of verbal comments or knocking on the front door

come In principle, this resulted in a legitimate interest in monitoring, however

lacked the necessary necessity.

In my opinion, the video surveillance was therefore unsuitable for

contribute to ensuring that harassment or even assaults do not occur, as it is one

There was no reference to the video surveillance, especially since the camera was not visible to unauthorized persons.

was acceptable. The external marking of video surveillance would already be sufficient

been in order to achieve a corresponding deterrent effect. In addition, the

Owner by locking the front door or attaching a privacy screen in the

Shop windows and the access door can take more effective action, the uninvited

Guests could have kept away. At the same time, this would have a far less severe intrusion into

the rights of the visitors - as well as the employees - means. Ultimately I would have too

had no objections if only a small, spatially clearly delimited area between

between the entrance door and the reception desk would have been video-monitored, especially since the

The female employees only stand behind the counter for a short time during the checkout process

hold the reception desk.

The owner of the studio finally decided to remove the camera completely.

to.

2.2.29 Video surveillance of employee areas at a truck stop

A total of 39 video cameras were operated in a rest area, which, in addition to the tank field,

Truck parking spaces as well as entry and exit also almost all of the

Shop located on the premises (customer area and cash registers with entrances and exits as well as the counting space) included. A total of ten cameras were installed in the shop itself, of which again four were aimed directly at the checkout area. This area was open plan and not separated from the rest of the shop by a continuous counter. At the entrance of the shop were signs pointing to video surveillance and additional pictogram attached. Only the checkout area and the cameras capturing it were the subject of an (employee) complaint.

The employees working behind the counter were recorded simultaneously by four cameras, which lich and were positioned on the rear wall of the room. The cameras were set up that they completely covered the workstations located behind the counter. those who work there As a result, employees were exposed to constant pressure to be monitored practically could not escape.

84

2.2

From the permissions of Art. 6 Para. 1 General Data Protection Regulation (GDPR) only letter f came into consideration here. According to this regulation is a video surveillance permissible as a means for the fulfillment of own business purposes, insofar as the processing for safeguarding the legitimate interests of the person responsible or a third party, so far not the interests or fundamental rights and freedoms of the data subject who require the protection of personal data, especially when it the data subject is a child.

The protection of the employees as well as the Prevention and investigation of criminal acts (burglary, vandalism, tank thieves stole, robbery and fraud). There would be an average of five each month Offenses in the parking lot also account for about the same number of cases of fuel fraud. fuel fraudster When confronted with their crime, they regularly stated that they had already paid.

In addition, the commercial area in which the truck stop is located is a well-known crime activity hotspot. In principle, on the basis of these incidents and circumstances, a legitimate interest in monitoring cannot be denied. There is no question that petrol station operators and employees are at increased risk of becoming victims of crime (particularly robberies). will.

For the extensive video surveillance of the entire work area behind the counter was missing but in the present case it is necessary. The necessity is determined in terms of a Proportionality test according to the characteristics of suitability, necessity and measuredness of a measure. Although there is a general principle at cash registers increased risk of robbery. For the intended purpose, in particular the proof of a fuel fraud, it would have been sufficient if only the two on the cash registers located at the sales counter and the area in front of the sales counter would be monitored only insofar was the necessity of video surveillance in view of the monitoring given for the purpose of The employees would then have a retreat area available tion in which they could pursue their tasks without constantly being in the field of view of the moving cameras. Your interests worthy of protection could thus be sufficiently protected be taken into account.

For a targeted monitoring of the employees, there was also a lack of the Requirements of Section 26 of the Federal Data Protection Act. The video monitoring for the investigation of criminal offenses by employees. Such suspicions but the service station operator did not just present it - according to evidence, it was about him stated purposes instead of the protection of its employees and possible criminal offenses other people, such as customers.

As a result, the operation of the video cameras in the counter area was largely inadequate. casual. In this respect, there was already a lack of the necessity of recording in order to achieve the pursued purposes. I have therefore given up the operator, the entire area behind

the counter with the exception of the immediate vicinity of the tills from the registration areas

the cameras. In the event of a fuel fraud, the otherwise incomplete

loose monitoring in the shop and the actual checkout area,

who entered the shop and whether a payment transaction took place. Even if the identification

of a person due to the mask requirement imposed to protect against the coronavirus pandemic

is made more difficult, sufficient personal characteristics remain for identification

enough.

The operator complied with my demands and provided the necessary blanking

taken. He informed his employees by means of a notice on the bulletin board

the scope of the video surveillance, in particular the specific detection areas.

2.2.30 Dash Cams and Helmet Cams

With dash cams and helmet cameras from (motorcyclists and cyclists) I'm regularly in the

dealing with the processing of reports of administrative offenses (cf. 6.4). at low

However, in the event of serious violations or problems with the verification, these procedures

placed and transferred to the supervisory area.

The following must be carried out for the legal assessment of the admissibility of dashcam operation:

The only possible way to operate a dashcam as a form of video surveillance

The relevant admissibility provision is Article 6 (1) (f) of the General Data Protection Regulation

(GDPR). This provision specifically regulates that the processing, i.e. the operation of a

Dashcam including the storage of video recordings is only permitted if

they are required to protect the legitimate interests of the person responsible or a third party

is legal, unless the interests or fundamental rights and freedoms of the persons concerned

other, which require the protection of personal data, prevail, especially when

if the data subject is a child.

First of all, it must be checked whether the scope of application of the General Data Protection Regulation
net is. According to Art. 2 Para. 1 GDPR, the regulation applies to the fully or partially automated
processing of personal data and for the non-automated processing of personal
personal data stored or intended to be stored in a file system
len.
The recordings made by means of a dashcam contain personal data in the sense
of Art. 4 No. 1 GDPR, because video recordings of people undoubtedly constitute information
such as physique, driving behavior, whereabouts, vehicles used, clothing
information, statements about these natural persons. These persons are also identifiable
attractive, either through their looks (faces) or through the vehicles they use
86
2.2
(e.g. license plates, advertising or company inscriptions), via (with activated micro-
fon) their voice, the content of the conversation or about the professional or private environment of the
dashcam operator. With a dashcam, personal data of other traffic
participants processed. According to Art. 4 No. 2 GDPR, processing is possible with or without help
process carried out by automated processes or any such series of processes in combination
related to personal data such as collecting, recording, or storing
tion. The video recordings contained on the storage medium of a dashcam are
the result of such collection and storage. The operation of a dashcam essentially
particular also an automated processing of personal data (cf. Euro-
European Court of Justice, judgment of December 11, 2014, C-212/13, headline 2, juris).
In addition, a dashcam operator acts when he monitors the public traffic space,
regularly not exclusively for personal or family activities, i.e. the
2 Para. 2 Letter c GDPR (private budget) regularly applies at this point.
not if the aim is to use a dash cam, for various purposes

(especially in connection with traffic accidents) to secure evidence. Also for

The following also applies to call recordings made at the same time as the dashcam: if over

phone calls made using the hands-free system or calls made in the vehicle are recorded

net, with the exception of conversations with family members, this is

undoubtedly no longer to be assigned to the personal or family area.

Something else may possibly be used by cyclists or motorcyclists

Action cams (mostly helmet cameras) apply. As far as the cameras in these cases recognizable with

the goal of the documentation of a joint venture (motorcycle trip

or bike tour) and/or a particularly scenic route

and the persons recorded in the foreground are recognizable from the recordings

participate, I believe that the budgetary privilege will be successful

and can also extend this here to friends and acquaintances.

Dash cam users who use their camera regularly, i.e., cannot refer to this

without such a special occasion - that could also be the case with motor vehicles, for example

be a wedding parade – use them on their daily trips.

Once the applicability of the General Data Protection Regulation has been clarified, dashcam operation

be measured against the provision of Art. 6 Para. 1 Letter f GDPR mentioned at the beginning.

Insofar as the person responsible protects and protects his property with the operation of the dashcam

wants to secure wisely, the legitimate interests of the uninvolved, traffic-

fair behaving passers-by and vehicle drivers, not without cause and secretly by private

to be monitored by fathers on public property. With the secret video surveillance

The right to informational self-determination is severely affected

interfered with other road users. These are based on the use of sidewalk and road

instructed and - without having given a cause or reason for this - by

Dashcam operator placed under general suspicion and monitored by video camera. the

Storage of the video recordings harbors a considerable potential for abuse, since they
Internet can be spread practically without limits. Only the dashcam operator has it
in the hand to decide when and for how long without the knowledge of the other
takes pictures and how he uses them further.

Also for any audio recording of the conversations that may take place
no legal basis evident. With regard to the regularly pursued purpose of
security in traffic accidents, there is already a lack of necessity for the recording of
conversations held in or next to the vehicle. Art. 6 Para. 1 Letter f GDPR separates
so also here as a legal basis. The Federal Court of Justice, judgment of May 15, 2018, VI
ZR 233/17, has clearly expressed in this regard that the Basic Law before
protects that conversations are secretly recorded and secret sound recordings (not
in public discussions) even more strongly in the right of personality
of the persons concerned intervene than already secret recordings of the (consciously in
the public moving) road users. The right to the spoken word
guarantees the self-determination of the own representation of the person in the communication
tion with others. This right to self-determination finds expression in the power of the
People to decide for themselves and alone whether to put his word on a phonogram
and thus may be accessible to third parties, with word and voice of the
Communication participant detached and independent in a form available for third parties
be done. According to Section 201 Paragraph 1 No. 1 of the Criminal Code, this even constitutes a criminal offence.
fills; in this respect, due to a lack of knowledge of the persons concerned, there is usually only a lack of
related lawsuits.

It should also be noted that the question of the civil or criminal law evidence
utilization must be strictly separated from the admissibility under data protection law. If civil and
Criminal courts accept video recordings made with dashcams as evidence in individual cases.

know, they regularly check the admissibility of the use of the data protection law
Dashcams openly and only dealt with the question of whether a data protection
legal inadmissibility of operating the dashcams, a so-called evidence processing
prohibition in specific civil or criminal proceedings. The instead specifically with the question of
admissibility of the operation of dashcams under data protection law
courts, on the other hand, have clearly confirmed that the use of dashcams by private individuals in public
traffic is in violation of data protection.
The above-mentioned judgment of the Federal Court of Justice of May 15 is also in this sense
2018 to understand. On the one hand, the Federal Court of Justice ruled that dashcam recording
under certain conditions can be used as evidence in accident trials.
On the other hand, however, he clearly stated that the video recording submitted in the proceedings
is inadmissible under the applicable data protection regulations. You violate
§ 4 Federal Data Protection Act (BDSG), since it was done without the consent of those affected
and not on § 6b Para. 1 BDSG old version or § 28 Para. 1 BDSG old version
88
2.3
can be supported. In any case, a permanent recording of the whole without cause
Happenings on and along the route of the plaintiff is to perceive his
interest in securing information is not required, because it is technically possible to
to design lass-related recording directly of the accident, for example
by continuously overwriting the recordings at short intervals and triggering
permanent storage only in the event of a collision or severe deceleration of the vehicle. In-
between the General Data Protection Regulation has used the Federal Court of Justice
The provisions of the Federal Data Protection Act are superseded, but this does not change anything
the basic legal assessment, because Art. 6 Para. 1 Letter f DSGVO writes a
Comparable balancing of interests, as previously already § 6b BDSG old version.

As a result, the use of a dashcam can only be assessed as data protection compliant if

if it is ensured that video recordings made with it - without a longer one

Storage justifying event - after a short time; therefore after a maximum of three to five

minutes to be deleted again. In fact, there are currently very few dash cams on

the market that actually allows the setting of such a tightly dimensioned loop loop

. Older recordings are usually only overwritten when the capacity limit of the

inserted memory card is reached. But this means at the same time that then regularly

the card already contains several hours of illegal video recordings. who

uses such a camera in traffic runs the risk of being subjected to a fine.

sets to become. So who at this point - there are many cheap offers - when purchasing a

Dashcam saves, it can be expensive for you later (see 6.4). In addition, this always applies

even if vehicle drivers have activated the microphone function of the dash cam.

2.3

Consent Questions

2.3.1 Revocation of consent given to municipalities

A designated data protection officer asked me for support in deleting personal

personal data in connection with the revocation of consent.

According to him, this is problematic if, for example, on the basis of a

permission to take photos at the anniversary celebrations of the volunteer fire brigade, in a

were given to the printers and then distributed to the participants.

Art. 17 Para. 1 Letter b of the General Data Protection Regulation (GDPR) states: "The responsible

liche is obliged to delete personal data immediately if one of the following

reasons apply: […] The data subject revokes their consent on which the

Processing [...] based, and there is no other legal basis for the processing

processing." With reference to this, the data protection officer asked the following questions:

•

All members who have received the brochure must be asked to

to blacken any mention of the person concerned by name and also to include him in all photos

make known?

•

Is the same thing done on the website of the volunteer fire brigade?

• What happens to the remaining brochures?

I pointed out the following to him: First of all, the obligation to delete only affects the

responsible. If the brochures have already been distributed, it is not as regards these

more responsible. The previous transmission was also due to the not yet revoked

no consent lawful. Although the person concerned can, according to Art. 7 Para. 3 GDPR,

revoked the consent at any time, but "through the revocation of the consent, the legality

not affected by the processing carried out on the basis of the consent up to the point of revocation". It lay

and there is still an "other legal basis for processing" in the sense

of Art. 17 Para. 1 Letter b GDPR.

If, however, as was further described by the data protection officer, brochures

have not yet been distributed or these are also available in parallel on the website of the Frei-

willing fire brigade (in the password-protected area) made available to the members

are to be deleted/destroyed or, for example, by blackening

to be edited.

The same applies to the portfolios of children that were also requested, which

day care centers (and also recommended by the Saxon education plan).

2.3.2

LernSax - the Saxon school cloud

During the school closures caused by the pandemic, a large part of the Saxons used

Pupils LernSax, the internet

based platform for communication and cooperation. When designing it, I was

start involved. At first, LernSax was a voluntary offer that was offered at participating

could only be used by interested students with their consent. This con-

The concept of voluntariness became apparent with the looming school closures by the

sian Ministry of Education (SMK) put to the test. It would have led

that in the case of non-consenting students (or their legal guardians)

taking part in lessons is not actually possible when a school decides in favor of LernSax

would have been.

I have therefore agreed with the opinion of the SMK that the school's internal electronic

nical communication between teachers and students from the educational mission

according to § 1 SächsSchulG and therefore does not require any further consent, provided that this

not done outside of an educational context or with third parties.

90

2.3

However, the use of LernSax is only required for direct teaching purposes

by students and their teachers. If communication with third parties outside of

educational context, consent must therefore also be obtained in advance,

such as the use of LernSax by legal guardians or external educational

partner.

These framework conditions are also referred to at lernsax.de.

2.3.3

Collection of health data from employees in the

coronavirus pandemic

In the spring of last year I received a complaint about the collection of health

security data of employees of an authority as well as with these employees in a house

halt living relatives.

The employees of the authority were asked by e-mail to have a deadline for health

data relating to chronic pre-existing conditions from themselves and also from relatives

who live with them in the same household to indicate that they are at risk of

indicate Covid-19 disease. The questions should be answered with "Yes" or "No"

be spoken. The authority wanted this information to take account of individual concerns

of employees when resuming regular business operations after the Corona

use pandemic.

According to Section 11 (1) of the Saxon Data Protection Implementation Act (SächsDSDG), public

personal data, including data within the meaning of Art. 9 Para. 1 Data

General Data Protection Regulation (GDPR) by employees, insofar as this is necessary for the implementation

management of the service or employment relationship or to carry out organisational, personal

Sonral and social measures, in particular for the purposes of personnel planning and

of personnel deployment is required or a legal regulation, a collective agreement or a

Service or company agreement provides for this. When processing personal

Any data within the meaning of Art. 9 Para. 1 GDPR are appropriate and specific measures

to protect the interests of the data subject (Section 11 (2) sentence 1

Saxon DSDG).

The agency asked workers via email whether the worker or a person associated with

lives in a household with him, has a chronic pre-existing condition that has caused him to develop a Covid

19 disease is exposed to a significant health risk. It's about

Health data according to Art. 9 in conjunction with Art. 4 No. 15 DSGVO, since the queried

Information on the physical health of a natural person, here the employee as well as

who are living with him in the same household or from whom information

Information about the state of health of the individual employee or the

Persons who live with him in a household emerge. This query e-mail represents

data processing within the meaning of Art. 4 No. 2 GDPR.

This data processing is neither for the execution of the employment relationship nor for

Implementation of organisational, personnel and social measures, in particular

Purposes of personnel planning and personnel deployment, according to § 11 paragraph 1 sentence 1

Saxon DSDG required.

Within the framework of the necessity test, the conflicting positions of fundamental rights

to weigh the production of practical concordance. The interests of the employer are

bers in the data processing and the personal right of the employee to an exit

equal, so that both interests are taken into account as far as possible

the. In order to be necessary, the aforementioned data processing must comply with Section 11 (1) sentence

1 SächsDSDG serve, suitable, necessary in the narrower sense

and be appropriate.

Data processing is suitable if it contributes to achieving the legitimate aim. target

It was the responsibility of the authority to take care of individual concerns when work was resumed

of employees who themselves have chronic illnesses and/or family members

who live with him in the same household and have chronic pre-existing conditions,

which exposes them to a significant health risk if they contract COVID-19

are to be taken into account.

Considerable doubts already existed as to whether the general query was suitable at all

to achieve the aforementioned goal. In particular, it was unclear which previous illnesses

lead to a significant health risk. Even the Robert Koch Institute (RKI) led

on his website rki.de under "Information and assistance for people with a

heren risk for a severe course of COVID-19 disease” (as of May 13, 2020) on that

due to various influences such as previous illnesses, age, obesity, smoking and de-

possible combinations, the risk assessment is very complex and therefore a

It is not possible to make a general determination of classification into a risk group. According to the RKI, it is rather

an individual risk factor assessment in the sense of an (occupational) medical assessment

required.

In the narrower sense, data processing is required if there is no equally suitable, mild

resources are available. As already stated, the RKI saw one on its website

(Occupational) medical assessment as the more appropriate means, the individual risk factors

to evaluate, at. This is also important for employees from a data protection perspective.

less intervention-intensive, since the employee does not report his previous illnesses to the employer

who informs the company doctor. Due to the medical confidentiality, the health data

from access by the employer, possibly also use for other purposes,

92

2.3

specially protected. On the other hand, the SARS-CoV-2 occupational safety standards of the Federal

of the Ministry of Labor and Social Affairs (as of April 16, 2020) occupational safety measures

take steps that employers should take to protect their employees. Through this

Measures could be appropriate to the individual concerns of employees who

have been exposed to increased COVID-19 disease, are received and these are

to the notification that the employee and/or persons working with him in a

Living at home, has/have a chronic pre-existing condition, a milder remedy.

The processing of health data is also not based on consent in accordance with Art. 9 Para. 2

Letter a GDPR justified.

Consent within the meaning of Art. 9 Para. 2 Letter a GDPR can only be effectively granted,

if the data subject is involved in the processing of health data for one or more

has expressly consented to specified purposes and the requirements of Art. 4 No. 11

and Art. 7 GDPR are fulfilled (cf. data protection conference, brief paper no. 20, consent according to

of the GDPR, available at datenschutzkonferenz-online.de; European data protection
shot, WP 259 rev. 01: Guidance on consent under Regulation EU
2016/679; Activity report 2019, 2.3.1, page 57 f.).
The e-mail addressed to the employees already contained no instruction about the
term possibility of revocation.
On the other hand, the declaration of consent was not voluntary. Due to the existing
The dependencies in the employment relationship are special requirements with regard to
on the assessment of voluntariness. This applies in particular with regard to the
conditions under which the consent was given and that they are particularly sensitive
data (health data).
In the e-mail to the employees it was pointed out that the questionnaire within
a period of a few days and then incoming feedback
presumably can no longer be taken into account.
The employees therefore had to assume that if they did not provide information or
do not take any further or special precautions in the event of a lack of feedback
Protection against Covid-19 would be taken by the authority. Against this background
It cannot be assumed that the health data will be given voluntarily.
Incidentally, this also constituted a violation of the basic ban on coupling in the
within the meaning of Art. 7 Para. 4 GDPR. Ultimately, the employer couples the consideration
ment of individual concerns when resuming service to the indication of
Health data by the respective employee, although, according to the SARS

CoV-2 occupational safety standards of the Federal Ministry of Labor and Social Affairs, other pos-
opportunities exist to take these into account.
Due to my activity, all data collected by means of the questionnaire

were deleted. I have pointed this out to the authority in accordance with Art. 58 Para. 1 Letter d GDPR

pointed out that personal data, in particular health data of employees,

may only be processed insofar as this is necessary for the performance of the service or employment

niss or to carry out organizational, personnel or social measures, in particular

in particular for the purposes of personnel planning and personnel deployment

and when processing health data, appropriate and specific

Measures to protect the interests of the data subject must be provided.

2.3.4

Mandatory consent to advertising on a

shopping portal

Not every effort to create clarity succeeds. So that contractually bound customers themselves

not want to be surprised about later e-mail advertising, but their basic permissible

an online portal had a mandatory button

set, which read: "I revocably agree at any time, ..." In the event of non-confirmation

Due to this, however, it was technically no longer possible to place an online order. The complaint

defuhrin suspected a violation of the coupling ban according to Art. 7 para.

