Activity report

of the Saxon

Data Protection Officer

Reporting period:

January 1 to December 31, 2021

Activity report

of the Saxon

Data Protection Officer

2021

Reporting period:

January 1 to December 31, 2021

Legal status: December 31, 2021

Data protection is protection of freedom

Andreas Schurig, Saxony's top data protection

officer until the end of 2021, and Dr. Juliane Hundert, now Saxon

Data protection officers, talk in an interview about

the tasks and challenges, the power of tech companies

and the joy of a good book.

Machine Translated by Google

Mr. Schurig, you have now resigned as Saxon Data Protection

Officer. Is there any advice you would like to pass on to your

successor?

Schurig: No, because every generation faces its own tasks and

challenges, and I am convinced that Dr. Hundred will master theirs well.

Already

before my first term as Saxon Data Protection Officer

I worked as a commissioner in the authority. I still remember my early

days in 1993. At that time there was no internet connection. Compared

to today, electronic data processing was in its infancy.

Miss Dr. Hundred with what feelings you have your

new office?

dr Hundred: With a good one! I know Mr. Schurig and

most of the employees do

longing. He significantly shaped data protection in Saxony. I have great

respect and appreciation for his achievement; not only as the new head

of the authority, but first and foremost as a citizen. Together with my coworkers

I would like to do this work

now continue. And I look forward to new challenges

ments.

What is data protection for you personally?

dr Hundred: I am a child of the GDR. I still have from her

noticed so much that I know what it's like when the

State penetrates deeply into private life and systematically

spying on the population. For me, data protection is therefore

primarily a right of defense against the state. Nevertheless we live

today at a time when the threat to our freedom is also coming from a

different direction. By that I mean the tech companies that have made

spying on their customers their business model. My dealer around the

corner would have been my business partner for the longest time if

he me after a visit to his shop on mine

the following way to other shops so that he can offer me better products

next time

fit my needs. But that's exactly what we're allowing on the Internet - and

many people don't realize that it is

so is. Data protection is also about clear rules among private individuals.

With the General Data Protection Regulation and national law, the EU

and the Federal Republic of Germany have created regulations that are

intended to enable us to protect our freedom and privacy, also vis-à-vis

companies. The citizens can count on my support.

Schurig: That is an aspect that I can only emphasize.

There is a manageable number of tech companies that have become

incredibly powerful. They can hardly be regulated. Of course we still

have to try that

put these corporations in their place. They too must

adhere to the rules of the game, which are essentially laid down in the

General Data Protection Regulation. However, it is much more important

that we – those responsible and users – handle our data or the data

entrusted to us with care. We have to keep reminding ourselves:

Data protection is protection of freedom!

Miss Dr. One hundred, as of January 1, 2022, you are the one

Saxon data protection officer and are now presenting their first

annual report in accordance with the General Data Protection

Regulation. However, it documents the work of your predecessor.

Surely that wasn't an easy task, was it?

dr Hundred: First of all, I would like to thank Mr. Schurig for the excellent

transfer of office. This enabled me to familiarize myself quickly. Some

oversight operations included in

can be read in this activity report, have me be

already during my time as a parliamentary adviser

and legal advisor to the Bündnis 90/Die Grünen parliamentary group in

the Saxon state parliament. These include, among other things, data

protection issues in connection with the pandemic measures. The real

challenge was rather to identify the important events that I had not

previously known about, but which are just as interesting and helpful for

data protection officers and the public.

Mr. Schurig, how was data protection in 2021?

Saxony ordered?

Schurig: It was the second year of the pandemic. That demanded a lot

from data protectors everywhere. Because sometimes the data protectionfriendly solutions are associated with some effort. I

am thinking, for

example, of the correct handling of health data; i.e. when entering contact

data or when the employer requests vaccinations, recovery and tests.