4 General Data Protection Regulation (see also recital 43 of the regulation).

The purpose of the declaration that was plausibly explained to me by the person responsible

was by no means therein, the already legally existing one created by contract

additionally secure the processing basis with consent. the consent field,

which had rightly been criticized as a result, did not serve to give consent, but

only a definitive confirmation of acknowledgment of the already legally applicable

provisions. According to the person responsible, the advertising objection should be

the first contact with the customer is by no means prevented. With only superficial

However, based on the understanding of the clause, it was to be expected that customers using the portal

would not be in a position to develop such a thing.

The deviation from the standard of digital terms and conditions is at my instigation al-

however, was quickly corrected.

2.3.5

Advantages over data – advertising or otherwise

Data use as a subject of the contract

In my opinion, the regulatory work of my authority also has the

groups involved in data processing and private autonomy.

94

2.3

However, a development can also be observed in data protection issues that

safety of the individual in terms of welfare rhetoric. Art. 7 para. 4 and recital 43 of the

General Data Protection Regulation (GDPR) seem to support this trend in the field of advertising

strengthen, as they make it more difficult for data subjects to disclose data voluntarily

shine. But not when viewed fully. It may help ground

to study the General Data Protection Regulation in its entirety, including Art. 1 para.

3: “The free flow of personal data in the Union is prohibited for reasons of protection

of natural persons in the processing of personal data is not restricted

nor be banned.” In Germany, this freedom also materializes in the constitution

in the legal institution of contractual freedom. In this sense, 2019 also has a higher regional court

decided that if personal data has value (resulting in the enactment of the

General Data Protection Regulation has contributed), their use by those affected

person cannot be prevented from dealing with a company (cf. Higher Regional Court

Frankfurt, June 27, 2019 - 6 U 6/19, motto and para. 18th; see also activity report

2019, 2.3.5., page 62 ff.).

Should compensate for the acceptance of advertising with goods or monetary benefits

no data protection consent is required. Required is the

common will of both parties to conclude a transaction under defined conditions.

But: Only the agreement reached in advance with unmistakable clarity with

the declarations of intent make it necessary to consent to data processing

according to Art. 7 GDPR obsolete. The core business can then be based on Art. 6 Para. 1 GDPR

will. And the integral consideration of the person affected by data protection law can in this respect

also consist in the acceptance of advertising messages reaching him.

2.3.6

Insurance broker consent forms

Several complaints during the reporting period revealed that various insurance

brokers used uniform consent forms for all types of insurance. There-

according to were also in car or building insurance et cetera flat rate next to

further data sensitive health data from the consent to the data processing

includes.

Such a broad declaration of consent is due to a violation of the requirement of the

4 of the General Data Protection Regulation (GDPR) is ineffective. Because a reason

sentence of data protection law is the restriction of data processing to the

specific purpose required (cf. Art. 5 Para. 1 Letter c GDPR (data minimization)).

95

Chapter 2 Principles of data processing

In addition, corresponding clauses are also allowed according to §§ § 305c paragraph 1 BGB, 306 civil

German Civil Code (BGB) to be ineffective. After that, surprising and unclear clauses in all

general terms and conditions (GTC) ineffective; these are the regular

cheap

Such processing that goes beyond the specific purpose of the contract can of course

cannot, of course, be effectively agreed as part of a contract. For the terms and conditions

This already follows from the provisions of the BGB from the scope of the standards for which data

General Protection Regulation from Art. 6 Para. 1 Letter b GDPR from the

the extraneous necessity of processing for the contract.

In all cases, I was able to

Appropriate clarifications in the forms or the use of the respective

effect contractual purpose of adapted forms. The data protection compliance more appropriate

Consent forms reduces the corresponding risks from data transactions based on

processing and counteracts a lack of data protection awareness on the part of those responsible.

Against the background of the comprehensive willingness to cooperate of those responsible

apart from pursuing the violations that have been stopped, especially since intent cannot be determined

was, and it was plausibly demonstrated that no corresponding illegal data processing

works would have taken place.

2.4

Sensitive data, special categories

personal data

2.4.1

Privacy-friendly collection of health data

employees

A teacher employed at a public school in Saxony has resigned because of the survey

contacted me about health data. After an accident through no fault of one's own

gender incapacity, she should fill out a form (report form for events caused by third parties)

fill out an accident report, with which, among other things, medical diagnoses are made

will. This form should be sent to the State Office for

Taxes and finances are sent. The school she works at also wanted that from her

save the completed form.

In the event of accidents involving workers caused by third parties, the

employee may have a claim for damages due to loss of earnings

to which the employee has incurred as a result of the inability to work in relation to the third party

ten/accident causer. This claim for damages against the third party/accident

The polluter is transferred to the employer by law, insofar as this is passed on to the employee

has continued to pay wages (cf. Section 6 (1) of the Continued Pay Act).

96

2.4

According to Section 6 (3) of the Continued Remuneration Act, the employee must inform the employer

plus the information required to assert the claim for damages

make. Due to these legal regulations, the employer is therefore fundamental

authorizes this data, which also records health data, to be used by the employee

long or to process them. For civil servant teachers, § 111 Saxon

sches civil servants law before a comparable regulation.

With regard to the information on the consequences of injuries and hospital stays, which are

lar are queried for events caused by third parties, these are special categories

ria of personal data according to Art. 9, Art. 4 No. 15 General Data Protection Regulation.

With regard to this data, appropriate and specific measures are to be taken to protect the

interests of the person concerned (§ 11 Para. 2 Sentence 1 Saxon Data Protection

Implementation Act (SächsDSDG)). This reporting form is currently available via the personnel administration

authority, here the State Office for Schools and Education, to the State Office for Taxes and

to forward finances, since this faces the above-mentioned claim for damages

asserts legal claims against the person who caused the accident. The State Office for Schools and Education adds

the registration form filled out by the employee, a copy of the sick note and the

amount of the annual holiday entitlement in which the damaging event occurred. This procedure

I have discussed this with the responsible office in the State Office for Taxes and Finances.

I was given a more privacy-friendly design of the procedure described in

With regard to the unnecessary knowledge of employees' health data

the personnel administration position promised. I will do this as part of my

continue to pursue visual activity.

Regarding the storage of the registration form for accidents caused by third parties by the school

I informed her that the data would not be stored in accordance with Section 11 (1) and (2) SächsDSDG

is required. The aforementioned subrogation of the claim for damages takes place

not on the individual school, but on the Free State of Saxony. For the legal validity

Making the above claims for damages is within the public

Administration of the Free State of Saxony commissioned the State Office for Taxes and Finances and

just not the individual school. A requirement to store this data for the

Implementation of the employment relationship or to carry out organizational, personnel

and social measures by the individual school is - due to the described conditions

authority of the State Office for Taxes and Finances - therefore not apparent and accordingly

accordingly not data protection compliant. Also with regard to the data of third parties, such as the

Data of the person who caused the accident is the principle of data minimization according to Art. 5 data

General Protection Regulation to be taken into account.

2.4.2

Reimbursement of union dues by the employer

In the last reporting period, I received an inquiry about the data protection-compliant procedure

the reimbursement of union dues by the employer.

The background to the request was the agreement of a new collective agreement. This one contained one

Regulation according to which the employer should be obliged to inform each union member of the

annual union dues reimbursement.

In order to implement this collective bargaining agreement in the company, the employer wanted

Gen submission of a certificate from the trade union support organization that the

Union membership confirmed, union dues paid with payslip

equip By presenting the contribution certificate, however, the employer would

Be disclosed about union membership. As an outflow of the coalition

freedom according to Art. 9 Para. 3 of the Basic Law, membership in a trade union is a sensitive

les personal data, which deserves special protection, since in connection

related to the processing significant risks for fundamental rights and freedoms

may occur. In this respect, the information is sensitive information

Within the meaning of Art. 9 Para. 1 General Data Protection Regulation (GDPR), the processing of which is only

within the narrow limits of Art. 9 Para. 2 GDPR.

It is the submission of the membership certificate and the assertion of the

chen claim by the employee is not a consent situation according to Art.

9 Para. 2 Letter a GDPR, however, this application situation is similar to consent. The ever

The current employee can decide for himself whether he has reimbursed the membership fee

and decide accordingly whether to file an application with disclosure of trade union

membership or waives this benefit.

Doubts regarding the voluntary nature of the employee's decision, in particular

especially with regard to the dependency of the specific employment relationship

employed person, did not exist in this case, since the workers have an economic

have gained an advantage.

I therefore have no data protection concerns about the procedure described

for reimbursement of union dues.

98

3.1

3

data subject rights

3.1

Specific Obligations of the Controller

3.1.1

Data protection information according to Art. 13 GDPR -

One-fits-all solution allowed?

When examining the video surveillance of a large landlord, I was confronted with

that the person responsible in principle adheres to the

two-stage information concept recommended by the authorities (cf. activity report 2019, 3.1.1,

page 71

(available at

datenschutzkonferenz-online.de), but with the complete information in

had integrated a data protection information on its website, covering practically its entire

covered the processing of personal data, but was still different in scope

still limited to one page.

as well as the video surveillance guide

et seq.)

I have pointed out to those responsible that, on the one hand, such a generally

and on the other hand such comprehensive data protection information has a serious impact

shows a lack of transparency and therefore does not comply with the provisions of the data protection

Basic Regulation (DSGVO) is in line (Art. 5 Para. 1 Letter a and Art. 12 Para. 1

GDPR).

Specifically related to video surveillance was very limited for those addressed

comprehensible which of the information contained in this information sheet specifically for the

Video surveillance apply. Such a "one-fits-all" architecture in which the addressee first

painstakingly the data processing that is possible for him or for the data processing that interests him

must seek out statements that may be valid does not meet the transparency requirements

provisions of the General Data Protection Regulation. This means that he does not reliably know which data

processing carried out and which data under which circumstances to which recipients
be transmitted. Especially for non-tenants, but of course under
circumstances also persons affected by the video surveillance, contained the information
leaf out a lot of irrelevant information.
I have therefore first asked the landlord to set up a separate one for video surveillance
to create a complete information sheet and of course recommended him to do so
based on the model recommended by the supervisory authorities.
My above criticism of the “one-fits-all” architecture of this data protection information also applies
beyond video surveillance also in relation to all other processing activities
ten. The information obligation according to Art. 13 GDPR is to be fulfilled in a processing-specific manner; one

only data protection information for all processing activities is for the persons concerned
completely non-transparent and contradicts the requirement of Art. 12 Para. 1 GDPR. So
For example, the information provided to tenants when concluding a rental agreement must
tion according to Art. 13 GDPR specifically (and exclusively) on the processing of tenant data in
within the framework of the tenancy.

3.1.2 Information obligations of lawyers as professional secrecy

In the last reporting period, I received an inquiry about the information obligation of lawyers
or a law firm. In connection with a claim turned over
a law firm approaches an involved party. The person affected complained that the
Obligation to provide information on the letter from the law firm sent by conventional mail
pursuant to Articles 13 and 14 of the General Data Protection Regulation (GDPR) was not satisfied. on
the law firm's letterhead would only indicate that the data

Proceedings are processed. The data subject asked whether the attorney

law firm provides the data subject with the data protection information in accordance with Art. 13, 14 GDPR

or should have forwarded it with the first brief or not. in a stele

The Bar Association made a statement to the person concerned

reference to the professional secrecy existing for lawyers and denied a corresponding

corresponding obligation.

As a result, I share the opinion of the Bar Association. Considered in concrete

In individual cases, also due to the way in which it was collected, only information pursuant to Art. 14 GDPR, data

data collection from third parties. Pursuant to Art. 14 Para. 5 Letter d GDPR are persons subject to professional secrecy

exempted from the information obligation. According to my

the protection of the relationship of trust between the person subject to professional secrecy and the beneficiary

of professional secrecy, the client, towards third parties. That is

The information requirements of Art. 14 GDPR do not include the data itself, but only

lich the categories of data or their processing, nevertheless

the information obligations according to the wording of the regulation are completely excluded.

It should also not be overlooked that with a certain frequency and in an unforeseeable

bare and manageable references even general information conclusions on the

content subject to professional secrecy and this serves the purpose of the exceptional

could jeopardize determination as a whole.

As a result, there is no obligation on the part of lawyers as persons subject to professional secrecy.

However, this only applies to third parties, not to our own clients.

the beneficiaries of professional secrecy, so that towards the latter the

According to the catalog of Art. 14 Para. 1 and Para. 2 DSGVO content to be explained

or must be kept ready.

100

3.2

Lawyers and law firms are also the information

obligations by means of so-called easily accessible "data protection declarations" on the website

to demand.

The above considerations apply to other non-public professional secrecy relationships

cher positions - responsible person - basically transferable. In other circumstances, for example

in the case of public authorities, however, the exemption clause for persons subject to professional secrecy becomes special

and to be considered more differentiated.

Finally, it should be emphasized that the exception is only for the protected

activity as a professional secrecy subject. As a digression, an interesting decision by the

Federal Fiscal Court, which was based on the question of whether a lawyer as an external

data protection officer works as a commercial entrepreneur or lawyer. the bun

desfinanzhof decided that a data protection officer does not belong to the profession of legal

walt's reserved activity, but to separate from the legal activity

commercial activity (cf. Federal Fiscal Court, judgment of January 14, 2020, VIII R 7 20/17).

Section 29 (3) of the Federal Data Protection Act refers to the group of persons subject to confidentiality

1, 2a and 3 of the Criminal Code. After the newly added para.

2a of the criminal law provision, however, data protection officers themselves as

professional secrecy treated, so that a different type of activity of an approved

Attorney would play no role in the case. In other cases, the non-attorney

but precisely not that of a person subject to professional secrecy, but merely commercial

lich. In these cases, the person who is also a lawyer is not one of them

exempted from information obligations.

For the capacity as the person responsible for the external data protection officer, compare the

Post under 2.1.2.

3.2

right of providing information

3.2.1

Request for information to the school in a service law

matter

Petitioners informed me about the following facts: Your daughter, who until then had not

days, was on the last day of school at the request of the headmistress by the police

lizei to the school - without the school having previously tried to telephone the mother

asking about her daughter's whereabouts. As a result, disciplinary proceedings against the

Headmistress initiated. On the penultimate day of school we had an overnight stay together

with a voluntary breakfast together. Both at the overnight stay

and the daughter had not taken part in breakfast.

Information or a copy of the data processed in this context

her daughter according to Art. 15 General Data Protection Regulation

(GDPR), specifically one

However, it is up to you to send the opinion of the headmistress and the class teacher

been denied. The State Office for Schools and

Education (LaSuB) confirmed this representation.

It initially justified this by saying that the scope of the GDPR does not open up

because there was no automated processing of personal data. This

however, was not convincing. According to Art. 2 Para. 1 GDPR are the provisions of the GDPR

apply if personal data is processed fully or partially automatically

are processed or if personal data are processed in a non-automated manner that are

are or should be stored in a file system. To automated processing

this is not the case here. But it is to be assumed, since it is personal

Data that was processed as part of a supervisory complaint that this

Data in a file system (personnel file or fact file) in the sense mentioned above

are saved. Otherwise, Art. 15 GDPR is based on Section 2 (4) sentence 1

Saxon Data Protection Implementation Act

(SächsDSDG) generally accordingly

apply, since the LaSuB is undoubtedly a public body for which

the SächsDSDG applies (§ 2 Para. 1 SächsDSDG).

Furthermore, the LaSuB referred to Art. 15 Para. 4 GDPR. This determines that right

upon receipt of a copy must not adversely affect the rights and freedoms of other persons.

Recital 63 of the GDPR explains:

“This right should protect the rights and freedoms of others, such as trade secrets

or intellectual property rights and in particular copyright in software

affect. However, this must not result in the data subject being deprived of any

future is denied."

Whether the requirements of Art. 15 Para. 4 GDPR are met in the specific case could be determined by

cannot be judged on me, since factual information was missing. privacy rights of

The principal and the class teacher would in principle be considered rights of third parties

draw. Whether these were the basis for decision-making and whether they are also relevant in this context

was dealt with the question of how far these rights extend in official acts,

however, is not demonstrated. Otherwise, the person responsible bears the burden of proof for the existence

the requirements of Art. 15 Para. 4 GDPR.

Finally, it was pointed out that the right to information under data protection law

there would be a possible right to inspect files. However, it is not the purpose of the

right to information, to circumvent a non-existent right to inspect files.

102

3.2

It is true that the right to inspect files and the right to information under data protection law

fundamentally convey two juxtaposed claims. On the one hand, they

different purposes and, on the other hand, relate to different objects. This

fundamental juxtaposition can be repealed, however, if the legislature with

the regulations on the right to inspect files, the right to information according to Art. 15 GDPR

wanted to restrict. However, such a restriction would have to meet the requirements of Art.

23 GDPR are sufficient. There is no right to inspect files in procedures for administrative complaints

Law. In particular, Section 29 of the Administrative Procedures Act (VwVfG) is not applicable because it

These procedures are not administrative procedures according to § 9 VwVfG in connection with

§ 1 sentence 1 SächsVwVfZG. It is therefore not subject to a restriction of the information

to go out on the right.

My corresponding letter to the LaSuB led to the

information was finally given.

3.2.2

Refused information on the address reference for the letter shop model

In one case, a person responsible for the dissemination of his advertising has a

had served the address pool owner, declared to a data subject that the advertising

agency for data protection reasons. This misunderstanding could

I clean up. The person concerned who requested the information received the information.

In general, I welcome the implementation of data protection principles

reduced and the stock of own advertising data reduced to the required minimum

is restricted. Views that generally point to a shared responsibility for the

I do not follow the lawfulness of the processing undertaken (cf.

also on the lettershop model and shared responsibility 4.2.3).

It is advisable for reputable advertising companies to research their data sources very carefully.

choose and for sufficient documentation by self-specified random sample -

in particular to provide evidence of consent.

3.2.3

Right to free data copy for bank statement data

In several cases, those affected turned to me, to whom the responsible credit institution

with reference to contractual or statutory fee provisions only for a fee

pien of the processed data wanted to grant.

According to Art. 15 Para. 3 General Data Protection Regulation (GDPR), the data subject has the right

to obtain a copy of the data stored and processed by a person responsible

personal data. According to Art. 12 Para. 5 GDPR, the copy is to be provided free of charge.

The right to a free data copy exists independently of contractual or statutory

Regulations that set a fee for certain documents or copies. That's how it is

This right also applies, for example, if there are contractual fees for account statements or copies thereof

are agreed. This also applies, for example, to the patient's right to a copy

the patient file (cf. activity report 2017/2018, part 2, 3.2.3, page 195).

However, the right to a data copy under data protection law does not include a right to one

specific structure of the copy. The person responsible has received a copy of the available files

However, to provide raw data in a common format, this does not have to be in

bring a certain structure. Accordingly, the person concerned cannot make free copies

ask for bank statements. A structured listing of payment terms is required

in the form in which the data is available to the credit institution, or another common form

Format.

The background to the concerns of the banks is regularly that they are responsible for copies of account statements

gene want to charge not inconsiderable fees. Free of charge et cetera according to Art. 15

Para. 3 GDPR disturbs these expectations.

In my opinion, only a copy is owed, but not necessarily in

form of account statements. If the person responsible has a copy of the available files
to issue raw data in a common format, it doesn't have to be in a –
provided by the information seeker - specific structure. Accordingly, the
met do not ask for free copies of bank statements, but they do ask for an orderly one
List of payment transactions in the form in which the data is available to the bank
or in another common format.
The question of whether the person responsible has to provide copies of account statements
if he uses this - in addition to the underlying data, among other things in his
management system – saved as such in PDF format, for example, did not have to be
be answered, but in my opinion it should also be answered in the affirmative.
The argument put forward by those responsible and business associations that
Granting such a copy is inadmissible due to conflicting rights of third parties
theoretically true. However, it must be taken into account that the corresponding
data has already been made available to the data subject in the form of account statements,
and the renewed provision insofar as the economic social sphere of the third party
should at most touch peripherally. Insofar as rights of third parties are actually opposed here
should stand, the right to a copy is not completely excluded, but
limited at most. In any case, if the person responsible complete the issue
offers copies of data in the form of account statements for a fee, the reference appears
Third-party rights to refuse the corresponding free information clearly as a
104
3.2
pretense. Such a contradictory impairment of the rights of those affected
would be weighted as a data protection violation.
The Cologne Higher Regional Court, judgment of July 26, already has an unlimited right to information
2019 - 20 U 75/18 (not legally binding, pending at the Federal Court of Justice under Az. IV ZR 213/19) and

the Austrian Federal Administrative Court, decision of December 10, 2018, W211

2188383-1, decided.

Courts of instance, authority and literary opinions that claim the right to information without

limit legal support cannot be followed for fundamental reasons.

the:

Restrictions find no legal support: rather, the reasons for which

right to information may be restricted, in the data protection laws conclusively

lists. Financial interests of those responsible, with the relevant information

making gains are clearly not included.

To allow restrictions not provided for by the General Data Protection Regulation would have

inevitably result in a gray area in which those responsible

met "let starve to death by the long arm". In fact, that would be what is provided for by law

Right to information eroded.

The purpose of the right to information, to enable data subjects to check

would be thwarted as well as the purpose of the right to copy, competition and exchange

to lower barriers.

My authority provides the rights to a copy of data in accordance with Art. 15 GDPR

solely on the legal restrictions and the general figure of the legal

customary, which in Art. 12 Para. 5 Sentence 2 GDPR as excessiveness of the request

finds legal support. Comfort and poor bookkeeping on the part of the person concerned count

I not below.

This solution also appears to be legally congruent, since those responsible regularly

Example of commercial and tax law, the data must be tracked in a structured way, and a - usually

moderately electronic copy should hardly cause any (additional) costs.

The basic question of the scope and limits of the right to information and a copy is in

much still unclear. Even if all Saxon procedures at least with regard to account

information could be resolved amicably so far, a binding one appears

Supreme court clarification, for example as in Austria, is desirable in order to ensure lasting clarity

Identify responsible and affected persons.

105

Chapter 3 Data Subject Rights

3.3

Right to Erasure

3.3.1

Obligation to delete account statements by the

Job centre?

As part of a submission, I dealt with the question of whether the petitioner has a right to the

Deletion of his account statements as soon as he no longer receives unemployment benefit II (Hartz IV).

The petitioner is of the opinion that former Hartz IV recipients have the right to immediate

have all personal data deleted. He refers to § 84 paragraph 2

Tenth book of the Social Code (SGB X) old version.

According to Art. 17 Para. 1 Letter a of the General Data Protection Regulation, the data subject has

(DSGVO) the right to demand that the person responsible

related data will be deleted immediately if the personal data for the

Purposes for which they were collected or otherwise processed are no longer necessary

are.

Art. 17 para. 1 letter a GDPR essentially corresponds to that until the entry into force of the

GDPR applicable law in Germany. According to Section 84, Paragraph 2 of the Social Code, social data was X old

Version then to delete if their knowledge for the responsible body to lawful

Fulfillment of the task lying in their responsibility was no longer necessary and no

There was reason to assume that interests worthy of protection were affected by the deletion

ner would be affected.

The personal data, in this case bank statements, must, according to Art. 17 Para. 1 Letter a GDPR for the purposes for which they were collected or otherwise processed, be agile. It had to be checked whether the job center needed the account statements and still did will need.

According to § 67b SBG X is the storage, modification, use, transmission, restriction the processing and deletion of social data by the bodies named in § 35 SGB I only permitted insofar as data protection regulations of SGB X or another Scripture of the SGB allow this.

Section 51b SGB II came into consideration as the area-specific legal basis for processing. According to § 51b Abs. 1 SGB II, the responsible carriers of the basic security for job seekers continuously the necessary for the implementation of the basic security for jobseekers data. § 51b para. 3 SGB II stipulates that the data collected under paragraphs 1 and 2 Data will only be processed and used for the purposes listed there - numbers 1 to 5 that may. Here number 5, combating benefit abuse, came into consideration.

106

3.3

The regulation for the collection of data according to § 51b of the SGB II regulates which data is Implementation of the basic security for job seekers are to be raised. According to § 1 No. 2 and 3 of this regulation are, among other things, data on the type and duration of the needs, the output to collect benefits and income as part of the basic security for jobseekers. In addition Account statements must be counted, which document income and expenses, for example. To § 45 SGB X is the withdrawal of an unlawful beneficial administrative act up to possible expiry of ten years after its announcement.

The file plan SGB II of the Federal Employment Agency of October 1, 2012 regulates a flat rate retention periods of ten years.

According to § 51b paragraph 3, the job center is required to keep the copies of the account statements

SGB II required. A right of the petitioner to have his account statements deleted under Art. 17

Para. 1 letter a GDPR, after he no longer receives SGB II, therefore does not exist.

The Federal Social Court (BSG) ruled on May 14, 2020 (Az.: B 14 AS 7/19)

that bank statements that the job center has taken for the benefit file, about a

period of up to ten years may be filed. They are at this time

space therefore not to be erased. The account statements may also be copied for this purpose. alone that

Reference to the preparation of file notes on the submission of account statements

however, the court expressly does not allow this to suffice (cf. also 0).

3.3.2

The deletion of customer profiles and accounts

In the last reporting period, I received a message from a flirt portal customer who said

after self-triggered deletion of his customer account further reminder emails,

said he had received "nudgemails" from the portal and feared that this would affect his

would bring new partner in unfortunate need of explanation. The ultimate cause

was, however, that he had to confirm the e-mail before implementing the deletion

(in the sense of double opt-out) and his account was never deleted.

The question of whether endless memories with no consequences have been contractually agreed in this case

are, I had initially left aside in view of the input lecture. She could all-

dings reappear when a customer does not cancel, but only from "We miss you" -

Messages want to be spared (cf. also 2.2.20).

With the deletion of the profile or customer account, those affected often have to assume

ensure that any objection to advertising is also deleted. Would later

If you register again with the same e-mail address, you cannot

assumed that the (old) contradiction in advertising would continue, but would have to

reformulate if necessary. Of course, this does not apply in the case of an advertising blocking file created by the

Responsible as a service after the end of the business relationship and a civil law violation

reasonable grace period should only be conducted on the basis of consent.

3.3.3

Common complaints about unsolicited email marketing

Even in the current reporting period, unwanted advertising has a not inconsiderable number

Percentage of entries identified. Structural failure of those responsible is

however usually hardly the cause. Of course I'm only talking about reputable market

who can be reached and who can provide company details, addresses and phone numbers

to their business.

As far as unknown senders are concerned, data subjects should inform themselves in the case of sending

unsolicited email or other electronic communications via browser and client

Fix the settings or contact the Federal Network Agency in the event of phone number misuse.

Do electronic mailings contain extortion or sensitive data of those affected, e.g

Example bank information, one should contact the police.

So far, my supervisory authority has not been able to protect against those that are not easily identifiable

To identify spammers or senders of unwanted emails or even their business model

to dry out.

Regarding the terminology of “advertising”:

“According to general usage, the concept of advertising encompasses all measures

of a company aimed at promoting the sale of its products or services

are directed towards genes. In addition to direct product-related advertising, this also includes

Direct sales promotion - for example in the form of image advertising or sponsoring -

detected. Advertising is therefore in accordance with Art. 2 lit. a of the Directive

2006/113/EC on misleading and comparative advertising any statement made when exercising

a trade, business, craft or freelance profession with the aim of selling goods

or to promote the provision of services",

according to the Federal Court of Justice in its judgment of September 12, 2013 (I ZR 208/12, Tz. 17).

By far not every advertising approach that was perceived as undesirable in the

A complaint was inadmissible. Fortunately, according to my

attention with reputable responsible persons no structural, but predominantly individual

individual mistakes made by employees in the incoming complaints process.

It is not uncommon for complainants to have insufficient knowledge of the legal

rern for submissions to my office. On the one hand, advertising messages are made by customers

considered inadmissible without consent, which was mistakenly perceived as a prerequisite,

on the other hand, one recognizes not (completely) fulfilled solutions due to legal regulations

Demand for repairs after termination of contractual relationships as a data protection violation.

In the area of e-commerce, the intended (advertising) subsequent use, which was originally intended for

E-mail address collected during contract processing, communicated to the persons concerned.

In many cases, however, this is not in the interests of contract customers, which is often

Knowledge of the legal situation leads to data subject submissions. Many of those affected give in their

Complaints that they have never consented to a marketing approach via e-mail and continue to do so

therefore outright inadmissible.

The following or comparable notice is often found on platforms in the e-commerce sector

to find: "After entering your e-mail address, you will receive personalized, on your purchase

related offers and recommendations. You can opt out at any time at no additional cost

object, for example via the unsubscribe link at the end of each of our emails."

Such information takes on the legal situation according to § 7 paragraph 3 law against unfair

Competition (UWG) reference, advertising to (existing) customers with electronic

scher Post allows, but does not refer to a consent given in the ordering process.

It can also be seen from "Your purchase" that the notice only applies to existing customers

directs.

Advertising is permitted in these cases, but the person concerned has the option of objecting

to raise an objection to direct advertising (cf. also activity report 2017/2018, part 2,

3.4.2, page 198 f.).

In my opinion, an objection to advertising must be given to the person responsible

at any time - i.e. also before the first newsletter - and in every available one

form can be explained, but not by replying to no-reply senders. expedient

"Opt-Out" boxes set up on the website by those responsible are also

or immediate unsubscribe buttons, which are not only used as a consumer but also as a

exercising the right of data subjects would be regarded as data protection-friendly, although I

currently see no way to demand or prescribe this.

However, it should also be noted that advertising in the event of aborted order processes,

that have not led to a valid contract remains inadmissible.

It is not uncommon for input cases in which the persons concerned to have received advertising

request the "complete" deletion of your personal data from the person responsible

gen. These then contain complaints about communications from those responsible that the

the deletion desired by the data subject could not take place for legal reasons.

In fact, there are legal deadlines for the physical deletion of certain types of data,

in particular according to Section 257 of the German Commercial Code (HGB) and Sections 140 et seq. of the Tax Code (AO).

up to ten years. This 10-year period mainly includes accounting documents as well

Bills. The retention period for commercial letters - i.e. business communications

cation, possibly also e-mail traffic - is six years (§ 257 Para. 4 HGB).

As a result, this data is also subject to a restriction of use, in particular

special for transmissions to third parties and for advertising purposes.

Anyone who, as a customer and data subject, has already received a binding - not "subject to change" -

Inquiry/order has concluded a contract cannot subsequently be completed

Enforce deletion of all data concerning him (see also activity report

2017/2018, part 2, 3.3.1., page 197).

It is not uncommon for those affected to request written confirmation of the successful implementation. A

Data protection claim for confirmation of a deletion/usage

restriction or justification for non-deletion by the person responsible

although not as a genuine claim. However, those responsible should at least not

respond to fully achievable erasure requests with a convincing justification,

also in your own interest. You often avoid the much higher effort,

resulting from a request for information. In addition, the use of my

authority can then also be waived by the person concerned.

3.3.4

Ongoing processing of personal data

potential heirs by a person in charge

A Saxon bank was involved in the determination of heirs by a probate court

been informed in another federal state that there is neither a

certificate of inheritance had been issued, nor had a waiver of inheritance taken place. Next to it was

been informed without any apparent legal basis that a brother of the deceased

existed. The bank now tried to name the brother of the deceased as heir for the

to make significant estate liabilities liable, since this is fundamentally a statutory

(joint) heir came into consideration. Even after he announced that he was not an heir,

he was further contacted and informed, only if the actual heir was named

or after it has become known, further processing of it

data are disregarded.

The person concerned had contacted my office to have his data deleted

obtain from the credit institution.

110

3.3

However, since the data processing is used to assert legal claims and thus

legitimate interests, existed according to Art. 6 Para. 1 Letter f of the General Data Protection

ordinance (DSGVO) has a legal basis for this. As long as it is not certain that the brother

who has not actually become an heir, the legitimate interest can also be personal

Data may only include potential heirs.

For a claim for correction was not specific and after

verifiably submitted, on what grounds the complainant considered legal

inheritance was not an option as an inheritance. A right to deletion does not exist as long as

there is a basis for processing and a corresponding purpose. thereby came

it does not matter here whether the probate court forwards the relevant information

could. In any case, the prerequisites for a permissible change of purpose were concrete

according to Art. 6 Para. 4 GDPR.

There was also no right of objection within the meaning of Art. 21 GDPR in the specific situation

given. The complainant expressed concerns about possible credit risks

the assertion of claims. However, since a registration of untitled, disputed

in credit bureaus is not permitted (cf. Section 31 (2) of the Federal Data Protection Act),

there was no concrete risk that the creditworthiness or the corresponding assessment

tongues could be damaged by credit bureaus. In any case, against corresponding

According to unlawful registrations, there was a right to cancellation and a claim for damages

the.

The possibility according to Art. 18 Para. 1 DSGVO the (temporary) restriction of processing

was to be achieved against the background of Art. 18 Para. 2 DSGVO further permissible Ver-

processing ("to assert, exercise or defend legal claims") here

ineffective.

With the applicable data protection law, preliminary civil law issues cannot be solved by themselves

attempted, but the data processing for the assertion of legal claims

expressly privileged (cf. e.g. Art. 9 Para. 2 Letter f and Art. 18 Para. 2, 2nd alternative GDPR).

The pending state of admissibility of data processing on the basis of potential

liability could only be asserted before the statute of limitations for the alleged claim

way to be terminated, which the complainant was made aware of.

3.3.5

Much ado about nothing: baseless anger about old people

video cameras

The starting point for a curious case were three video cameras that one himself had in the area of the

Complainant active in data protection reported to me. With that background, he was the one

firmly convinced that there was a breach of data protection, especially since there was even a camera

was aimed entirely at the public domain. He further noted that there -

it was a commercial property - no indication of the responsible camera

ra operator give. Not even a pictogram for video surveillance is available. On-

Due to a nursing home opposite, he went from a large number

affected persons.

Apparently the complainant left the alleged video recording of his person

no peace, so that despite his complaint he came to me on the same day

Gene Faust did further research. In doing so, he came across the Internet under the

address to a security company, to which he immediately sends a request for information under Art. 15

General Data Protection Regulation (GDPR). In this regard, he pointed – only

based on his observations and findings on site - in the manner of a supervisor

listen to the illegality of the processing carried out with the video surveillance

personal data, saw several fine regulations violated and

requested at the same time the deletion of the records relating to him. With that he brought

a stone rolling, which should make him realize that he should probably do something better

should have taken it easy and trusted the work of my agency.

I must at this point clarify that I am not solely based on the mere

Existence of one or more video cameras already with detailed legal information

accusations seen to those responsible. which are imposed on me by law

enforced impartiality requires it rather, the person responsible first opportunity to

comment on the facts presented to me. In addition, in the

shown only too often in the past that the facts of the complaint presented themselves differently than they did

the petitioners presented to me and when it first appeared to me.

Back to the specific case: the following day, the managing director of the

said company by telephone to the complainant and attempted to explain to him that

the company is not (any longer) the owner or user of the property in question and he

follow also could not answer the request for information. What followed was obviously a

Verbal exchange of blows in which the complainant with his data protection

Tried to score points for knowledge. On the same day he wrote a written summary

recorded the telephone conversation and sent it to the e-mail address of the business

leader. In an instructive manner, he renewed his request for information. the

managing director, however, repeated his previous telephone argument by e-mail, according to which

the company is not the owner or user of the property in question and therefore neither is he

could not give any information.

The managing director then in turn researched the complainant. Since last

who also acted as data protection officer for other companies, he quickly came across

his employer. Its business area extended to data protection issues, which

112

3.3

Managing Director has a questionable business model in this respect and a professional

connection. Accordingly, he assumed that the employer also

was informed about the previous "exchange of blows". So he felt compelled to

via e-mail to draw attention to the "leisure activities" of his employee. Equal-

probably this had no knowledge of the private activities of his employee, which led to further

Entanglements and mutual accusations - I will refrain from details on this one

Body - the now three people involved and an extended complaint of the employee

beiters led to me.

It remains to be noted that my authority ended up with a complicated, almost without reason

Mixture of personal misconduct, quasi-regulatory behavior, data

intellectual property and also civil law issues have been confronted, which

would not have arisen if the complainant had merely waited. In addition

This procedure results in further data protection conflicts, such as the inclusion

of the complainant's employer, was downright provoked. A simple look

in the commercial register would have made it known that the information to be found on the Internet

were no longer up-to-date and the security company was named as being responsible

had relocated their place of business years ago. That would have avoided all the excitement

been.

I have made it clear to the complainant that he is clear about the objective in this matter

has shot out and data protection, for which he himself worked professionally, none

has done good service. Nevertheless, and despite all the annoyance, the supervisory case was over

also for the managing director of the security company reason and opportunity to get to know each other in more detail

with the data protection requirements also placed on his company, in particular

special the right to information according to Art. 15 DSGVO and the admissibility of data transmission

gene to deal with.

As far as the trouble-making CCTV cameras go, I have them

identify current property owners and be able to ask about the facts. As he me

announced that the cameras were already present when the property was purchased, however

the connection cables would be severed and otherwise there would be no more in this regard

Technology, therefore it is a matter of dummy cameras. He would like the complainant

invite you to a cup of coffee in his nearby commercial establishment.

I passed this on to the complainant, but have no knowledge of it,

whether a meeting has taken place.

3.4

Right to Data Portability, Miscellaneous

3.4.1

Transmission of the payslip

As part of a complaint, I was confronted with the question of whether employees

through their employer a right to the creation and transmission of the payslips

information in machine-readable form.

According to Article 20 of the General Data Protection Regulation (GDPR), the data subject has the right

the personal data concerning you that you have provided to a person responsible

has to receive in a structured, common and machine-readable format.

I informed the petitioner that such a claim against the (former) worker

donor does not exist. The transmission of the pay slip is in machine-readable form

not subject to the right to information within the framework of Art. 20 GDPR, because this data

are not made available to the employer by the employee concerned, but

the employer creates independently - only using the employee data - the

payroll and uses information from the employee, among other things.

114

4.1

4

Obligations of controllers and processors

4.1

Responsibility for processing, technical design

4.1.1

Website testing tools and operator requirements

from websites

I still get a high number of complaints about websites. Typical loading

serious issues are opaque data protection declarations, complicated, misleading

Changing or missing cookie banners or data transmissions without consent in insecure

third countries. I investigate all complaints and regularly check websites

her behaviour.

One of the most useful tools is the one developed by the European Data Protection Supervisor

Evidence Collector website, available at edps.europa.eu. The tool is as open source

Software designed and freely available. The developer is also open to suggestions and additions

openly or the tool can be used for your own purposes with the help of scripts

be matched. The Website Evidence Collector is used by me during tests in a laboratory

application on a Linux workstation. The tool is given the address of a

handed over to the website to be checked and in the background the website is checked by a Chrome

Browser surfed with empty user profile. The Website Evidence Collector creates an audit

protocol. This results in all connections of a website to other websites - with

for example to advertising networks, social media, fonts hosted by third parties – as well

all web storage objects stored in the browser (cookies and DOM storage). Additionally
Screenshots of the site are made and all objects in a report and a local
Storage summarized. The tool thus makes the checking of websites very efficient
cient. The results are then evaluated and checked to what extent for each detected
Connection to third parties, which means data transmission of usage data such as the IP address of the
corresponds to the user, and for each cookie or web storage object, which creates a profile
believes there is a legal basis.
A look at the data protection declaration does not help in many cases. Unfortunately I experience it
quite often that test results and thus reality have little to do with the more or less literal
have to do with richly designed data protection declarations. Either the involved
Services are not named at all or services are named that are not listed on the website at all.
are bound. Or a few general statements are made about the use of cookies
met, which is not true in most cases when you take a closer look at the website.
Such a privacy policy is unlawful.

The same applies to data connections and web storage for which consent is required.
If such information appears in the Website Evidence Collector, there has been a violation of the law
since the tool surfs to a website without interaction and therefore does not give consent
can be. In practice, I often experience those responsible who are not even aware of the violations
are aware and as a rule endeavor to remedy the violations that are the subject of the complaint. The-
I can still only recommend to everyone responsible that their own website and data
subject to a critical examination of the data protection declaration. A website can be created by anyone
are checked and is often the first contact with a customer or citizen. If one
If a knowledgeable visitor notices data protection violations at this point, the first
pressure already clouded. Especially if a privacy policy with the standard phrase

"We take the protection of your personal data very seriously!" begins. Lots of complaints

me are avoidable if the subject of the website is taken seriously. Next to the site

Evidence Collector, I use other tools such as the Burp Suite or those available in browsers

Analytics tools to generate snippets of data and website behavior

to investigate.

On the admissibility of data connections and the setting of cookies and web storage

objects, numerous references can be found in the guidance provided by the supervisory authorities for

Providers of telemedia, available at datenschutzkonferenz-online.de. Especially for the

set of Google Analytics, the supervisory authorities have drawn up information, which also

can be accessed on the website of the data protection conference. A reading recommendation

I would also like for the FAQ of the State Commissioner for Data Protection and Freedom of Information

of the State of Baden-Württemberg, the error that is often encountered in practice

and

under

baden-wuerttemberg.datenschutz.de.

avoidance

vivid

represents

available

whose

With regard to the judgment of the Federal Court of Justice of May 28, 2020 in the proceedings of the Federal

of the Association of Consumer Centers against the address dealers and lottery operators

About active Planet49 GmbH is in particular when using cookies or web storage ob-

Projects that allow potential profiling, according to the current situation, always require consent

necessary (cf. 9.4).

4.1.2

Standard Data Protection Model (SDM)

In 2020, the SDM sub-working group started to develop building blocks, which in the year

2018 initially as test modules by some of the supervisory authorities actively involved in the SDM

authorities were published, to submit to the data protection conference (DSK) and thus one

to achieve a broad consensus in the application. In 2020, a total of seven construction

stones are passed and published:

116

4.1

•

•

•

•

•

•

•

Store

Document

To log

Separate

Extinguish

Correct

restrict

Due to the chairmanship of the technical working group of the DSK, these are available on the website of the

State Commissioner for Data Protection and Freedom of Information Mecklenburg-Western Pomerania in each

to find the current version: datenschutz-mv.de

The modules cover process-critical components of processing in addition to

methodological part of the SDM with suitable measures and instructions on how to proceed

and can thus establish a holistic data protection management system described in the SDM

help.