Here, however, data protection has once again proven that it does not

stand in the way of containing the pandemic, but rather ensures

transparency and thus broad acceptance of the measures. The Corona

Warn app is a prime example of this. Of course, data protection had to

be used again in 2021 to distract from our own failures and a lack of

regulation, for example in the billing scandals in Corona test centers.

That those responsible prefer to blame the

looking for others never seems to go out of fashion. the co

rona measures were only one topic, with

which I dealt with in the reporting period. Also at

I contributed to the Register Modernization Act, we also dealt with the

implementation of the Schrems II judgment, cookies and tracking on the

Internet and much more.

Miss Dr. Hundred, there is obviously no lack of topics,

or how do you rate that?

dr Hundred: (laughs) No, definitely not. The Transparency Act will soon

be added, according to the Saxon

cal state parliament decides. The course was set for this

in the reporting period. Then, like almost all federal states,

Saxony also has a law that regulates the information

freedom rules. The draft stipulates that my authority has

to investigate possible complaints. If citizens are of the

opinion that the state is withholding information from

them that it must provide under the Transparency Act,

those affected can in future

I hope to contact my authority.

Do new challenges also need new ones?

structures?

Schurig: I think that reinforcements are needed, especially

in terms of personnel. Data protection problems have

increased with digitization. New tasks are already on the

horizon, such as checking systems that use artificial

intelligence.

This must also be reflected in the official equipment

hit. With more staff, the authority could also check compliance with data

protection better, for example with unannounced checks. That was only

possible to a very limited extent in 2021.

dr Hundred: With the eight new posts that land us

tag made available last year, however, we are taking a big step forward.

But you are right: the increase in tasks that the supervisory authorities

have had to deal with with the introduction of the General Data Protection

Regulation is enormous. Just the vote

with the other regulators requires a lot more

time than before. And it is good that you, Mr. Schurig, have also made

an effort to further develop the data protection conference. Under the

leadership of Saxony, the DSK 2.0 working group prepared a number of

important specifications last year. In essence, it is about the harmonization

of data protection supervision in Germany.

The innovations include, for example, a weekly video conference at

management level, in which the DSK members coordinate on current

topics. I will do my best to promote cooperation within the

Develop data protection conference.

Mr. Schurig, how will you use your free time now?

Schurig: How am I going to spend my time? This is subject to data

protection! (laughs) More time for the family and a good book more often

– I'm really looking forward to that.

dr Hundred: I wish you a lot of joy and hope

fe that you remain committed to data protection - and that I can call you

again and again if I have any questions (laughs).

All the best!

|9

Table of contents

List of Figures

List of abbreviations

Below are laws and other regulations

listed in alphabetical order of the official abbreviation, in

exceptional cases also non-official abbreviation,

alternatively the official abbreviation.

regulations
TO THE
tax code
Residence G
Residence Act
BarchG
Federal Archives Act
BDSG

Civil Code

Federal Data Protection Act

Civil Code

BMG

Federal Registration Act

BZRG

Federal Central Register Act

CoronaSchutzV

Coronavirus Protection Ordinance

GDPR

General Data Protection Regulation

eKFV

Small Electric Vehicles Ordinance

GG

Basic Law for the Federal Republic of Germany

GKDZ-StV

State treaty on the establishment of a common

Competence and service center of the police forces of the

states of Berlin, Brandenburg, Saxony and Saxony

Anhalt and Thuringia on the territory of the police

Telecommunications surveillance as a legal entity

public law

GMO

bailiff regulations

GVGA

Business instructions for bailiffs

IfSG

German Infection Protection Act

IfSGZuVO

Infection Protection Act - Competence Ordinance

JI-RL

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

ArtUrhG

Law on copyright in works of

OWiG

Administrative Offenses Act

SaxonArchiveG

Archive law for the Free State of Saxony

fine arts and photography

SächsBRKG

Saxon law on fire protection, rescue services and civil protection

SächsCoronaNotVO

Saxon Corona Emergency Ordinance

SächsCoronaSchVO

Saxon Corona Protection Ordinance

SächsDSG

Saxon Data Protection Act

SaxonDSDG

Saxon Data Protection Implementation Act

SächsGemO

Saxon Municipal Code

Saxon ME

Saxon Lawyer Training Act

Saxon JAPO

Saxon legal training and examination regulations

SächsISichG

Saxon Information Security Act

SächsPet AG

Saxon Petitions Committee Act

Saxon PVDG

Saxon Police Enforcement Service Act

SächsStVollzG

Saxon prison law

SächsVwKG

Saxon Administrative Costs Act

SaxonVwOrgG

Saxon Administrative Organization Act

SächsVwVG

Administrative Enforcement Act for the Free State of Saxony

SchulKitaCoVO

School and Kita Corona Ordinance

SGB

social code

StPO

Code of Criminal Procedure

StVZO

Road Traffic Licensing Regulations

TestV

Coronavirus Testing Regulation

TTDSG

Telecommunication Telemedia Data Protection Act

UWG

Unfair Competition Law

AWAY

Homeownership Act

WEMoG

Condominium Modernization Act

ZPO

Code of Civil Procedure

Miscellaneous

Abs.

Unit volume

Art.

Article

The.

File number

BAG

Federal Labor Court

BASt

Federal Highway Research Institute

BGH

Federal Court of Justice

BR-Drs.

Federal Council printed matter

BSI

Federal Office for Security in Information Technology

BT-Drs.

Bundestag printed matter

16 |

Machine Translated by Google

letter

Letter

BVerfG

Federal Constitutional Court

BVerwG

Federal Administrative Court

DSK

Conference of independent data protection officers

Federal and state data protection conference

ECtHR

European Court of Human Rights

eKF

micro electric vehicle

EU

European Union

GKDZ

Joint competence and service center

Police forces of the states of Berlin, Brandenburg, Saxony, SaxonyAnhalt and Thuringia in the area of the police

Telecom Surveillance

K. d. ö. R.

Public corporation

LaSuB

State Office for Schools and Education

LDS

State Directorate of Saxony

LG

district Court

LJK

State Justice Fund

LJP

MY STOMACH

State Judicial Examination Office

Mercator Forum Migration and Democracy

OLG

Higher Regional Court

OVG

Higher Administrative Court

item no.

marginal number

SMI

Saxon State Ministry of the Interior

SMK

Saxon State Ministry for Culture

SMS

Saxon State Ministry for Social Affairs and Society

St.A

Public prosecutor

social cohesion

SVN

Saxon administration network

TOA

Offenders victim Compensation

Wow

administrative regulation

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*

2.2.11

order processing

see 3.1.3, 3.1.4, 4.2.1, 4.2.2,

4.2.3, 4.2.4, 5.1

Beliehene*

• Doctors

• Health Professions

• Miscellaneous, general

2.4.4, 2.4.6

| 19

Machine Translated by Google

Trade, services, trade, industry • Credit agencies,

debt collection service providers, detective agencies

• Banks, finance

• Trade, see also internet/e-commerce

• Craft, trade, industry

3.1.3

• Hotel and gastronomy, leisure, tourism, sports • Insurance;

2.3.2, 2.4.2

see if necessary social affairs, service providers

9.3

• Advertising, market and opinion research

• Miscellaneous, general

3.2.2

Infrastructural Sector

• Energy, water and utility industry • Traffic and

transportation • Housing industry, real estate management

2.2.7

• Data centers

• Miscellaneous, general

Internet, media, communication

social affairs

• social authorities*

2.4.3, 6.1.2

• Day care centers

• Service providers •

Miscellaneous, general

2.4.4

Statistics*

2.2.10

For technical and organizational measures, see

see 5.1

security of processing, if applicable, see list of processing

activities, if applicable

Clubs (also parties), associations, foundations

see 2.3.2

transportation

2.1.1, 2.2.4

Administration*

• General, basic • Specialist

2.2.1

administration* (e.g. building

1.2, 2.2.8

administration, immigration authorities)