In 2020, several data protection concepts based on the SDM are available to me.

accepted. It became clear that part B of the SDM in particular,

requirements of the GDPR, helps controllers to meet the complex requirements of the

GDPR to apply to a specific procedure and thus a verifiability of a processing

to produce.

4.1.3

"Autofill" function - default setting for e-commerce sites

The customer of a shopping portal turned to me with an observation that preset and

"Autofill" function that can only be deselected manually (automated filling in of data

support) regarding me. With the consent of a friend who was also affected

enter their e-mail address and postal code on their end device and receive the complete one

address, date of birth and telephone number of their acquaintances. i had this

then checked and can see that this is indeed server-side with no binding to

a suitable cookie could be issued on any end device. Condition

was only that the "Autofill" function was not canceled when the authorized person entered it for the first time.

had been chosen.

As a result, a data protection-compliant conversion was made for the shopping portal

men. Without cookies already on the device, no automatic

cal pre-filling or greeting by name no longer takes place.

It cannot be ruled out that default settings will also be used on other portals

come. With Art. 32 General Data Protection Regulation, such processes cannot be included

reconcile. Affected persons are advised to use E-Com

merce appearances initially deal with their own technology and the functionalities of the provider

to become more familiar with.

4.1.4

Authentication via IBAN when calling

meter reading message

The actions of a utility company were the subject of a complaint from a

met person who wanted to communicate meter readings himself by telephone. From the service person

of the company, they were asked on the phone to provide their full IBAN

that. Alternative ways to determine the authentication are not offered to her

been made and reference was made to internal instructions.

When I asked, the company confirmed to me that the full IBAN as

suitable instrument for the authentication of the registering and contractually responsible

authorized customers will be checked by the service center and that, for example, the last four

digits of the account details were found to be insufficient. However, the

grievance process does not correspond to the internal instructions according to which customers who

object to the comparison of the IBAN, a substitute criterion (e.g. the amount

of the monthly payment) should be offered. The company gave me one

renewed clarification to the service staff and in a later implementation

reported that due to my involvement, it was fundamentally again about the

I have dealt with the topic and as a result have reduced the IBAN query (to the

last six digits).

That the requirements for the authentication of telephone subscribers in the course of new

First decisions by supervisory authorities and case law in the direction of increased security

It is hardly surprising that safety can be adjusted. Checking the IBAN for the last four

Restricting digits is probably not enough due to the widespread use of this masking.

In principle, however, in the case of data that is perceived as sensitive, only one additional sufficient partial data set can be queried. On the other hand, on the customer adherence to access to complete information, to the function and the tasks scope of work of the employee arrive. Should callers be able to get from a single contact person - for example with regard to updating master data full insight into the customer data is required. So much for graded access to customer data has been implemented, there will also be a reduction in the visible IBAN six digits preferable.

118

4.1

The topic of a secure and at the same time data-saving authentication in the customer fidelity is also currently the focus of the data protection supervisory authorities and the judge (cf. 9.5 on the decision of the LG Bonn of November 11, 2020 - 29 OWi 1/20).

4.1.5 WhatsApp group in sales structures with integration self-employed

A self-employed sales employee of a company had presented himself to my authority about complained that all of this company's self-employed sales force in joined a chat group run by a prominent messaging service provider to connect there to exchange degrees.

The professional use of messaging services is fundamentally problematic. if however, as here, it is a voluntary (!) participation of the self-employed, nothing to object to initially, as long as the actual prerequisites for an informed informed and voluntary consent. In addition, customer data was also affected because the shared information sometimes includes client names, addresses, and order lumina comprised. Such personal data are fundamentally subject to the protection and must be adequately protected accordingly.

However, this protection is not absolute, but has to do with the specific risk

tential for those affected. Here was a default of the industry standard

appropriate end-to-end encryption so that only group members can

speaking data. The classification of such data processing

depends crucially on the information content and the sensitivity of the processed data

as well as the risk potential for the data subjects arising from their specific processing

to. In the present case, it was decisive that only rough data on solar installations was affected

fen were, which at best allowed very little conclusions to be drawn about the persons concerned.

A team-internal exchange of rough information on customers of a joint order

geber can be customary in the industry and, in my view, is not objectionable insofar as it is

only slightly sensitive data of the economic sphere is involved, the mis-

risk of use remains limited. However, the resulting data protection regulations are

to contain risks through technical and organizational measures by the person responsible,

in particular, the participating self-employed are to be made aware of data protection law.

4.1.6

Reimbursement of travel expenses: handling of insured data

health insurance

The handling of personal insured data by the person responsible, here a

statutory health insurance, was the subject of an inquiry as part of the application for

Reimbursement of travel expenses in connection with inpatient treatment.

Regarding the facts: The form for reimbursement of travel expenses is primarily used,

if insured persons make reimbursable trips, as here in connection with an inpatient

your stay, use public transport or a private car. It

may the medical confirmation on the back of this application, at which treatment

gene which means of transport was medically necessary to determine the reimbursement amount

to be able to determine.

For service reasons, the application is already filled with the insured person's data: name, address,

health insurance number.

The insured person fills out the front page himself. The possibility of the health insurance company

automatically transfer the customer's saved bank details to the form,

stands and is primarily in the branches with personal delivery to the customer or

used when requested by telephone. The application is only available on the health insurance company's website

available as a blank form. If the application is sent by post, the insurance

crete a cover letter and customer information.

The reimbursement form, pre-filled with the data of the insured person and bank details

Only the insured person or his or her supervisor or authorized person receives the application

yourself, not the doctor or any other medical institution on the part of the health insurance company.

According to information from the relevant health

kasse the advantage that fewer third-party recipient bank details are given, the

Bank details for the clerk have been checked and correctly documented and the (administrative

leg) reading ability is increased.

After notification by the health insurance company, customers can then decide for themselves whether they

whether you want to pass this application on to the doctor treating you or not. In addition, can

- according to the information from the health insurance company - the insured person, for example, his bank details

Make unrecognizable or request a blank form from the health insurance company before

he passes the application on to third parties.

As a result, the health insurance company only sends the pre-filled form to the customer

made available to and not to a third party.

120

4.2

Due to the course of action thus placed in the decision of the insured person, I have

no data protection concerns were raised against the procedure. Like that

Insured has concerns about the use of a pre-filled form, I suggest

proceed as described by the health insurance company.

4.2

Jointly Responsible

4.2.1 Joint controllers for video surveillance in

soccer stadiums

Higher-class football clubs (from the regional league) are due to association requirements

moderately required, also video surveillance systems in the stadiums used by them

to keep.

In a specific case, with regard to the content of this

regarding information signs to clarify the question of who is responsible on these signs

is to be named.

Given the circumstances that the clubs often do not own their - even for

other events used – are venues, whereby it is usually also used in addition to the owner

there is still an operating company, and on match days there is also the police in the

Operation of the video surveillance systems, at least in the use of the video recordings,

is involved, there is in relation to the question of who is responsible in each case or in general in the sense

of data protection law is not a universal answer.

In the case before me, the football club was only a tenant in the stadium. at

own events or events that are not accompanied or led by the police

the owner or his operating company the video surveillance

situation itself. If the police are involved, for example at soccer games, the system

use and control exclusively by the police. For the records, in particular

However, the operating company remains responsible for their security and storage duration.

wording. The video recordings are made by the police or the operator

society to prosecute criminal offenses or violations of the stadium regulations.

It should also be noted that the owner - represented by the operating company

regularly transfers domiciliary rights to the football club as the organizer of football matches.

Of course, he may also be interested in the video recordings, for example

if he is dismissed by his association as a result of incidents caused by his fans in prison

direction is taken.

121

Chapter 4 Obligations of controllers and processors

With the large number of participants (owners, operators, organizers, police), the

The question of who is responsible for video surveillance in terms of data protection

13 of the General Data Protection Regulation

(GDPR) subject. According to Art. 4 No. 7 GDPR, "responsible person" is the natural or legal

cal person, authority, agency or other body, acting alone or jointly with others

decides on the purposes and means of processing personal data.

Basically, the operator, the organizer and the police come first

under consideration.

However, the temporary transfer of domiciliary rights from the operator to the organizer means

not at the same time the transfer of responsibility for the operation of the video surveillance

plant. This remains with the operator on the one hand or goes into the relevant

On the other hand, some cases are also transferred to the police. Access to the video

drawings by the owner of the domiciliary rights to pursue their own purposes, for example to identify

cation and use of disruptors is possible and also permissible after consultation,

Article 6 paragraph 1 letter f GDPR. However, this does not imply any decision-making authority with regard to

the purposes and means of video surveillance (Art. 4 No. 7 GDPR).

For the rest, however, it is a case of joint responsibility of

drivers and police. As a special feature, it should be noted here that the owner in the application
area of the General Data Protection Regulation (GDPR) moved while for the police
the requirements of Directive (EU) 2016/680, i.e. the Saxon Data Protection Environment
enactment law (SächsDSUG) or the Saxon Police Enforcement Service Act
shall prevail. Within the scope of the General Data Protection Regulation is the
Joint responsibility regulated in Art. 26 GDPR, within the scope of the Directive
linie (EU) 2016/680 the regulation of § 19 SächsDSUG is relevant.
The joint responsibility must be evident from the signs pointing to the video surveillance
emerge. A variant would be a special sign only for the police
Video surveillance and thus only related to certain events, which is practical
tical questions fails. On the one hand, this led to a rather confusing double sign
change, because the operator must of course also provide information about his video surveillance,
on the other hand, the cases of (also) police video surveillance are not present
so clearly definable and predictable. In particular, they were not limited to football
games of the main stadium tenant. Only temporarily or event-related visible
Signs that had to be made cash were rejected by those responsible because they were impractical
excluded. An information sign was therefore preferred as a solution, which both operators
ber and the police as responsible.
As jointly responsible, the operator and the police also have the resulting from the
General Data Protection Regulation or the Saxon data protection implementation
to fulfill the obligations resulting from the Federal Act. This also means that affected

4.2
persons in the exercise of their rights do not mutually distinguish between the two
verbatim may be referred, even if the responsible person addressed
objectively does not see a right to fulfill the rights of the data subject (cf. Art. 26 Para. 3 GDPR,

§ 19 sentence 4 SächsDSUG). The jointly responsible persons have the realization of the
To organize the rights of those affected internally and to accept incoming requests in this regard
if to be forwarded to the other person responsible. Affected persons are free to choose
which person in charge you should contact with your request. A corresponding
A closing agreement according to Art. 26 Para. 1 GDPR is also required for this.

4.2.2 Joint Controllers: Owner and Property Manager

A property manager of an owner-occupied facility presented me with a request for advice
draft of an "Agreement on the joint processing of data
Art. 26 GDPR" between owners and property management should serve. In it they should
Owner for the "Purpose of Joint Processing of Personal Data" below
inter alia, to take over a relevant remuneration in favor of the administrator
will. Another contractual provision contained the clause according to which the parties
according to Art. 82 Para. 5 DSGVO would have to be liable according to their shares.
I asked the property management to give up the project and pointed out
that the property management of a homeowners association is solely responsible
licher for the processing of personal data in connection with the activities
is that were transferred to her from the property management contract. This also applies regardless
gig on whether it is the management of community or private property.
That the community referred to in the Law on Home Ownership and Permanent Residence
The association of the apartment owners is the data-processing office and responsible
applicable. However, this uses a resolution pursuant to Section 19 to appoint an administrator who
che tasks for the community of owners or the individual owner
perceives independently. The owners thus transfer this responsibility to the
manager. He is therefore also solely responsible under data protection law for those with his
activity related data processing. Joint responsibility according to Art. 26
GDPR, on the other hand, is characterized by the fact that those responsible jointly

determine the purposes of the processing and the means used for this purpose (cf. briefing paper no.

16

on

datenschutzkonferenz-online.de, Art. 26 GDPR). Such a connection, which also leads to

would lead to joint and several liability, the relationship between owner and property manager

but just not. The owners also continue to process personal

collected data for their own purposes and separated from the property management.

- Together

Responsible,

processing

available

the

for

123

Chapter 4 Obligations of controllers and processors

As a result, this assessment applies not only to the WEG administration, but also to the

contractual management of other real estate.

A conflicting decision by the District Court of Mannheim is not convincing in the

Reasons (cf. AG Mannheim, judgment of September 11, 2019 - 5 C 1733/19).

4.2.3

Lettershop process - no joint controllers

Occasionally, the opinion is held that clients and advertising letter senders

be jointly responsible.

The so-called "Lettershop" procedure is a process in which the

Client of an advertising broadcast the contractor who entrusts "Lettershop" with it

to personalize the shipment. In some cases, the clients provide the data of the customers or

address details available. In some cases, however, the advertising company does not have any
the address and communication data, but only the contractor who does the labeling
carrying out envelopes or sending an e-mail to addressees or
this temporarily receives the addresses from a third company.
I regard the division of labor and the distribution of personal data as im
Basically privacy friendly. However, it is also a prerequisite that the information
mation obligations are complied with and data processing, which the individual responsibilities
wording of the data processing bodies is made transparent. Otherwise
affected persons can be found in view of the distributed tasks of the companies involved
not right and are then unable to exercise their rights as data subjects, in particular information
and to object to commercials (cf. Art. 15 and 21 Para. 2 and 3 Da-
General Data Protection Regulation (GDPR)).
Nevertheless, in my opinion, problems that arise cannot have a constructive
joint liability or Art. 26 GDPR can be dissolved, so that an
Finally, in addition to the address pool, the person responsible also has the non-data
working position can be claimed. One from a personal
Data processing decoupled data protection responsibility knows the data protection
basic regulation does not. The person responsible is solely who meets the requirements according to Art. 4 No. 7
GDPR fulfilled. Jointly responsible are those involved in the "Lettershop" procedure
On the other hand, do not regularly post. However, other civil law attributions can
may be more extensive.
However, it is advisable for the bodies involved in the "Lettershop" to make procedural agreements
to respond to the concerns of those affected in order to ensure the best possible and most effective
ensure processing.
124
4.3

4.3

order processing

4.3.1

Commissioning of an IT service provider by the municipality

A municipality consulted me on the need for a data protection regulation

when hiring an IT service provider. The intention was to introduce such a

To contractually bind maintenance and care as well as expansion of the IT infrastructure. Next to the

“normal” service descriptions, there was also a misrepresentation in the contract offer

safety obligation integrated, at the same time an obligation to comply with data

protection law due to the processing of personal data.

From the point of view of the municipality, it was now questionable whether the confidentiality obligation

is sufficient. This was justified by the fact that the service provider does not collect any personal data

should process data, but only the insight into this data, due to the above-described

bene services. They therefore do not want to end the contract with unnecessary

successfully overloaded.

In my answer I pointed out that according to Art. 28 Para. 3 b General Data Protection Regulation

must be guaranteed in a contract for order processing "that the processing

processing of the personal data has committed persons authorized to confidentiality

or an appropriate legal duty of confidentiality”. This applies

even if the order is not aimed at the processing of personal data

is, but the (technical) possibility of processing personal data exists –

to ensure data protection in these cases as well.

The mayor sent me a "thank you very much for the quick reply" and

shared, "That helped us a lot." So I'm assuming my response to that

conclusion of the contract has been taken into account.

4.4

List of processing activities, cooperation

obligation with the supervisory authority

For the list of processing activities, see the article under 1.2 on implementation

the documentation at municipalities.

Art. 31 General Data Protection Regulation (GDPR) standardizes a general obligation of

Responsible and the processor to cooperate with my authority.

Supervisory procedures are regularly followed by my department with an informal

Request for information or comments initiated. In individual cases it is also direct

a note. Only in the case of serious violations or if the person responsible for

Processor does not provide the information necessary to fulfill my task,

what happens in rarer cases, my authority arranges by way of

administrative act with a formal notice of engagement. Overall, it can be stated

that the obligated bodies make an effort and behave in accordance with the norm. Although a violation of

Art. 31 pursuant to Art. 83 Para. 4 Letter a (GDPR) subject to a fine. However, on the part of

my department has not yet initiated any administrative offense proceedings.

4.5

security of processing

4.5.1

Data protection-compliant disposal of devices in medical

area

A freelance midwife asked how she used her professional technical devices,

Dispose of or secure smartphones, laptops, etc. in accordance with data protection regulations

personal data can be deleted in accordance with data protection.

I informed her that if these devices were to be discarded, appropriate measures would be taken

must be taken for data protection-compliant disposal (cf. Art. 5 and 32 data protection

basic protection regulation).

If personal data without health reference and with

stored at a manageable risk, deletion will take place in individual cases according to the state of the art

nik and the subsequent possibility of a transfer (e.g. sale) in question. This

(e.g. for smartphones) if necessary with the involvement of a service provider

be accomplished. For more detailed information, I have referred to the relevant information

ons of the Federal Office for Security in Information Technology.

For data carriers on which health data is processed, it is usually risky

to adequately use a professional data medium destruction and the destruction

to be documented accordingly. Corresponding service providers are available on the market.

However, for competitive reasons, I cannot recommend specific companies

pronounce. However, the service provider should at least comply with DIN 66399 "Office and data

technology – destruction of data carriers" and protection class 2/security level

4 can offer.

In general, full encryption of all personal data involved in the processing

recommended to carry in case of unplanned loss (e.g. theft/burglary)

to have taken appropriate precautions.

126

4.5

4.5.2

Use of private messenger accounts and private

end devices for professional purposes

Employment Type

New communication methods are increasingly being used by companies. Of the

The use of such funds by the self-employed or small traders should not

be based on the following consideration (but cf. 4.1.5 on a WhatsApp group
in sales structures for the self-employed). I had already signed up for messenger
services in the school sector (cf. activity report 2019, 4.1.2., page 79 ff.)
In the last reporting period, I was also confronted with the question of whether the deployment
private messenger accounts and private end devices, smartphones and tablets, for business
personal purposes by employees in companies is permissible. Here you will communicate
tion without further processing of personal data of data subjects, e.g
in a vote on internal personnel planning, from a more in-depth information
have to distinguish processing. Promoted messenger communication via pri-
vate systems with the associated possibility also file attachments and voluminous contents
processing, at least from a technical and organizational point of view, ensures
security issue. Those responsible must ensure that access to personal
Employees entrusted with personal data are not able to transfer data that is worthy of protection
to transfer their private systems and infrastructure.
In addition, employers or principals are fundamentally responsible
obliged to provide the employees with the necessary work equipment. will ar-
Infrastructure that meets the information security requirements of the employer
set up, this is basically not objectionable. Outsourcing of data processing
processing on private devices, on the other hand, which would also lead to information being
private phone numbers and accounts of the employees are also processed, but it is
moderately not required and permissible. Insofar as they are agreed and
is owed, this must be considered in more detail in the specific case and in terms of data protection law. In each
In this case, the use of private end devices provides particularly sensitive data
are processed by those responsible, for example in the public service or in the nursing
and hospital area, a serious technical-organizational and information
security defect (cf. Art. 25, 32 General Data Protection Regulation (GDPR)).

If private end devices are used and are then or via private measurement

Closer accounts personal, subject to confidentiality or particularly sensitive

processed valuable data within the meaning of Art. 9 GDPR, the person responsible goes to the

Controlling and monitoring the processing of the data entrusted to him and the system security

safety. Especially in the field of health care or other areas where

sensitive data are processed, according to Art. 5 GDPR this must be excluded.

When using private equipment, there is also the problem that, if necessary

it would be necessary to check employees' private end devices in order to implement a data protection

to ensure and control the fair handling of personal data. Included

would have to access the private end device or private

created accounts, in turn, the data protection regulations for employee data

protection, in particular with regard to the principle of the lawfulness of data processing

tion, the voluntariness of consent, behavior and performance controls as well as the

existing information and disclosure obligations are complied with. In addition, a responsibility

literalness of the employees within the meaning of Art. 4 No. 7 of the GDPR for the corresponding

exclude data processing.

My authority does not consider the same with private end devices and accounts for data

can be implemented in a protective manner.

4.6

Data Breach Reporting

4.6.1

Increase in reported data breaches

According to Article 33 of the General Data Protection Regulation (GDPR), those responsible are obliged to

In the event of a breach of the protection of personal data, immediately and if possible

to report the violation to the supervisory authority within 72 hours of becoming aware of it,

unless the personal data breach is unlikely to occur

results in a risk to the rights and freedoms of individuals.

I received 635 such reports in the reporting period. Compared to the

year under review, this corresponds to an increase of more than 40 percent. With that he-

has again seen a significant increase in data breach notifications.

635

450

700

600

500

400

300

200

100

0

227

2018

2019

2020

Figure 6: Data breach reports

128

4.6

The following groups of cases were reported particularly frequently in the reporting period:

wrong shipment

The incorrect dispatch of documents due to incorrect assignment, incorrect enveloping or

Mixing up the recipient is still one of the most common case groups that

is reported to me in accordance with Art. 33 GDPR. It is critical to note that in this category

of the case groups often health data are affected, which are sent to the wrong recipient

will. Especially in the area of health data, due to the high sensitivity of the

data and the special confidentiality, a particularly high degree of care

to be requested from the responsible body. However, there is a high risk for those affected

fortunately not usually found since the wrong recipients do this regularly

notify the responsible body, destroy or return the documents and

so that the consequences for those affected are kept within manageable limits.