• Financial, tax and subsidy management*

(incl. municipal offices)

• Municipal self-government* • Registration

2.2.11, 4.1.4, 6.3.2

authorities* (including the right to register,

2.2.11

civil status)

| 21

Machine Translated by Google

Videography and image processing •

Official monitoring/processing* • Employees, cf.

otherwise

employee data processing

• Dash cam, drones

6.4.2

• Trade, business

• Residential areas

• Miscellaneous, general

2.2.4, 2.2.5, 2.2.6, 2.4.2,

3.1.2

right to vote*

see 3.1.1

Certification, accreditations, seals of approval

see 6.2.8

Directive (EU) 2016/680

Police*

see 2.4.5 and 2.4.6, 6.4.1

Administrative offense authorities*

see 2.1.1 and 6.1.3

Preliminary note on the use of language

In this activity report, the generic masculine is used

below to indicate the flow of reading

and to facilitate understanding. Of course

however, all genders are meant. For reasons of grammatical

correctness and correct use of the present participle,

substitute forms are used

such as users or users waived.

1 Data protection in the Free State of Saxony

1.1 Processing of employee health data during the corona pandemic

ÿ § 26 BDSG; Art. 7, 9 GDPR; Saxon CoronaSchVO

In the past reporting period, my authority had to deal with the measures to combat the pandemic and the associated data protection issues to a considerable extent, which also affected employee data protection. The various problems are presented below in a chronological order.

As part of the corona pandemic, the Saxon Ordinance Infection protection measures are regulated by the Saxon Corona Protection Ordinance (SächsCoronaSchVO), which also had and continue to have an impact on the employment relationship. These regulations led to a wide range of questions in the area of labor law and data protection and regularly moved between the poles of effective protection against infection.

At the federal level, too, the legislator has attempted to regulate the labor and data protection issues arising from the measures to protect against infection, such as the employer's right to ask questions about the vaccination status of employees, by amending the Infection Protection Act several times.

Corona-Tests

Newly developed options for containing the corona pandemic, such as

antigen self-tests, allowed employers to offer them to their employees as early as the beginning of 2021. This resulted in a number of labor and data protection issues.

My authority was therefore already in January 2021 with the Request for advice from an international company, which also has branches in Saxony, on the data protection-compliant implementation of corona tests employees including the associated data processing, in particular of test results, confronted. Since this company has more branches genes in other federal states and thus the responsibility of other German supervisory authorities was given, a response from the responsible supervisory authorities was sent via the employee data protection working group to the company coordinated.

In my opinion, this set the first standards with regard to data protection requirements

Processing of employee health data

As part of the corona pandemic, especially in Be regarding the processing of corona test results, the relevant legal basis on which such processing of health data can be based at all, and with regard to technical and organizational measures to be implemented by the person responsible.

Among other things, the requesting company was informed that the processing of personal data in the context of carrying out the corona selftests is not based on Section 26 (3) sentence 1 of the Federal Data

Protection Act (BDSG), Art.

9 Para. 2 Letter b General Data Protection Regulation (GDPR) can be

supported. According to these regulations, employees' health data can be

processed if the processing is for the purposes of the employment

relationship, to exercise rights or to fulfill legal obligations under labor law,

the law

of social security and social protection

is and there is no reason to believe that the protection

worthy interest of the data subject in the exclusion of processing prevails.

For what purposes may the test

and health data are processed?

However, there were already considerable doubts as to whether the

coronavirus self-test for infection

health data collected with the coronavirus SARS-CoV-2

data should be processed for the purposes of the employment

relationship or for the purpose of combating a pandemic by preventing

infection. Also from the point of view that testing employees could serve

employers' duty of care towards their employees and thus also serve

the purposes of the employment relationship, employers may only

process an employee's health data pursuant to Section 26 (3) BDSG in

order to fulfill their duty of care towards the employee employees

affected by the data processing themselves. The fulfillment of legal

obligations towards third parties does not entitle the employee affected

by the processing of his or her personal data to be processed.