Open mailing list

The open e-mail distribution list is still the classic data breach.

Even if the risk for those affected is generally considered to be quite low

such a data protection violation must be reported under Art. 33 GDPR because

the General Data Protection Regulation a potentially non-reportable low risk

just don't know. The notification according to Art. 33 GDPR is only unnecessary if with

the data breach is not expected to pose a risk to the rights and freedoms of natural

Persons would be connected, which cannot be ruled out, however, if

the e-mail address is made up of the first name and surname before the domain name

and for their transmission, depending on the group of addressees, regularly none

legal basis is given.

lost in the mail

A notifiable group of cases that occurred to a particular extent in this reporting year

is the loss of documents in the post

the fact that this case group primarily appears in the area of banking

tion has occurred, which may have special consequences for the persons concerned

can. If such a problem becomes known, here is a critical assessment of the

shipping service provider offered.

burglary and theft

Another frequent case group of reports of data breaches are intrusions

and thefts. This case group is particularly problematic because it is in the area

of criminal acts and the associated risk for the persons concerned

is particularly high. Within the scope of this case group, the technical and organizational measures

required to keep all data carriers properly and regularly

Carry out backups to ensure the availability of the data through the possibility of

to ensure production. In addition, personal data are stored on digital data

data carriers through suitable encryption. The functionality of the full

Hard disk encryption is already integrated in many operating systems today, so that in

In many cases no additional special software would be required.

cybercrime

Another group of cases is summarized under the general term of cybercrime.

takes. This very unspecific term generally includes all acts/penalties

committed through the use of communication and information technologies

the. Typical fields of action are the encryption and tapping of personal

data from e-mail inboxes, from servers or other data carriers. in particular

particular in the field of cybercrime, with regard to the necessary technical and organizational

Toric measures to attach particular importance to information/data security and

always sensitize the people involved.

In order to avoid reporting cases, it is necessary to always deal with possible technical and organizational

to deal with torical measures for the protection of personal data, which

to implement necessary measures accordingly and to keep them up to date. So-

as far as the reporting cases are due to human error, it is always necessary
to sensitize the people involved with regard to corresponding sources of error and -
as far as possible - to implement technical and organizational precautions to avoid
mention.
Furthermore, I would like to point out the accountability that exists in principle
according to Art. 5 Para. 2 GDPR in particular for the reporting cases existing documentation
obligation according to Art. 33 Para. 5 DSGVO as well as the possible obligation to notify the
data subject according to Art. 34 GDPR.
In connection with reports of data protection violations, I was under
among other things as follows in an auditing and advisory capacity:

4.6.2

Cyber attack on high-performance data center

The operator of a high-performance data center reported in the reporting period that the compromise
averaging multiple systems. Using a previously unknown vulnerability
as well as by using stolen SSH keys and access data, the targeted
Installation of a backdoor by an attacker. In addition, a worm-like spread
of the attack between several high-performance data centers in Europe.

The person responsible has been informed of the existence and potential exploitation of the vulnerability
informed by the manufacturer of the software system. As part of a related forensic
The compromise was determined by a technical analysis. The person in charge responded
Measures to eliminate the vulnerability. As part of a comprehensive IT security
security management process, the affected systems were analyzed and my authority
informed.
The incident was evaluated in detail in an on-site appointment. In particular,

the determined course of infection as well as measures for restarting and prevention

discussed.

The target of the attack was not primarily personal data. On a system became a

so-called crypto miner discovered. Cryptocurrencies are experiencing increasing popularity

and have also been used as objects of speculation for some time. Regarding spectacular value

and anonymity when creating and using blockchain-based currencies

is a high incentive for cybercriminals.

Digital currencies are generated by computationally intensive cryptographic calculations.

By using very large computing power, it is possible to generate digital values.

Cyber criminals aim to infiltrate crypto miners into powerful

Data centers to generate digital values. The cost of generation as a result of that

Energy costs, the use of hardware and software and the qualitative impairment of the IT

Services are borne by the operator of the compromised data center.

4.6.3

Vulnerability in university information system

Several universities reported a software vulnerability in the operated university information

mation system. The reports did not allow a clear conclusion on the mode of action of the

vulnerability and risk assessment.

As part of an on-site appointment with one of those responsible, the basic work

architecture and infrastructure of the university information system. From this could

Conclusions can be drawn about the impact and risks of the vulnerability.

Basically, it was determined that the vulnerability was fixed by the manufacturer within the scope of its own

quality control was revealed. The affected customers were informed by the manufacturer

formed and a corresponding security patch made available for troubleshooting.

None of those responsible are aware of any actual exploitation of the vulnerability

become.

An information obligation according to Art. 34 General Data Protection Regulation was not determined.

Nevertheless, those responsible were recommended to inform those affected about the discovery of the

To inform vulnerabilities and their elimination in a general framework - in the spirit

a transparent information policy.

The responsible state ministry was asked to provide for all facilities in the business

to check and ensure that the affected university information system is used

len that the vulnerability in all responsible by installing the provided

security patches is closed. A corresponding execution was reported to me.

4.6.4 Open Web Server

A media company reported a data breach to me, stating that the syntax of a

Release links could be traced and by changing the release link the assignment

Access to data from third parties on the web server of the person responsible was possible.

The entire problem could be discussed at an on-site appointment. It turned out

out that the data stored on the web server is not unprocessed

were no longer raw data, but rather processed data provided by the data subjects

should be released for publication. So that was the data breach

associated risk should no longer be rated as high, but rather as low. It

was discussed with the person responsible that the technology used does not require user authentication

tification and the syntax of the release link could be understood without any problems.

could. The technical and organizational requirements were therefore not met. the

responsible informed that after becoming aware of the vulnerability, the web service immediately

had switched off. During the on-site appointment, we discussed the future data protection

compliant implementation of the web service. The solution envisaged a user-related release.

In addition, it was guaranteed that the syntax of a release link could no longer be traced

could become.

4.7

Data Protection Officer

Compare the contributions under 1.2 and 2.1.2 as well as the statistical information under 6.2.6.

4.8

Code of Conduct and Certification

4.8.1

On the status of accreditations and certifications

With Articles 42 and 43 GDPR, the General Data Protection Regulation (GDPR) has the basic

for a uniformly regulated certification of products, processes and services

genes for the processing of personal data and thus the allocation of data

protection seals and test marks created. In this way, the data

protection compliance of the processing of personal data is guaranteed. For

By using a data protection seal or test mark, data subjects are given a

cal overview of the data protection level of relevant products and services

possible and compliance with the applicable data protection law is visible. But also for

The choice of service providers to be involved as well as their own

accountability with regard to compliance with applicable data protection law.

Certifications and thus the award of data protection seals and test marks in the area

of the General Data Protection Regulation require prior accreditation of the certification

place. In Germany, this is done by the responsible German accreditation body

GmbH (DAkkS) in cooperation with the German supervisory authorities. An overview with

further information as well as a comprehensive description of the entire accreditation

process can be found on the DAkkS website: dakks.de

At the beginning of the reporting year, an agreement was reached between all German supervisory authorities

administrative agreement in order to cooperate within the scope of the accreditation

to regulate the process. This includes, among other things, the composition of committees that

Possibility of mutual support as well as the Germany-wide validity of certificates

decorations, data protection seals and test marks.

Furthermore, the accreditation

tion requirements as supplements to DIN EN ISO/IEC 17065 and according to Art.

64 GDPR for an opinion to the European Data Protection Board. the

approval procedure could be successfully completed, so that for the accreditation

supplementary requirements are now available. The PDF document can be

datenschutzkonferenz-online.de can be downloaded.

The German supervisory authorities are planning a document as an aid for 2021

for certification bodies and program owners to be completed, which contains the minimum requirements

genes of certification criteria. This document is also submitted to the German supervisory

authorities as the basis for a uniform assessment and approval of certification

serve program.

There are currently several certification programs at DAkkS or the responsible

authorized regulatory bodies for program review and approval of certification criteria

before. Such a procedure has not yet been initiated for my area of responsibility. Bun

Furthermore, it can be assumed for 2021 that the first accreditation procedures will be completed

s will be and accredited certification bodies with the certification of responsible

and processors will begin.

Chapter 5

International traffic

5

International traffic

5.1

Consequences of the decision of the European

Court of Justice on international data transfer

The decision of the European Court of Justice of July 16, 2020 - C-311/18 - ("Schrems

II") has for the data processing processes in particular of the companies that have been on

basis of the Privacy Shield personal data to the United States of America

rika have transmitted decisive effects. These companies should focus on

Setting up and changing standard data protection clauses.

But also the use of the standard data protection clauses are, according to the decision of the

a certain legal uncertainty by the European Court of Justice. So will the

Requires controllers and processors to check whether the law of the third country

des to which the data is transferred according to European law "appropriate protection of the

personal data transferred on the basis of standard data protection clauses

guaranteed" (see paragraph 134 of the decision). Nevertheless, due to

their business processes have no alternatives to the standard data protection clauses

have, since individual contracts or consent solutions from multiple practical

reasons should be eliminated. Relocations of data processing from the United

States and third countries in the European Economic Area are not easily

and can be implemented overnight. According to Art. 49 General Data Protection Regulation

(GDPR) provided exceptional conditions under which personal data in

are transmitted to third countries should not represent a broad solution.

The person responsible who cannot do without processing in third countries is

In this respect, it is advisable in any case to refine your data processing processes and to

European Court of Justice planned examination of the level of data protection in the third country

lize. Technical and organizational measures can be intensified in parallel if necessary

such as a reduction in the amount of data, the use of

encryption technique. The approach should be granular, like a data

protection and information security concept are documented.

The independent federal and state data protection supervisory authorities are involved

together with the other European data protection authorities on possible procedural

improvements and substantive solutions. A corresponding ad hoc working group has been set up

set up for this.

According to the decision of the European Court of Justice, the supervisory authorities are, too

my authority, although also obliged in the event of a complaint to

134

5.1

to examine the existing guarantees for data transfer (see paragraph 120 of the

manure). If necessary, insofar as there are no effective adequacy decisions

genes and no suitable guarantees allow data transmission, this according to Art. 58

Para. 2 letter f GDPR. According to the court, it can also be suspended in accordance with

Para. 2 lit. j GDPR to remedy the situation.

See also the entry under 9.3.

135

Chapter 6 Saxon data protection officer

6

Saxon data protection officer

6.1

Jurisdiction and Requirements for Complaints

6.1.1

responsibility of the Saxon data protection officer

the GDPR

More than two years after the introduction of the General Data Protection Regulation (GDPR),
by processing a wide variety of case constellations, the supervisory practice for determination
the lead authority within the meaning of Art. 56 Para. 1 GDPR already established to the extent that
to be able to draw at least a preliminary summary.

To determine the lead (domestic) supervisory authority, Section 40 (2) of the Federal
Tenant Protection Act, I already had statements in the 2019 activity report (6.1.2, page 111).
did. Art. 4 No. 16 Letter a GDPR, the idea of the location of the "main administration
tion" of a person responsible as a decisive assignment criterion. recital
Reason 36 of the GDPR specifies the “effective and actual exercise of
management activities”.

The supplementary explanation in the aforementioned recital suggests that so far in
the majority of the processes applicable domestic German criterion of register relationship
to question wise alleged headquarters in special cases. As is so often the case,
deep reflection when an individual case cannot be solved according to the conventional scheme
becomes. In the period under review, for example, I had several discussions with a subsidiary
which is based at the former seat of its (independent) predecessor as a corporation
community, but actually does little more than cultivate tradition there,
virtually keeps a golden company sign shiny, while the entire data processing on
The parent company is based in another federal state. An effective control
by me - if necessary with on-site inspection - in the sense of a responsible
Supervision was no longer feasible in this constellation.

That, as shown by the company, data from all companies and parts of the group
be processed separately and decide on the means and purposes of
processing meets each society for itself, says about the inner structure of a formally self-
permanent daughter alone is still not enough. Much more important is the place where the actual
che main focus of business and processing; often enough lies with the

Management of parent and subsidiary companies also propose a personal union. So was

it also in the process to be decided by me. The actual

Real business address, also in the data protection declaration and with the one for the location of the

Group address responsible data protection supervisory authority was able to reach agreement in

zug on taking over the processes can be achieved.

136

6.1

This type of company name was still an isolated case and a hitherto rare one

Exception. However, it affected a large company and a large number of people

sons. In this respect, it must be demanded that the person responsible in the data protection information

already provides clarity. It is also advisable to contact the responsible data protection supervisory authority

in the information to be provided in accordance with Articles 13 and 14 GDPR in order to

to avoid effort and time delays.

I had already commented on area-specific responsibilities (cf. on this

also activity report 2019, 6.1.1., page 110 f.). In accordance with Art. 85 GDPR,

member states to make their own regulations for the journalistic sector.

The Saxon legislature has this with § 11a sentence 4 Saxon law on the press

made use of and controlled according to the GDPR in data processing for journalistic

table and literary purposes only to a very limited extent. Because of this

mentioned media privilege and the continued case law of the Federal Constitutional

richts (see, inter alia, the decisions of November 6, 2019, 1 BvR 16/13 and 1 BvR

276/17) I do not consider myself authorized to post editorial content on rating portals

and control reporting appearances. If yes, the classification has journalistic

cal purposes without prejudice to quality or its consistency. This concerns

also requests for deletion of possibly outdated content. For certain circumstances

Also noteworthy is a decision of the European Court of Justice, which

bar of processing for journalistic purposes (European Court of Justice of 14.

February 2019, C-345/17).

Affected parties can also file their complaints - insofar as those responsible

subjected to control – also to the supporting association of the German Press Council e. v,

Fritschestrasse 27/28, 10585 Berlin.

In the case of the processing of personal data, the postal company is responsible

due to Section 42 (3) of the Postal Act and in the commercial provision of telecom

communications services based on Section 115 (4) of the Telecommunications Act at the Federal

commissioned for data protection.

With regard to the data protection declaration and the naming of the person responsible for Internet

offered, it should be noted again that the provider's obligation to provide information - "imprint obligation" -

to be distinguished from. For proper information according to the Telemedia Act,

related to Saxony, the Saxony State Directorate is responsible.

In cases where the controllers are within the scope of the data protection

Basic Regulation maintain no branch, I decree, also the market place principle

following mostly not about possibilities of intervention. Entries can therefore unfortunately

see of any advice I can give to data subjects, regulatory

be done satisfactorily.

Companies, clubs, associations, institutions of all kinds, in general: all of my data

Responsible persons who are subject to protective supervision can, within the scope of my advisory

according to Article 57 Paragraph 1 Letter l GDPR and Article 40 Paragraph 6 Clause 1 of the Federal Data Protection Act

contact me with their concerns. According to the wording of the Federal Data Protection Act

The advice only applies to company data protection officers. However, I am

Of course, we endeavor to answer inquiries from those responsible who do not have a

appoint a data protection officer.

However, requests for advice can only be processed if the person seeking advice

mentally recognizable. The advice of a person in charge who remains anonymous is mine

not possible. I therefore also ask of corresponding inquiries, which are often made by law firms

and data protection officer to me to refrain.

Also, I only advise those responsible in Saxony. Other requests, such as

which points to all supervisory authorities without the person responsible being located in the Free State

I regularly with reference to the responsibility of the respective data protection supervisory authority

away.

In my next job, I intend to

activity report in depth. First of all, only this: Those affected can contact the for

responsible authority (foreign authority) or in the federal state of residence

contact the supervisory authority (authority of residence) at the registered office of the person concerned. An overview of

Foreign data protection supervisory authorities can also be obtained via my website

rich. Complaints addressed to the Federal Commissioner with only

Country reference only have a transfer to the data

safety supervisory authority.

6.1.2

Factual incompetence in an online encyclopedia

I received a complaint about an entry on the dewiki.de website.

This website or the retrievable content is - similar to

Wikipedia – a freely accessible encyclopedia maintained by volunteers and volunteers

authors is created.

The petitioner complained that personal data concerning him were published on this website

ternet and the operator of the website sees no reason to delete it.

6.1

I had to inform the petitioner that I am not technically responsible and

Generic entries on this website essentially do not fall within the scope of protection of the data

General Protection Regulation (GDPR). I could therefore only refer the petitioner to the

Possibility of claiming civil or judicial legal protection

point out.

This notification was based on the following legal assessment: The protection of data protection

Basic regulation in favor of the individual concerned consists in questions of the informational

the right to self-determination or personal rights is not complete. That one-

The General Data Protection Regulation provides for exceptions to the material scope of application, such as

for example in Art. 2 Para. 2 GDPR. In particular, with Art. 85 GDPR, the European

legislator an opening clause with far-reaching leeway for national regulations

created to protect freedom of expression and information. The purpose is that the data

protection must not come at the expense of freedom of expression and information, since both

are legally protected interests.

According to the changed wording of Art. 85 Para. 1 DSGVO compared to the previous

9 of Directive 95/46/EC of the European Parliament and of the Council

of October 24, 1995 on the protection of natural persons in the processing of personal

gener data and the free movement of data, it is made clear that data processing also

do not serve privileged purposes, may still fall under Art. 85 GDPR.

For processing carried out for journalistic purposes or for scientific, artistic

or literary purposes, Member States shall provide for derogations or exceptions

Chapter II (Principles), Chapter III (Rights of the data subject), Chapter IV

(Controller and processor), Chapter V (Transfer of personal data

to third countries or to international organizations), Chapter VI (Independent

authorities), Chapter VII (cooperation and coherence) and Chapter IX (rules on special

their processing situations) if this is necessary to exercise the right to protection of the
personal data with freedom of expression and information
to bring them into line (Article 85 (2) GDPR). With § 11a Saxon law on the
The state legislature has implemented a corresponding regulation for the press. The rule
applies to “press companies”. However, I attach the scope due to the
Jurisprudence of the European Court of Justice (see also 6.1.1 on jurisdiction
of the Saxon Data Protection Officer according to the General Data Protection Regulation).
The literary purpose is also included in the privilege described above
been. According to this, data that is used exclusively for the production of fiction or factual
literature, excluded from the scope of the General Data Protection Regulation
men. The term "literature" is to be interpreted broadly and includes both scientific li-
both literary and entertainment literature. An online
Lexicon or encyclopedia maintained or published. This

counts as a reference work for non-fiction and is excluded from the scope of data protection
Basic Regulation largely exempt.
In the present case, it could therefore remain undecided whether the further privileges
according to Art. 85 Para. 2 GDPR, such as for scientific or journalistic purposes
purposes, also exist and therefore also the factual incompetence of my
hörde would justify.
See also activity report 2019, 6.1.1, page 110 f.
chemical background.

6.1.3

Change in regulatory responsibility for
Federal motorways and federal roads

The Fernstrassen-Bundesamt (FBA) is a new higher federal authority in the business area of the Federal Ministry of Transport and Digital Infrastructure (BMVI) and was in October Built in 2018. This independent supervisory and approval authority for the Federal Autobahnen und other federal trunk roads has its headquarters on January 1, 2021 fully recorded in Leipzig. Federal motorways are no longer commissioned administration by the federal states, but in federal administration. The FBA is essentially assume sovereign tasks and in particular the responsible hearing and planning approval authority in planning approval procedures for motorway projects in federal to be in charge.

As a result, the competence of the data protection supervisory authority changes. The regulatory Responsibility of the state authorities for data protection (e.g. the Saxon data protection officer) for the federal motorways, which in the respective federal state (here material sen) ended on December 31, 2020, as only up to this point in time of the federal motorways, the current federal order management by the federal states was standing.

Since January 1, 2021, the Federal Commissioner for Data Protection and the Freedom of Information (BfDI) data protection supervisory authority for federal motorways. Deviating from this, the Saxon data protection officer is responsible for data protection lichen supervisory authority with regard to the federal motorways, if for the decision in accordance with Section 74 (7) of the Administrative Procedures Act from the exemption pursuant to Section 3 (3) long-distance Federal Roads Office Construction Act is used and the state is therefore responsible competent authority, hearing and plan approval authority in plan approval procedures, plan approval authority is in the planning approval process.

140

6.2

For the federal roads, it remains with the order management by the respective federal states

the. Therefore, the Saxon data protection officer continues to

roads its supervisory authority for those federal roads that are

sen lie - even after January 1, 2021.

6.1.4

Collection area: minimum requirements for complaints

In the debt collection area, I receive constant complaints, which often have a concrete,

under any, data protection reference is missing. Instead, the petitioners regularly point out

point out that the contract on which an asserted claim is based is not

exist, be terminated or revoked.

In these cases, the complainant is regularly informed that the data

protection law is not an overriding consumer protection law, but expressly the legitimate

time privileged interest in enforcing claims - also and especially in

cases of doubt (Art. 18 para. 2 General Data Protection Regulation).

Of course, a detailed examination of substantiated complaints is carried out

to the possible breach of data protection obligations by those responsible.

These obligations also include at least a cursory check for plausibility and actual

physical existence of the claim. In the case of problems that have occurred before, the obligation to check can be

of the debt collection company can be increased (cf. Activity Report 2019, February 2nd, 2018, page 54 et seq.).

Insofar as the violation of debt collection obligations is reported or imposes itself

the person concerned is informed of the jurisdiction of the District Court of Chemnitz as collection supervision

sen The same applies to allegations or indications of criminal acts outside of the

data protection law.

6.2

Figures and data on activities in 2020

6.2.1

Overview of the main areas of work

For complaints and requests for advice, my department recorded the 2020

most processes – together around 43 percent. The statistics also reflect the

Technical and organizational work as chairman at the Data Protection Conference (DSK)

the. It accounted for almost a fifth of the transactions.

Noticeable compared to the previous year: There were more reports of data protection violations

according to Art. 33 of the General Data Protection Regulation (see 4.6.1). There was also growth

in international affairs. They mainly concerned the EU area.

Miscellaneous

3%

press inquiries

1 %

EU/International

10%

complaints

24%

reports from

Privacy-

injuries

12%

General

administration

13%

cooperation

with German

regulators

18%

consultations

19%

Figure 7: Main areas of work according to the number of processes

6.2.2

complaints and notices

The number of complaints remained at a high level in the reporting period. Since effective

of the General Data Protection Regulation in 2018, the annually received

the number of complaints and reports more than doubled. If in 2020 the entries in the non-

public sector, they increased significantly in the public sector compared to 2019 (Figure

8th).

142

6.2

1297

1247

1176

819

910

597

376

357

387

221

744

503

1400

1200

1000

800

600

400

200

0

2017

2018

2019

2020

public area

non-public area

total complaints

Figure 8: Complaints and notifications

1133

1019

834

687

446

384

446

608

368

240

185

1200

1000

800

600

400

200

0

62

2017

2018

2019

2020

non-public area

public area

consultations total

Figure 9: Consultations

143

Chapter 6 Saxon data protection officer

6.2.3

consultations

Compared to the previous year, consultations increased by 68 percent. The strong growth goes

exclusively on information from the public sector (Figure 9). This

were often related to the coronavirus pandemic. Some requests are

listed as an example in this activity report (cf., inter alia, 2.2.1 to 2.2.7).

6.2.4

data breaches

The reporting of data protection violations in accordance with Art. 33 GDPR has changed over the years

has increased steadily since the General Data Protection Regulation came into effect. Next to the registry

of the processes, the reports are to be evaluated and, if necessary, for a supervisory

to categorize rework. The article provides an overview of the content-related processes

4.6.1.

6.2.5

European procedures

The European data protection supervisory authorities regularly agree on cross-border

progressive cases. The Electronic Internal Market Information System (IMI)

for use. 2,364 processes were recorded there in the reporting period. All cases will

seen by my office. First of all, it is necessary to clarify whether we are responsible for the respective process

"Lead" or an affected supervisory authority. It is basically the supervisory

competent authority in which the principal place of business or the sole place of business of the

company concerned is located in the EU. When making a decision in each case

other supervisory authorities are also involved if they are affected. This is at-

for example the case when the company also has a branch in another country

or has already received corresponding complaints from the respective supervisory authority

are. After completion of the investigations, the lead supervisory authority shall

the supervisory authorities concerned submit a draft decision for comment. In 2020 was

my office was in charge of one case.

6.2.6

Register of designated data protection officers

In the 2020 reporting period, 1,281 reports to designated data protection officers were received

my office (Figure 10). These notifications included communications related to

Appointment of official and company data protection officers (DSB), to

changes or termination of this function.

According to Art. 37 Para. 1, the General Data Protection Regulation (GDPR) provides for the responsible

chen (public bodies in general; non-public bodies under certain conditions) the

Obligation to appoint a data protection officer. According to Art. 37 Para. 7 GDPR, a

144

6.3

Responsible or a processor the contact details of the data protection officer

not only to publish, but also to inform the supervisory authority. The documentary

The person responsible is responsible for naming and fulfilling the reporting obligation.

The messages sent are sent by the specialist departments of my authority, among other things

used to fulfill the reporting obligation according to Art. 37 Para. 7 GDPR or a possible

To check the existence of conflicts of interest according to Art. 38 Para. 6 DSGVO.

Pleasing: More and more responsible persons are now using the online

Form service on my website. The proportion of reports received via web form

gen, increased by 14 percent compared to the previous year. This type of transmission accelerates

the processing of the DSB reports in my authority. In addition, the reportable

After submitting the web form, immediately send a copy as a PDF document by e-mail.

sent. In the case of reports received by the office by e-mail, fax or post,

– to reduce administrative effort – no acknowledgments of receipt sent.

934

web form

saechsdsb.de

1,281

messages

named

Privacy-

representative

347

mail

e-mail

fax

Figure 10: Reports from designated data protection officers

6.3

resources

The workload in my office has increased due to the General Data Protection Regulation

regulation (GDPR) increased drastically. During the reporting period, however, my office recorded

a record. 17,152 inboxes were registered, around 23 percent more than in 2019

(Figure 11).

145

Chapter 6 Saxon data protection officer

25000

20000

15000

12839

10000

9360

5000

3479

0

22559

17152

18897

13984

17775

13179

4913

4596

5407

2017

2018

2019

2020

Outboxes

inboxes

total written material

Figure 11: Volume of documents

In the 18th activity report of the Saxon data protection officer for the public

Reich (2017), i.e. before the GDPR came into effect, I wrote:

“The new regulations will have a significant impact on my organizational structure, my

have powers and duties. The latter will expand enormously; depending on the type of count

one arrives at 50 to 60 new tasks for my authority. This results in a significant

additional staffing requirements. My agency currently, in early 2017, has almost the same number

of posts (21) as at the beginning of its existence (1993 19 posts), although the

Tasks since [….] have expanded enormously. The same applies - as a sign of a rise

welcome data protection awareness –

for the greatly increased number of

Citizen Inquiries. However, I am currently not in a position to carry out my statutory duties

fully and with the actually necessary breadth and depth. This is a

concrete disadvantage for the Saxon citizens and companies.”

146

Even in 2020, I was still not able to fully comply with the statutory duties.

men. There was still an imbalance between staffing and work

come up. A look at the numbers makes this clear.

6.3

2555

2359

2901

3500

3000

2500

2000

1500

1000

500

0

1043

2017

2018

2019

2020

consultations

complaints

Data Breach Notifications

Figure 12: Growth in key areas of activity

Personnel development in recent years, as of December 31:

2017: 22 posts

2018: 24 posts

2019: 28 posts

2020: 31 posts

From 2017 to the end of 2020, my office received nine additional positions and thus decreed

as of December 31, 2020 had a total of 31 positions. On the other hand, they tripled

annual new transactions in important areas of activity (Figure 12). this

The scope was not fully manageable in 2020 - especially since the "mountain of debt" that had been taken over

cases from 2019 was still to be processed. Not to forget: New employees who also work in the

Changed to my office as part of normal staff turnover, the other

considerable training time, which initially delays the processing of the processes.

The consequences of the too scarce personnel support: processing times of

years were still not uncommon, checks without cause were forced except for two

reasonably exposed, speaker activities at various specialist and advanced training

events could only be held to a limited extent (see 6.5.1).

In the course of the coronavirus pandemic, digitization has experienced a strong boost. she

is progressing rapidly and with it the electronic processing of personal data

At the same time, the GDPR has made people aware of data protection. It is therefore

acknowledge that the submitted complaints and reports of data breaches

continue to increase; the personnel bottleneck will not be resolved by a loss of predecessors

let gene solve.

Saxon

Data Protection Officer

official

Privacy-

representative

deputy

Data Protection Officer

 Budget officer

legal department/

administration

 Principle

 Legal department

 Administration

 Public-

skill work

Unit 1

Unit 2

Unit 3

Unit 4

information

technology

 Media

 Accreditation/

 Non-public

 Municipal

 Justice

area

 health

 Police

 Public

service law

being

 Constitutional

 eGovernment

protection

certification

 employee

privacy

 Social

 Statistics

 Science

administration

Subject 1

administration

Subject 2

 Personnel

 Household

 Secretariat/

registry

 Organization

 Registers

Figure 13: Simplified organization chart of the authority

6.4

6.4

Fines and sanctions, criminal charges

6.4.1 Administrative offense proceedings in the public sector

In the reporting period, the Saxon data protection officer was in the public sector

constantly for the prosecution and punishment of administrative offenses according to:

-
-
-
-
-

Section 38 (1) of the Saxon Data Protection Act, old version

(Section 38 paragraph 3 sentence 1 SächsDSG old version)

Section 22 (1) of the Saxon Data Protection Implementation Act

(§ 22 para. 3 Saxon GDPR)

Section 48 (1) of the Saxon Data Protection Implementation Act

(§ 48 para. 3 sentence 1 SächsDSUG)

Art. 83 General Data Protection Regulation

(Art. 58 para. 2 letter i GDPR, § 14 para. 1 SächsDSDG)

Section 85a Tenth Book of the Social Code – Social Administrative Procedures and Social Data

protection - in connection with § 41 Federal Data Protection Act, Art. 83 Para. 5 DSGVO (Art.

58 para. 2 letter i DSGVO, § 14 para. 1 SächsDSDG)

In the reporting period, a total of 74 fine proceedings were pending in the public sector.

Of these, 4 were concluded with a legally binding fine. In 15 procedures took place

an attitude or was refrained from the prosecution. 55 proceedings

which was still being processed at the end of the reporting period.

reporting period

pending total

from that

Procedure from previous reporting period

new procedures

closed

of which with a fine

with warning money

discontinued/absent from prosecution

still in progress

01.01. – 31.12.2020

74

53

21

19

4

0

15

55

Total legally binding fines/warnings in euros

4,040

149

Chapter 6 Saxon data protection officer

The sum of the legally binding fines and warnings amounted to 4,040 euros.

Compared to the previous reporting period, the number of new orders

infringement proceedings decreased slightly. Both the ongoing

increasing personnel bottlenecks as well as the temporarily reduced

limited functionality of the authority and the constantly increasing processing effort

in the area of administrative offenses had a negative impact on the duration of the proceedings. It

compared to the 2019 reporting period, the same number of procedures could

be closed. Compared to previous reporting periods, however, fewer

ger procedure to conclude, which in turn led to a lower total of the fixed

imposed fines.

Basically, in the reporting period, administrative offenses in public

can be differentiated into:

-

Operations falling within the scope of the GDPR –

Violations according to Art. 83 Para. 4 to 6 GDPR - and

-

Operations that do not fall within the scope of the GDPR.

Operations falling within the scope of the GDPR – breaches of Article 83

Para. 4 to 6 GDPR

Particular difficulties continued to exist in the processing of transactions

partly facts from the time before the direct applicability of the GDPR

and for which it had to be clarified which law was to be applied (cf.

Activity report 2019, 6.4.2, page 128 ff.).

After weighing up whether the previously applicable national administrative offense

norms or the GDPR were to be applied, in these cases regularly presented the

previously applicable national regulatory offenses norms represent the milder law in each case.

This was supported in particular by the lower level of fines (Section 38 (2) SächsDSG old version

with up to EUR 25,000, Section 85 (3) SGB X old version with up to EUR 300,000) against

above the GDPR with fines of up to EUR 20,000,000.

operations that do not

Violations by public prosecutors, police and correctional officers

service, regulatory offense authorities

within the scope of the GDPR

fall –

For the processing of personal data by the prevention, investigation,

cover, prosecution or punishment of criminal or administrative offenses as well as for the

Public authorities of the Free State of Saxony responsible for the enforcement of sentences, insofar as they have data

6.4

process for the purpose of fulfilling these tasks, since January 1, 2020, the

sian law implementing Directive (EU) 2016/680 (Saxon Data Protection Implementation

tion law – SächsDSUG).

For the administrative offense that occurs most frequently in the public sector - the

authorized processing of personal data or the unauthorized retrieval of personal

Son-related data from the police information or information systems

by police officers - the fine regulations have therefore been in force since January 1, 2020

ten of § 48 SächsDSUG.

When processing transactions, some of which relate to circumstances from before the

entry into force of the SächsDSUG, it had to be clarified in each case which right to apply

dung comes.

In administrative offense proceedings where the time of the offense was before January 1, 2020,

Section 4 (3) of the Administrative Offenses Act (OWiG) must be observed. § 4 para. 3 OWiG

votes in the event that the law in force at the time the act was completed, prior to the decision

of the administrative authority is changed, the most lenient law is to be applied.

In these cases, it was therefore necessary to weigh up whether the previously applicable SächsDSG was the old version or

the SächsDSUG was to be applied.

The SächsDSG valid at the time of the crime was usually the milder law.

In particular, the lower fine framework of the SächsDSG old version spoke in favor of this (§ 38

Para. 2 SächsDSG with up to 25,000 EUR) compared to the SächsDSUG (§ 48 Para. 2

SächsDSUG with up to EUR 50,000).

With regard to the relevant legal norms for police data processing and for

In these cases, the tasks and powers of the police enforcement service were extended to the

Saxon Police Act (SächsPolG) valid at the time of the crime, which as of December 31

December 2019 expired and the provisions of which are now essentially in

Find the Saxon Police Enforcement Service Act (SächsPVDG).

In the majority, around 76 percent, of the administrative offense proceedings were/are lagging behind

as before employees of the Saxon police suspected unauthorized personal data

processed and/or from the police information or information systems

to have retrieved. This was also the case regularly in this reporting period

privately motivated data retrieval from friends, colleagues, neighbors or other acquaintances, but

also for research on one's own person.

This results in the high proportion of administrative offense proceedings against police officers

mainly from the above-average reporting behavior of the police stations, which

che a data protection misconduct of their employees continues to be consistent

pursue.

In the other administrative offense proceedings, around 24 percent, existed/is opposed

employees of various Saxon (social) authorities suspected of not

to have processed personal data without authorization.

In four of the proceedings concluded with a fine in the reporting period, it acted

unauthorized retrieval of non-obvious personal data from the police

Databases (Section 38 Paragraph 1 No. 1 a SächsDSG old version), and/or unauthorized processing

gene of non-obvious personal data (§ 38 Abs. 1 Nr. 1 a SächsDSG old version

sung) by police officers. One case involved a fine

against an employee of a public social service provider because of an unauthorized

Processing of social data that is not generally accessible (§ 85 Para. 2 No. 1 SGB X old version).

Already the persistently large number of administrative offense proceedings against Saxon police

lizeibedienstte shows that there are still ambiguities in connection with the use

police databases exist.

Privately motivated retrievals of personal data from the police

information systems by individual suspects with the general function as police

law enforcement officers and the duty to avert security justified and/or justified by the fact that

because of the position as a police officer, there is general authority to

to retrieve data.

However, the retrieval of non-obvious personal data is only permitted if the

such knowledge is required for the retrieving person to carry out the task, i.e. only if

if the fulfillment of the legal - i.e. the resulting from an official reason

− task is not possible without the specific data collection. Even if the police

Information systems for the daily work equipment of a police

officials count and the data stored therein is generally accessible, must be for everyone

Data processing and for every data retrieval an official necessity

(Judgment of the Higher Regional Court (OLG) Bavaria of August 12, 1998, Az.: 5St RR 122/98; OLG Bam-

berg, decision of April 27, 2010 - 2 Ss 531/10).

Even if police officers according to § 2 SächsPVDG generally have the task of individuals

and to ward off dangers to the community, they are fundamentally involved in doing so

their specific task allocation and responsibilities. As is the whole

152

6.4

Police enforcement service may only process the personal data required to fulfill its

ner tasks are required (§ 53 SächsPVDG in connection with § 3 SächsDSUG), is also

the individual police officer is only entitled to fulfill his specific official duties

task to process necessary data.

This is clear from the Saxon Police Enforcement Service Act and the

sian police data processing relevant Saxon data protection implementation

law (§§ 53, 54 SächsPVDG, §§ 3, 4, 5, 9 SächsDSUG; cf. also judgment Bayerisches Obers-

tes regional court of August 12, 1998, case no.: 5St RR 122/98).

The decision of the OLG Bamberg (decision of August 28, 2018, file number: 2 p

OWi 949/18) also clarifies:

"The retrieval of non-public data in police research systems by a police

officer is only permitted if, from his point of view, the knowledge of the data for the police

fulfillment is necessary. If there is no official reason or if the person concerned acts privately

If you are interested, the data retrieval is unauthorized...".

Even if, according to the above-mentioned decision of the OLG Bamberg in the area of hazard

defense against an abstractly existing danger can be sufficient, it is assumed from the further

statements that for the admissibility of a data retrieval the existence of a

initial suspicion is required, “therefore one that goes beyond mere assumptions

concrete suspicion based on certain factual indications that a criminal offense

has been committed and the suspect is considered to be the perpetrator or accessory to that crime

comes."

Evidence of a purely privately motivated data query can also be found

the specific procedure of the data subject following the individual data retrievals

ben. If a police officer is outside of his local and factual responsibility

sphere of competence, it should therefore correspond to the official customs,

if he either creates a corresponding process himself and this at a given time

to the responsible office or at least a memorandum on the occasion, counter-

the status and result of the investigations and forwards this to the person responsible locally and factually

police station to initiate a process (OLG Bamberg, decision of

August 28, 2018, file number: 2 Ss OWi 949/18).

Only the pure property of being a police officer, which of course for defense

of dangers and the prosecution of criminal offenses according to § 2 SächsPVDG is sufficient

therefore regularly not sufficient for a business occasion and all technically possible

to justify data retrieval.

153

Chapter 6 Saxon data protection officer

The punishment of administrative offenses in the public sector is still essential,

to the employees of the authorities and public bodies in Saxony to their future

to admonish to observe special duties and act as a role model.

6.4.2 Administrative offense proceedings in the non-public area

In the reporting period, I had to register 80 new administrative offense reports. The

number was essentially at the level of the previous year. More than a quarter

of the reports (25) referred to – by the police within the usual framework

Traffic stops detected – Dashcams. In another 20 cases, the ads were directed

against the operation of other video cameras. This puts the focus, 56 percent, at

I received notifications of administrative offenses again clearly in the video surveillance.

In total, I had 180 administrative offense proceedings in the reporting period.

pending. Of these, I was able to close 54 cases and set 29 fines.

All fines related to the illegal use of dash cams by private individuals. the

The amount of the fine was between 100 and 1,000 euros (11,870 euros in total). As far as it goes

Dashcams were only minor violations or a pursuit

of the impermissible dashcam use has been waived for other reasons, I have

the fine proceedings are discontinued and instead a warning according to Art. 58 Para. 2 Letter

b General Data Protection Regulation (GDPR) or a corresponding notice

granted, Art. 58 Para. 1 Letter d GDPR.

In one case, the fine was imposed on a Romanian citizen. According to the

I therefore have permission from the Residence Act (AufenthG) after the end of the procedure

informed the competent foreigners authority about the imposition of a fine. Dem was

the provision of § 87 para. 4 sentence 1 AufenthG, according to which the for the initiation and

Implementation of a fine procedure competent bodies the competent foreigners authority

must be informed immediately about the completion of the fine procedure. The middle

The obligation to apply applies to all non-German nationals if - which is the case with data protection

is always the case - the administrative offense with a fine of more than 1,000 euros

is threatened (section 87 subs. 4 sentence 3 of the Residence Act). In particular, it also applies to EU foreigners (cf. §

11 para. 1 sentence 1 Freedom of Movement Act/EU). This is decisive in the basic data protection

maximum level of fines set by regulation; it depends on the actual amount of the fine

not on.

The case of an in-house inspection already described in the 2019 activity report (6.4.1, page 126 ff.)

search in connection with an apparently very extensive use of dashcams

I was able to conclude 2020 with a fine of 1,000 euros. In

Dashcam cases, the police who determine the violation regularly already provide the respective

Memory card as evidence, so that the proof of an administrative offense mostly

is easily possible. Here the case was somewhat different, since the person concerned initially only

with numerous administrative offense reports relating to alleged traffic violations

Third had become conspicuous. These administrative offense reports were mostly – only
very short video sequences attached, from which a permanent ad-
free and therefore illegal dashcam operation with subsequent longer-term storage
Securing the video recordings was to be derived, but in any case such a thing was not legally binding
could have been proven. As a last resort, there was only one way of doing things – in court, of course
ordered house search remained. From colleagues from other federal states
I am aware that there, too, in comparable cases, courts have issued appropriate search warrants
passed resolutions and this with the threat of high fines of the basic data protection
order on the one hand and the considerable importance of protecting personal rights
of the persons affected by the video recording on the other hand.
Dashcam operators should be aware of this risk.
After the required evidence was confiscated during the house search
had been taken, it was now also possible to provide evidence of the crime. had to
I find that the person concerned had not only used the video recordings to
to document and report alleged traffic violations by third parties, but
also to provide evidence to his former employer that he was in the frame
to collect extra work done during his job as a courier driver. To that end he had
created longer video compilations of his related journeys, which
how long it takes to fulfill individual travel orders and on which routes
had been and what causes (e.g. traffic jams) to a significant extension
the journey time. At the same time, these records should also be made available to customs in the
be made available to investigations against the employer of the person concerned.
That such a purpose is not suitable for dashcam use with continuous recording
to justify the drawing is obvious. The evidence requested by the person concerned
are also to be provided in other ways. That is, a permanent record of the road
traffic is not necessary for this. In addition, the interests worthy of protection predominate here

of other road users – during their stay on public transport

space not to be video-monitored by persons unknown to you – this

related evidentiary interest of the person concerned in particular also clear because they

relevant incidents and investigations (unlike, for example, in accident or dangerous situations)

are not involved in any way.

Insofar as the person concerned had also regularly used the dashcam to

to document violations of third parties against the road traffic regulations and to report them

parallels to the well-known case of the "Knöllchen-Horst" from Lower Saxony

(cf. Celle Higher Regional Court, decision of October 4, 17, 3 Ss (OWi) 163/17 and

Goettingen Administrative Court, judgment of May 31, 2017, 1 A 170/16).

155

The person concerned had the dashcam permanently in use, later in his opinion

cut out relevant video sequences and finally using them

reported to the police for alleged traffic violations by third parties. With the perma-

nent video documentation in case of committing traffic offences

through third parties, he was already not pursuing any of his own interests worthy of protection, because the surveillance

of road traffic is a sovereign task that is exclusively the responsibility of the responsible

road traffic authorities and the police. For this reason alone, the company

the dashcam was unlawful. In addition, there were also predominant ones here

legitimate interests of other road users. For them there was a risk that

them due to the advertisements with video recordings made by dashcams

right to be covered with administrative offense proceedings. The task of tracking

Traffic offenses or traffic offenses are not the responsibility of individual road users

mers such as the person concerned, but only the responsible authorities (cf. also

Activity report 2019, 2.2.2., page 34 ff.). The assessments and evaluations of the responsible

Incidentally, the police departments showed that the reports mostly not even

Traffic violations were to be found, such only in the imagination of the person concerned

existed some of the documented incidents were also caused by those affected

been provoked themselves - the potential for conflict in the delivery of mail and goods

ments is well known.

6.4.3 Who owns the procedural files in fine proceedings?

If the public prosecutor's office discontinues preliminary investigations into a criminal offence,

but this because of the possible realization of an administrative offense

give myself away, I can observe very different procedures. Usually

I will be sent the relevant files with acknowledgment of receipt without further comments

hand over. But there are also public prosecutors who give me the files to prosecute

handed over an administrative offense under their own responsibility, but at the same time also a return

after the end of the procedure or a transfer to other bodies from their consent

make dependent.

I have a hunch that such claims are merely from the unverified application

result from text modules. In fact, procedural rule goes with a toll

according to § 43 law on administrative offenses (OWiG) to the administrative authority, so here

to me, about. With the submission by the public prosecutor's office, the administrative authority follows

§ 35 Para. 1 OWiG responsible for the procedure without it being the initiation of a fine

procedural need. The decision on how to proceed, in particular the

taking further investigative measures, the termination of proceedings or the conclusion by means of

of a fine, then lies solely with the administrative authority. The administration

authority is only bound by the decision of the public prosecutor's office as to whether an act is a criminal

deed is prosecuted or not (§ 44 OWiG).

6.5

This means that the procedural files after the conclusion of the administrative offense
rens remain with the administrative authority in accordance with the applicable retention periods and
subsequently destroyed by them; a return to the public prosecutor's office
that out.
It is different only in the case of an objection against the issued by the administrative authority
its fine notice if the administrative authority does not remedy this objection. then
she has to transfer the fine files via the public prosecutor's office to the responsible district court
send (§ 69 Abs. 3 Satz 1 OWiG). With the receipt of the files by the public prosecutor's office
the tasks of the prosecuting authority are then transferred (again) to the public prosecutor's office
(Section 69 (4) OWiG). If the objection is not subsequently withdrawn,
So the fine files actually go to the public prosecutor's office.

6.5

public relation

I also received numerous press inquiries during this reporting period. Among them were
Inquiries about the joint competence and service center for telecommunications
on monitoring. It was 2018 by the police forces of the states of Berlin, Brandenburg, Saxony,
Saxony-Anhalt and Thuringia (cf. activity report 04/2017 to 12/2018,
Part 1, 1.1.3.1, page 15 f.). The center is based in Leipzig as an institution under public law
maintain the basis of a corresponding state enterprise. To desired technical
and organizational measures as well as security concepts or
However, I was not able to provide any new status at that point in time.
len. From April of the year, the inquiries about corona measures and thus a
associated personal data processing, in particular in connection with a
ner contact data collection and the admissibility of population register queries by health
public authorities for contact tracing in Saxony (see also 1.1, 2.2.1 to 2.2.7,
2.3.3 and 8.1). In the course of the reporting period, press law disclosures

look for the decision of the European Court of Justice "Schrems II" (cf. 5 and 9.3) and to

operations in the police. In addition, I received more than 100 other press inquiries. Many

were in connection with the chairing of the conference of independent data protection

supervisory authorities of the federal and state governments (see 1.3).

The employees of my department continuously provided information via the website

especially for data protection in the coronavirus pandemic. For that became one

created a rubric of the same name. It contains, among other things, articles on data protection compliance

Use of tele/home work, the evaluation of telecommunications data on the pandemic

and a model form for collecting contact details from employees.

It was important to me to prepare the information in a practical and understandable way.

Interested parties received further support and advice from the Virtual Data Protection Office,

in which we also participated. This is an information portal for citizens

ger, which is operated by institutionalized data protection control bodies: datenschutz.de

6.5.1

training and lectures

During the reporting period, employees from my office held 16 advanced training seminars

hold, among others at the Saxon Administration and Business Academy Dresden,

at the training center of the Free State of Saxony, at the State Office for Schools and Education,

at the Saxon State Archives and at a conference for data protection officers from the

area of justice. Compared to previous years, there is a decline in the number of lecturers

determine. On the one hand, this was due to the infection protection measures in connection with

the coronavirus pandemic, which is why a number of events were cancelled, on the other hand

on the work volume of the employees in the agency (cf. 6.3).

In the lectures during the reporting period, basics and current issues were discussed, among other things

to the General Data Protection Regulation. At other events, my

Employees about data protection in schools, in local government, in forensic institutions

and about data protection according to Book Ten of the Social Code (SGB X).

158

7.1

7

Cooperation of data protection supervisory authorities

den, data protection conference

7.1

conference activity

As already explained under 1.3, I chaired the data protection

conference (DSK). At the same time, we were also represented in the 26 working groups. hand

in the early years at the end of the 1970s at DSK it was still about loose

meetings of state data protection officers, over time an indispensable

has become a valuable working tool for data protection in Germany and Europe. Insight

to the following resolutions, decisions and guidance makes clear how

The topics that the DSK dealt with in the reporting period are varied and complex.

The documents are linked in the digital version of the activity report.

7.2

Data Protection Conference Materials – Resolutions

Resolutions are public statements by the DSK on data protection policy issues,

for example to introduce a new law. Resolutions need a two

Third majority in the DSK.

 Information procedures for security authorities and intelligence services conform to the constitution

design (25.11.2020)

 Operators of websites need legal certainty - federal legislature must

finally fulfill legal obligations of the "ePrivacy Directive" (25.11.2020)

 To protect confidential communication through secure end-to-end encryption

selung - stop proposals of the Council of the European Union (25.11.2020)

 Data protection also needs regional courts in the first instance (09/22/2020)

 Create digital sovereignty in public administration – personal data

protect better (09/22/2020)

 Patient Data Protection Act: Without improvements in data protection for the insurance

violate European law! (09/01/2020)

 Implement register modernization in accordance with the constitution! (08/26/2020)

 Police 2020 – see risks, seize opportunities! (04/16/2020)

 Data protection principles in dealing with the corona pandemic (04/03/2020)

Chapter 7 Cooperation of data protection supervisory authorities, data protection conference

7.3

Data Protection Conference Materials - Resolutions

Resolutions are positions that relate to the interpretation of data protection regulations

pertaining to corresponding recommendations.

 Telemetry functions and data protection when using Windows 10 Enterprise

(11/26/2020)

 Application of the GDPR to data processing by parliaments (09/22/2020)

 Use of thermal imaging cameras or electronic temperature recording as part of the

Corona Pandemic (09/10/2020)

 Decision of the conference of independent federal data protection supervisory authorities

and the federal states on preliminary objections to StreetView and comparable services

(05/12/2020)

 Notes on the use of Google Analytics in the non-public area (05/12/2020)

 Decision of the conference of independent federal data protection supervisory authorities and the federal states on the consent documents of the Federal Medical Informatics Initiative of the Ministry of Education and Research (04/27/2020)

7.4

Materials of the data protection conference –

orientation aids

Orientation aids and standardization are technical application aids for those responsible che, processors, manufacturers and the public.

 Checklist data protection in video conference systems based on the orientation guide Video-deoconferencing systems, status: 23.10.2020 (11.11.2020)

 Video conferencing systems (23.10.2020)

 Video surveillance by non-public bodies (03.09.2020)

 Measures to protect personal data when it is transmitted by email (05/12/2020)

7.5

Materials of the data protection conference –

Application Notes

 Accreditation requirements in accordance with Article 43 (3) GDPR in conjunction with DIN EN ISO/IEC 17065 (Version 1.4) (08.10.2020)

160

7.6

 Requirements for the accreditation of a monitoring body for rules of conduct according to Article 41 GDPR in conjunction with Article 57 paragraph 1 lit. p 1st alternative GDPR (09/23/2020)

 Standard data protection model version 2.0b (04/17/2020)

7.6

European Data Protection Board documents:

Guidelines, recommendations, best practices

The European Data Protection Board approved the following documents

ments that are linked in the digital edition of the activity report.

 Guidelines 10/2020 on restrictions under Article 23 GDPR

 Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers

of personal data between EEA and non-EEA public authorities and bodies

 Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the

GDPR

 Recommendations 01/2020 on measures to supplement transmission tools for

ensuring the level of protection under Union law for personal data

 Recommendations 02/2020 on the essential European guarantees in relation to over-

security measures

 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

 Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

 Guidelines 08/2020 on the targeting of social media users

 Guidelines 07/2020 on the concepts of controllers and processors in the GDPR

 Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the

GDPR

 Guidance 5/2019 on the right to be forgotten criteria in cases relating to

Search engines according to the GDPR (Part 1) - version adopted after public consultation

 Guidelines 05/2020 on consent under Regulation 2016/679

 Guidelines 3/2020 on the processing of health data for scientific research

research purposes related to the COVID-19 outbreak

 Guidelines 04/2020 for the use of location data and contact tracing tools

consequence related to the outbreak of COVID-19

 Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific

tific research in the context of the COVID-19 outbreak

161

Chapter 7 Cooperation of data protection supervisory authorities, data protection conference

 Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers

of personal data between EEA and non-EEA public authorities and bodies

 Guidelines 3/2019 on the processing of personal data by video devices

 Guidelines 3/2019 on processing of personal data through video devices - version adopted

after public consultation

 Guidelines 1/2020 on processing personal data in the context of connected vehicles and

mobility related applications

7.7

European Data Protection Day on the topic

"Cross-border data transfers"

In the second half of the reporting period, i.e. from June 2020, I was intensively involved with the

Preparation of the 15th European Data

schutztag on January 28, 2021 on the subject of "Cross-Border Data Transfers". For

I was able to attend the event, which was finally carried out as an online conference, together with

outstanding experts from the Federal Ministry of the Interior, Building and Community (BMI).

the Council of Europe and the European Union. The conference was with just under 1,000

Online visitors from all over the world the best-attended European Data Protection Day since

an existence.

Traditionally, the event of the European Data Protection Day on January 28th is

nes of each year to the DSK chairman of the previous year. Since the beginning of March 2020,

changing "corona conditions" with a first lockdown, i.e. the closure

larger meeting places, subsequent loosening and finally a second loosening

down, which became foreseeable in autumn 2020, did the organisation, preparation and

finally implementation of the data protection day 2021 to a complex, the forces of my

small teams to the limit demanding task. Basically, I always had parallel

probably to prepare a face-to-face and a video conference.

As a blessing in disguise, I felt the - extraordinary, due to the upcoming 40th

after the 1981 Council of Europe “Convention 108” (data protection)

work with the BMI. The Federal Ministry of the Interior proved to be a strong and helpful partner, with

it was a pleasure to work together. In autumn 2020 we decided together

to hold a purely online event. As a topic, we unanimously set the

Prerequisites for the transfer of personal data from the EU respectively

the countries of the European Free Trade Association (EFTA) in third countries ("Cross Bor-

of data transfers"). So we had a after the "Schrems II" judgment of the European

Court of Justice (ECJ) of July 16, 2020 (C 311/18) highly topical and above all for the economic

an important topic. Because with this verdict, the previous

Judgment of the ECJ of October 6, 2015 (C-362/14) on "Safe Harbor".

162

7.7

the requirements for data transfers from EFTA to third countries - urgently

gained importance. For the Council of Europe side, the Federal Ministry of the Interior should

As for the EFTA, I should win over the speakers.

On my side, I had the good fortune and honor of having Prof. Dr. dr h.c. Thomas von Dan

witz, judge at the ECJ and rapporteur in the “Schrems II” case, and Mr Aleid Wolfsen

LL.M., Vice-Chair of the European Data Protection Board and Chair

zender of the Dutch supervisory authority (Autoriteit Persoonsgegevens) as speakers

to be able to win. We would like to take this opportunity to thank both of them. My selection was in

wonderfully supplemented by the speakers won by the BMI, Ms. Alessandra Pe-

rucci, Chair of the Convention Committee of the European Union’s Data Protection Convention 108

roparats, and Dr. H. c. Tim Eicke QC, Judge at the European Court of Human

human rights (ECtHR).

The event, which was finally held on January 28, 2021 from 12 p.m. to 4 p.m., began with

Greetings from the Parliamentary State Secretary in the BMI, Mr. Stephan Mayer, the General

Secretary of the Council of Europe, Ms. Marija Pejčinović Burić and myself. After that-

The speakers then presented their views in approx. 20-minute presentations.

ter Eick spoke about the importance of the Data Protection Convention 108 and reminded of the important

most recent data protection cases of the ECtHR in the last 20 years. Ms. Perucci presented the

history and the scope of Convention 108. The Convention is dated 56

states have been ratified, including six African and three South American states

ten. Since 2018, there has been an amendment log to adapt it to the GDPR, which

has since become the "Convention 108+". Unfortunately, this adapted convention has only been implemented so far

eleven contracting states have been ratified (38 states would be required for entry into force). Woman

Perucci nonetheless expressed the hope that more states would join the convention.

den, as they ensure an adequate level of protection for the transfer of data

contribute Thereafter, Mr. Wolfsen LL. M. that just at the current uncertain

Legal situation well-equipped supervisory authorities for data protection are important because it

would now be in the hands of every company itself, the prerequisites for a legal

moderate transfer to a third country. Professor Dr. von Danwitz equated

At the beginning of his remarks, when asked by the moderator, it was clear that he was correct

Application of the provisions of the GDPR have no other decision than in "Schrems II".

can meet.

In the discussion that followed, the speakers answered the numerous questions from the

likums. Among other things, they denied the question of whether between endangered and less

endangered data could be distinguished and the latter with less effort into one

third country could be transferred.

At the end there was a final word from the new chairperson of the data protection conference, the Saar country representative Monika Grethel.

My thanks again go to all the speakers and everyone who helped to carry out this outstanding have contributed to the event.

The event can be viewed later in the media library of the BMI.

7.8 Joint review of media companies by data protection authorities

The setting of cookies and the integration of third-party services through websites are as before the subject of numerous complaints. With the entry into force of the data General Protection Regulation (GDPR) enforced that many of these data processing one require consent, the manner in which this consent is obtained is violated however, often against applicable law. With the judgments of the European Court of Justice (ECJ) of October 1, 2019 of the Federal Court of Justice (BGH) of May 28, 2020 Case law expressed to the effect that an active consent to the setting and reading cookies is required. The data protection supervisory authorities acted early dealt with these legal issues and with the guidance for providers of Telemedia in March 2019 (available at datenschutzkonferenz-online.de) application of the GDPR for questions regarding the design of websites. In addition, has the data protection conference (DSK) in relation to the use of Google Analytics ßert, probably the most widespread tracking service. The information from the DSK final can be downloaded from datenschutzkonferenz-online.de.

In spring 2020, a total of eleven of the German data protection supervisory authorities concluded, a joint examination of the respective media companies with the widest coverage

to be carried out in the respective state. For this purpose, a permanent working group was established

which questionnaires on the use of cookies, third-party providers and the design of

consent solutions for the websites operated by the media companies.

These were sent to the media companies in the summer and the returns are currently being processed

evaluated. The questionnaires are used exclusively within the respective responsibilities

evaluated by the supervisory authorities, but there are still individual questions about the evaluation

a lively exchange takes place.

Even if the 2020 examination was not yet completed, it can be stated that

the proportion of cookies and tracking elements set without consent in comparison

by around 50 percent by spring 2020 when the questionnaires were submitted in autumn 2020

has gone. This is certainly also due to the judgments of the highest courts,

but clearly shows that those responsible have realized that changes are necessary

(see also Activity Report 2019, 9.4, page 167 and 9.10, page 172 ff.).

8.1

8th

8.1

Directive area – Directive (EU) 2016/680 – and

other areas

Use of "Corona visitor lists" for

law enforcement purposes

The reporting period was dominated by the pandemic and the measures to prevent it

the spread of the SARS-Cov2 virus. One way to trace contagion routes

being able to do so was seen in the obligation of certain companies and institutions to make lists

to lead in which visitors or guests their contact details in the event of a

should indicate any necessary contact tracing.

For a few months it was not undisputed whether the police used these lists for criminal prosecution purposes.

was allowed to use. While the lists served the stated and limited purpose of

to enable health authorities to trace the contacts of infected people. All-

However, there was the obligation to keep visitor lists and their narrow purpose

their basis only in ordinances of the federal states.

The federal regulations of the Code of Criminal Procedure (StPO) for the publication of

Objects and documents that are important as evidence for criminal prosecution

can be, for their seizure and confiscation remained of the state law

Purposes unaffected. Legally, the police demand for the release of

Visitor lists for law enforcement purposes are therefore not objectionable. There was no bun-

of the legal regulation that allows the lists to be used for purposes other than those of infectious

on protection prohibited.

This changed when the amendment to the Infection Protection Act (IfSG) came into force on 19.

November 2020. Section 28a (4) IfSG now stipulates that contact lists or the

data they contain for no other purpose than delivery upon request

may be used by the competent health authority, which in turn will use the data from

finally may continue to use for the purposes of contact tracing.

This federal provision constitutes a special federal usage rule

succeeded within the meaning of Section 160 (4) StPO, which is the use of data from contact lists

to track infection chains for law enforcement purposes.

165

Chapter 8 policy area - Directive (EU) 2016/680 - and other areas

8.2

Use of bodycams by the Saxon police

In the fall of 2019, the concept for the nationwide introduction of body-worn

new recording devices (“bodycams”) in the Saxon police force. Already before

I became involved both in the legislative process and in the development of the establishment
closely involved in the arrangement by the Saxon State Ministry of the Interior. After a
previous testing phase in selected police departments and creation of a
special authorization basis in the new Police Enforcement Service Act was planned -
starting with the year 2020 - over a period of two years, the organizational units
(including the facilities for training and further education as well as the patrol
dienst) with a total of around 1,500 cameras, with which image and sound recordings are made
can be equipped. The primary goal of the application is to protect the
be police officers. The body cams are intended to help resolve conflict-ridden situations
de-escalate and thus prevent violent attacks on third parties. Furthermore, that should
Procedures that support evidence in the context of criminal prosecution. The preventive
set of bodycams for self-protection or to protect third parties is in all publicly accessible
areas possible and is based on Section 57 paragraphs 4 to 9 of the Saxon Police
Train Service Act (SächsPVDG). legal basis for use in criminal prosecution
§ 100h paragraph 1 no. 1 StPO, § 100f paragraph 1 Code of Criminal Procedure (StPO).
According to § 57 Para. 6 SächsPVDG, the use of bodycams is special in a suitable way
to make recognizable. Therefore, the body cams are only open and in connection with the
speaking neon yellow sign "Video Audio". The beginning of the recording
is generally communicated to the data subject. The bodycams are configured in such a way that
recordings are externally recognizable. The police officers are required to
to limit the recording of uninvolved third parties to an unavoidable minimum.
According to the legal regulation (in § 57 Abs. 4 SächsPVDG) the so-called pre-record
thing allowed. The recordings are briefly stored in a buffer for up to
Stored for 60 seconds, but then permanently overwritten. Only when starting the actual
civil admission (under the conditions of § 57 para. 5 SächsPVDG - existence of a
concrete danger to life or limb) the images of this "initial phase"

stored longer and are available for further processing.

According to § 57 paragraph 7 sentence 3 SächsPVDG, the recordings are made after 30 days

automatically deleted if not used to prosecute criminal offenses or to verify the

legality of the measure or the recording itself.

This is according to the legal regulation in § 57 paragraph 7 sentence 4 and 5 SächsPVDG

Procedure for inspecting bodycam recordings in an administrative regulation

regulated (VwV insight Bodycam).

166

8.3

According to this, affected persons receive - these are all persons from whom in the context of a

Bodycam use image or sound recordings were made, including police officers

and uninvolved third parties - inspection of the records. Access is limited to

Records pertaining to the applicant. Exceptionally, the inspection

also be granted in recordings, the image and sound sequences to other people

included, insofar as this is absolutely necessary for reasons of the factual connection. Here-

the other persons should be anonymized if possible.

The right to inspect records belonging to the others in Section 57 (7) sentence 3

SächsPVDG mentioned purposes, for example in criminal proceedings, or

already included for this purpose is based on the respective regulations

the inspection of files (e.g. § 147 StPO). In addition to having the right of inspection

the persons concerned have a right to information from the police about the

processing of personal data in accordance with Section 92 (2) SächsPVDG

with Section 13 of the Saxon Data Protection Implementation Act.

The use of bodycams is no later than the arrangement in § 57 Para. 9 SächsPVDG

Evaluated by the state government at the end of 2024.

From a data protection point of view, the legal regulation and the sub-legal

regulations a pleasingly high degree of transparency in the processing of personal

obtained data using bodycams. I assume that the legal appli-

conditions and safeguards unreasonable interference with rights

prevent more affected also in the practical application.

8.3

Right to information of the person concerned

fine proceedings regarding the person making the complaint

In the period under review, too, I received complaints from people against whom a fine

monetary procedure was conducted and to whom the administrative authority granted the

information about the person making the complaint, mostly with reference to the protective

worthy interests of the complainant. Such action by the administrative authority is

in any case unlawful if the information or statements of the person making the complaint

basis for the fine procedure, as is the case in procedures based solely on so-called civil

Ads based, mostly is the case.

If the competent administrative authority initiates fine proceedings, the processing takes place

personal data insofar not within the scope of the basic data protection

regulation (DSGVO). The exception of Art. 2 Para. 2 Letter d GDPR not only covers

Criminal offenses, but also administrative offenses under German law. In the relevant

scope of application of Directive (EU) 2016/680, the processing of personal

ner data according to the provisions of the Administrative Offenses Act (OWiG), the criminal

of the Federal Data Protection Act

(BDSG).

The data protection right to information of the person concerned according to § 57 BDSG, the

according to Section 57 Paragraph 1 No. 2 BDSG, information about the origin of the data can also be collected

according to Section 57 (4) in conjunction with Section 56 (2) BDSG, among other things

if legal interests of third parties would be endangered and the interest in avoiding this danger

drive the information interest of the data subject prevails.

In addition to the general data protection law, the data subject has a right to information

§ 57 BDSG also a right to inspect files (§ 49 paragraph 1 law on administrative offenses

(OWiG)). According to this provision, the interests of third parties that are worthy of protection must also be taken into account

and, if they predominate, may prevent the person concerned from gaining insight.

If the person concerned has a defense attorney, his right to inspect the files is governed by Section 46 (1).

OWiG in connection with § 147 paragraph 1 StPO. A special feature of this right – in comparison

to the claims of the person concerned without a defense attorney - consists in the fact that property worthy of protection

interests of third parties do not constitute a reason for denying access to the files. Only the danger

Execution of the purpose of the investigation before the conclusion of the investigation is justified according to § 147 para.

2 StPO the (partial) refusal of access to files.

If the name of the person making the complaint was also filed with a complaint, it is extended

the defense attorney's extensive right to inspect the files also extends to this information.

Even if the person concerned does not have a defense attorney, it will be disclosed in fine proceedings

the identity of the complainant if he is named as a witness

(either by the administrative authority, insofar as they base their fine notice on the perception

statement of the person making the complaint, or by the court or the person concerned in the judicial

technical procedure).

In such constellations, the rule of law and the principle of fairness require

Procedure in which the “evidence” is named to the person concerned and he/she agrees

must be able to deal with the evidence (witness testimony).

It is part of the essence of a constitutional procedure in the area of prosecution

of criminal and administrative offenses, where the state's monopoly on the use of force is particularly

it becomes clear that the competent state authorities are acting "with open visors".

8.3

Decisions connected with interventions in the legal positions of the accused/affected
are generally not allowed to be made on the basis of "secret" information
will.
The more important information is for the procedure (and the official decision),
the greater and more worthy of protection is the interest of the accused or
agreed to have access to this information; not least to evaluate the information
and to be able to defend yourself properly. Especially in cases where the ad
of a third party and, if applicable, their photo of an alleged violation of the rules
are the only basis for the official procedure and this in the written
Statement/hearing of the person concerned under the heading “evidence/witnesses” as also indicated
the complainant has an overriding interest worthy of protection in the secret
not regularly keep his name.
Prerequisite for a restriction of file inspection or information to the
Those affected with regard to the identity of the complainant would be that his protection-worthy
Interests (§ 49 Para. 1 Sentence 1 OWiG) or possibly endangered legal interests of third parties
ter (§ 57 Para. 4 in connection with § 56 Para. 2 No. 3 BDSG) in the interest of the data subject
the knowledge of the origin of his data, which the authority processes (against him), prevail.
The affirmation of a legitimate interest of the complainant in secrecy
his name alone is therefore by no means sufficient to convey the insight or
limit the data subject's right to information. Apart from the fact that the
possibility of such an interest can be discussed controversially (e.g. in
to cases of false suspicion, defamation and the like), there is a "predominance"
this interest of the person making the complaint in cases of "citizen's report" and without own, through
the administrative authority itself secured evidence from any point of view in

costume.

The administrative authority decides on its own responsibility whether to proceed alone

Based on information provided by third parties - with the consequence that their data

the person affected by the procedure at his request or ex officio in the fine notice

are to be disclosed - or whether employees of the authority at the location of the reported

make their own observations of the incident and secure evidence. Then, if the

can be supported in a court of law on its own evidence and the name of the reference

is irrelevant to the procedure, the decision on the

sen disclosure within the scope of the file inspection or the information to the person concerned

turn out differently.

Chapter 9 Jurisprudence on Data Protection

9 case law on data protection

9.1 Action for annulment due to a decision on costs Saxon data protection officer and application for reinstatement to the previous status

I had to deal with a supervisory procedure in the administrative court, which

ches already in January 2017 with the determination of a series of data protection violations

finally concluded with a corresponding cost assessment by my department

had been sent.

Trigger for the event-related supervisory process that began in September 2014

was a request to equip company trucks with GPS transmitters. In the course of processing

During the course of the supervisory process, a number of violations of data protection law were identified

and specifically named in the final notice of determination and costs. This

The decision became final in February 2017.

I was a bit surprised when I was the legal representative of those responsible

In March 2017, the administrative court first asked for reinstatement in the previous

status and also the annulment of the determination and cost notice

had requested. In my opinion, the application was unfounded because the applicant

due diligence that is reasonable under the circumstances is not observed, i.e. the

failure to bring an action in time was his own fault. This was

failure to answer primarily through the legal representative, but in this respect

to be attributed to the applicant accordingly (§ 173 Administrative Court Code in connection

tion with Section 85 (2) of the Code of Civil Procedure). Counsel had a sudden

Inability to work as a result of an accident cited as a justification, but in particular

unable to demonstrate that he had taken appropriate emergency precautions, which also

an unforeseen hindrance, the ability of the law firm to function, in particular the

Monitoring of deadline matters, guaranteed. Incidentally, inability to work does not mean

equal incapacity to act. Even in the event of an accident or a sudden

In the case of an illness, a lawyer can be expected to treat his clients accordingly

inform them so that they can avert any missed deadlines themselves.

The competent administrative court followed my arguments in this regard and has

the action dismissed with a court order for inadmissibility; reinstatement in the

previous status was therefore not granted.

170

9.2

However, the matter was still not over. After I good

Faith whether the legal force of the court decision two months later at the responsible

had reminded the still outstanding costs and they actually did too

had been settled reached me two months later, completely unexpectedly

a summons to an oral hearing on the same matter. cause of the non-occurrence
Legal force of the court decision were obviously problems with the proof of his
position to the procuratorate. This had only three months after Zu-
sent - after several unsuccessful inquiries - the electronic acknowledgment of receipt
sent for the court decision and asserted based on this, only to
to have taken note of this late date, so that the deadline for filing
of an appeal for him has not yet expired. The court actually recognized this
and meant that the mere information that the court order had been delivered electronically
which is not sufficient to consider service to have been effected. So be it
application for an oral hearing that was delayed by two months is still on time
been asked.
Ultimately, however, the oral hearing was also unsuccessful for the plaintiff. This
with regard to the allegation of a lack of emergency preparedness, increasingly entangled himself in
Contradictions, in particular by stating that no case of representation was presented
genes, since he was also provided with a deadline calendar and files in the hospital,
I just couldn't explain the statement of claim there. So the lawsuit was renewed
and now finally rejected.

9.2

Inventory data information: Legislative changes necessary

The Federal Constitutional Court ruled on May 27, 2020 (1 BvR 1873/13, 1 BvR
2618/13 "Inventory data information II") § 113 of the Telecommunications Act (TKG) and several
rere specialist laws of the federal government, which regulate the manual inventory data information, for with the
Basic Law declared incompatible and again constitutional requirements for the
structuring of the information procedure (follow-up decision to the decision of 24
nuar 2012 - 1 BvR 1299/05 "Inventory data information I").
The manual inventory data disclosure enables security authorities, from telecommunications

cation company information in particular about the subscriber of a telephone call
conclusion or at an IP address assigned at a specific point in time (dynamic
cal IP address). Customer data will be communicated in connection with the
conclusion or execution of contracts (e.g. address, account number
mer, so-called inventory data).

171

Chapter 9 Jurisprudence on Data Protection

The court affirmed that the legislature is responsible for the transfer of data by both
Telecommunications service provider and for the retrieval of this data by the authorized
authorities must create a reasonable legal basis that is clear in terms of norms.
These regulations must adequately limit the purposes for which the data is used by
they in particular factual encroachment thresholds and a sufficiently weighty one
provide legal protection. This includes the retrieval within the framework of security
and the activities of the intelligence services are fundamentally subject to a con-
concrete danger or for criminal prosecution of an initial suspicion. The assignment
dynamic IP addresses must also protect or enforce legal
serve goods of prominent importance. Furthermore, the retrieval regulations must
provide comprehensible and verifiable documentation of the basis for decisions.
The Federal Constitutional Court has ordered the federal legislature to § 113 TKG and the
subject-specific retrieval regulations by December 31, 2021 in accordance with the constitution
ten. With the resolution of November 25, 2020, the Conference of Independent Data
data protection authorities of the federal and state governments (DSK) in the interest of legal certainty
appeals to those responsible in politics not to exhaust this deadline, but rather to
closely to ensure that the procedure is constitutionally compliant. The DSK has itself
also advocated that federal and state legislators in the course of implementation
the decision all comparable provisions, the basis for the transfer and the

retrieval of personal data may be, in light of the requirements of the court over-

check. This applies in particular to the provisions of the police and constitutional protection laws

Countries that restrict the provision of information to the fulfillment of the tasks of the competent

tie the job. At my request, the Saxon State Ministry of the

Internally, there is already a need for changes to Section 70 (2) and Section 94 No. 1 of the Saxon Police Enforcement

service law (SächsPVDG). A corresponding instruction with the proviso that

that an inventory data information deviating from the wording of § 70 para. 2 SächsPVDG only

to avert a threat to sufficiently weighty legal interests (legal interests subject to criminal prosecution

or to prevent particularly serious administrative offences).

already in November 2020 to the police enforcement service. Furthermore, the Ministry of State

the consideration of the court decision in the planned amendment of the Saxon

promised by the constitutional protection law.

9.3

Jurisprudence of the European Court of Justice

international data transfer, C-311/18 – "Schrems II"

With a judgment of July 16, 2020, the European Court of Justice ruled that personal

Data from EU citizens is only transferred to third countries outside the European Economic Area

may be communicated if they have an essentially equivalent one in that third country

Enjoy protection like in the European Union. For the United States of America

172

9.4

a corresponding adequate level of protection was denied. The adequacy

conclusion of the EU Commission on the level of data protection in the United States, part of the

Agreements of the EU-US Privacy Shield, the data protection agreements between

between the European Union and the United States of America, was

Declared invalid by the court (see paragraphs 168 et seq. and 201 of the decision). reason were

unrestricted or disproportionate access to data, respectively

Surveillance by American security authorities and lack of legal protection against

access for those affected (cf. para. 179 et seq.).

On the other hand, the standard contractual clauses issued by the EU Commission - standard

standard data protection clauses - to bind the data processors outside the European

economic area continues to apply (paragraphs 127 et seq. and 149).

Compare also the article under 5.

9.4

Decision of the Federal Court of Justice on consent

in telephone advertising and in cookies for creation

of usage profiles for advertising purposes or

market research

The decision of the Federal Court of Justice of May 28 is of great practical importance

2020 - I ZR 7/16 - been. The decision is related to the judgment of

European Court of Justice on the requirements for consent in cookies for advertising purposes

cken (cf. the decision of the European Court of Justice of October 1, 2019, Case C-

673/17, presented in the activity report 2019, 9.10, page 172 ff).; see also 7.8).

The decision of the Federal Court of Justice concerns, on the one hand, telephone advertising in the

Within the meaning of Section 7 Paragraph 2 No. 2 Case 1 Act Against Unfair Competition (UWG) and a

effective consent to telephone advertising, namely when the consumer concerned

when declaring consent with a complex process of deselecting in a

list of partner companies listed, which may prompt him from

to refrain from exercising this choice and instead give the entrepreneur the choice

to be left to the advertising partner. Insofar as the data subject knows the identity and offers of the company

cannot take an overview, according to the Federal Court of Justice no effective

consent.

On the other hand, the decision relates to Section 15 (3) sentence 1 of the Telemedia Act (TMG). This
Part of the decision primarily came into the public eye because it
therefore on consent to cookies, text or program information, which in

are stored in the browsers of the users. According to this, Art. 5 Para. 3 Sentence 1
line 2009/136/EG (unofficial designation: "ePrivacy Directive"), the specifications for the
Data protection in the telecommunications sector regulates to be interpreted in such a way that the
Service provider cookies to create user profiles for advertising purposes or
Market research may only be used with the consent of the user. An electronically to be declared
The user's consent, which allows the retrieval of information stored on his device
information using cookies via a preset checkbox allowed,
satisfies the consent requirement of voluntariness according to the Federal Court of Justice
Not. The background was a procedure against the competition provider "Planet49", which
aim a check box with a preset tick used with that
Internet users should give their consent to the storage of cookies. Against it
the German Federal Association of Consumer Associations had turned to this.
According to the court decision, § 15 para. 3 TMG is to be interpreted in such a way that for retrieval
and the storage of cookies, the information in the end device of the user, in principle
the consent of the user of the website must be obtained, unless it is
(exceptionally) an "absolute necessity" within the meaning of Art. 5 Para. 3 Sentence 2 of the
Directive 2009/136/EG. Cookies that are necessary in this sense are programs
which enable the provided internet offer technically, functionally and optically, for example
play so-called session cookies, for example those that the login phase of a user
receive or control the language selection.
Especially in the case of tracking and advertising cookies, also and from third parties, will not be used by

to be assumed to be absolutely necessary. Whether this also with a consent

can be used under data protection law, the user must also check

fen.

To what extent, for example, analysis cookies are to be regarded as "absolutely necessary" is ultimately

finally still open. My authority strongly advises that the possibility of consent should also be

to offer.

9.5

Violation of Art. 32 GDPR –

Decision of the Regional Court of Bonn, Judgment of

November 11, 2020 – 29 OWi 1/20

A lawsuit against administrative offenses, which was continued in court, met with a great response in the media

tes procedure of the Federal Commissioner responsible for telecommunications companies

Data protection and freedom of information against a high-revenue company from

speaking sector because of the amount of penalty imposed. After a fine

in the amount of 9.55 million euros, the company sought legal protection for the headquarters of

174

9.6

regional court responsible for fines. As a result, the fine was paid by the state

court reduced to 900,000 euros. The court held that the benchmark was based on the turnover of the con-

Zerns-based assessment for no admissible criterion (cf. para. 91 et seq. of the decision).

The fine originally imposed was based on a violation of Article 32

Paragraph 1 of the General Data Protection Regulation (GDPR). Accordingly, the technical

and organizational measures taken by the person responsible are not sufficient.

The starting point for the identified data protection violation was that the company's call center

an unauthorized person, a former life partner who identified himself as the customer's wife

who issued the customer's new mobile phone number with their name and date of birth

knew how to get. In the possibility of authenticating oneself with scarce special knowledge
or to obtain customer data, the authority recognized a structural data
breach of protection, which was to be fined on the basis of Art. 83 Para. 4 Letter a GDPR. To the
the court followed in principle.
Apart from the amount of the fine, however, the court's decision on the question of
attribution of greater importance. After the decision, no concrete
to determine the responsible natural person in the company hierarchy. Pursuant to art. 83
GDPR, fines and the responsibility of companies have been finally regulated
the. In this respect, the court took the company for the action of a natural person
based on antitrust law and brought § 30 para. 1 Administrative Offenses Act
(OWiG) does not apply (cf. paragraphs 46 et seq., in particular paragraphs 53, 54 and 62 of the judgment).
As a result of the decision, the independent data protection supervisory authorities
of the federal and state governments further dealt with their concept of fines in order to
Identify adjustments to judicial adjudication practice and refinements.

9.6

Information according to Art. 15 GDPR by free
(Electronic) transmission of the treatment file

At the end of May 2020, the Dresden District Court issued the following judgment (Az.: 6 O 76/20):
The plaintiff demanded from the defendant, a Saxon university hospital, under
refers to Art. 15 Para. 3 General Data Protection Regulation (GDPR) free information about
the personal data stored with her. The plaintiff was in the university clinic
been in inpatient treatment, whereby from the plaintiff's point of view there were errors in treatment
has come.
The university hospital dispatched the documents from a cost assumption
plus shipping costs. In the court proceedings, she submitted that the right to information

be too vague. The GDPR is not applicable in this case. A right to information

am therefore only under § 630 g of the German Civil Code (BGB) under assumption of costs,

which the plaintiff just did not agree to.

The district court ruled as follows:

As a patient, the plaintiff is also subject to the special legal regulation of § 630g BGB

a claim under Art. 15 Para. 3 GDPR against the University Hospital.

The reason given is:

-
-
-
-

The area of application of the DGSVO is in the case of storage in the context of health

health treatment data is met. The processing takes place within the scope of the

activity of the defendant as a healthcare provider, which is expressly stated in the recital

reason (63) for the introduction of the GDPR.

It does not matter for what purpose (here it was civil liability

claims) the right to information is asserted.

The regulation of § 630 g BGB does not have priority over the provisions of Art. 15

Paragraph 3 GDPR. Consequently, a request for information, which is based on § 630 g BGB

Art. 15 Para. 3 GDPR is supported, to fully comply.

The defendant cannot claim the data transmission from the assumption of costs

Lich shipping costs dependent. Insofar as the plaintiff relies on Art. 15 para. 3

GDPR to justify their right to information is a claim

not provided for the costs of compiling and sending the data. the

Rather, initial information is free of charge. This is not opposed to the fact that in the case of a request

According to § 630g BGB, a cost bearing is also stipulated for the initial information.

A transmission in PDF format is a common electronic one

Format within the meaning of Art. 15 Para. 3 GDPR.

The decision is final.

176

9.7

9.7

Regarding the storage period of account statements in

Benefit Records

In its decision of May 14, 2020, Az.: B 14 AS

7/19, on the question of collecting and storing account statements in social service files

decided. Specifically, the plaintiff was concerned with the deletion of his account statements on the basis

17 of the General Data Protection Regulation (GDPR).

The main reasons for the decision are as follows:

1. A Benefits Authority has the authority to process a Benefits Application

Check the applicant's account movements and request account statements for this.

The required legal basis

for this data collection results from

Section 35, paragraph 2, first book of the Social Code (SGB I) in conjunction with Section 67 a, paragraph 1 sentence

1 SGB X.

2. When submitting bank statements, the admissibility of partial redacting

to assign.

The court had already ruled on this in its judgment of September 19, 2008, Az.: B 14 AS 45/07 R,

pointed out. For special types of personal data, it must be checked separately whether

the knowledge of which is required to fulfill the task of the collecting body. § 67 paragraph 12

SGB X lists information about racial and

ethnic origin, political opinions, religious or philosophical beliefs,

union membership, health or sex life. However, it must be ensured

ensure that the amounts transferred remain identifiable. It is therefore protected

only the secrecy of the intended use or the recipient of the transfer

instructions, not their amount.

3. Account statements may be filed for a period of ten years, i.e.

be saved.

Merely the reference to the preparation of file notes about a submission of con-

the court does not allow excerpts to be sufficient.

Also compare the entry under 3.3.1.

177

Publisher:

Saxon data protection officer

Andrew Schurig

Devrientstrasse 5

01067 Dresden

Postal address: PO Box 11 01 32, 01330 Dresden

Telephone 0351/85471-100

Fax 0351/85471-109

saechsdsb@slt.sachsen.de

www.datenschutz.sachsen.de

Cover photo:

Print:

New printing house Dresden GmbH

Edition:

1,500 copies

Publication:

June 2021

Relation:

for free

Central brochure dispatch of the Saxon state government

Hammerweg 30

01127 Dresden

Telephone: +49 351 210-3671 / -3672

publikationen@sachsen.de

www.publikationen.sachsen.de

Distribution note:

This activity report is prepared due to the obligation under Article 59

General Data Protection Regulation issued. He must not belong to any political party

nor used by their candidates or helpers for the purpose of election advertising

will. This applies to all elections. In particular, distribution to

election events, at information stands of the parties as well as the insertion, recording

print or stick on party political information or advertising material. is prohibited

also passed on to third parties for use in election advertising.