Duty of care as a processing purpose?

The general labor law duty of care pursuant to Sections 611a, 242 (2) of the German Civil Code (BGB) also did not oblige the employer to have the workforce tested for Covid-19 and thus to process the employee data required for this, including health data. Another argument against such a general obligation on the part of the employer was that the legislature had only recognized a test obligation for employees in very few cases by means of special regulations. Even the ordinance on the entitlement to testing in relation to direct detection of the pathogen of the SARS-CoV-2 coronavirus (coronavirus test ordinance - TestV) of November 30, 2020 "only" regulated a claim

certain groups of people to be tested under the conditions specified in Sections 2 to 4 of the TestV, but not one that is independent of the exercise of this right

Obligation of the relevant institution to carry out tests

respectively. In January 2021 there were only a few rights regulations that established a real obligation to conduct tests. The character of these – very few – statutory regulations as special standards, which provide for a test obligation, would be undermined if an obligation to carry out tests on employees were derived from the general labor law duty of care of the employer that goes beyond the special statutory standardized groups of employees.

Those responsible were also informed that such an
obligation could not be derived from Section 3 (1) of the
Occupational Safety and Health Act. No specific legal
obligation can be derived from the general requirements
of occupational health protection mentioned. Rather, the
assumption of a legal obligation on the part of the
employer would run counter to the above-mentioned
legislative decision to only provide for a test obligation in
the explicitly regulated cases. There was therefore no
corresponding obligation on the part of the company and no right e
to demand that such tests be tolerated; However, this would be
a prerequisite for the application of Art. 9 Para. 2 Letter b GDPR,
Section 26 Para. 3 Sentence 1 BDSG.

Public interest in the public domain
health as purpose?

A controller cited Art. 9 (2) (i) GDPR, Section 22 (1) No.
1 letter c, paragraph 2 BDSG (public interest in the field of public
health). However, the task of health care does not justify a general
authority of companies to process health data.
The regulations refer to their wording and their development
development history on the public health

wesen and health administration, insofar as it is carried out by public
and non-public bodies. This also results in particular from the reference

to compliance with professional and criminal law requirements for maintaining professional secrecy. In addition, such processing of health data for reasons of public interest must not result in third parties under another employer to process such personal data for other purposes; Recital 54 GDPR.

However, since the company “only” wanted to test its own employees and third-party employees who work for the company, this was not the case

public interests in the field of public health

health, but the productivity of the individual business premises should be maintained by avoiding major infections.

Consent as the legal basis for processing

The company was therefore informed that, according to the data protection supervisory authorities involved, only Art. 9 (2) (a) GDPR, Section 26 (2) in conjunction with (3) sentence 2 BDSG could be considered for the notified data processing, i.e. the consent of the employees.

Data processing in the employment relationship, which is based on consent, must always be examined extremely critically due to the existing relationship of dependency. Above all, the criterion of the voluntary nature of consent is mostly not met. In particular, pressure from the employer, which could influence the employee’s free decision, disadvantages, direct or in a direct way, which the employees could suffer if they decide not to carry out the tests, lead to doubts about the voluntary nature of the test and ultimately to it ineffectiveness of the consent.

The person responsible was also informed that the employees must be

comprehensively informed about all essential aspects of data processing,

such as storage duration, in order to be able to

validity of the consent within the meaning of Art. 4 No. 11 GDPR

ensure.

voluntary consent

The company announced that it is planning for this project

To use self-tests carried out in the laboratory of a subsidiary

should be evaluated by the company and this in turn

would communicate the test results to the respective

company branches. For this reason, the company was

informed that the consent also includes the transmission

of a possible positive test result to the employer and

therefore also to be transparently informed as to which

officials of the employer this transmission would take

place. In this regard, it would only be assumed that the

consent was voluntary if the employer did not receive any

feedback on the negative test results or which employee

accepted the test offer or not. Otherwise, employees

would have to fear that if they did not take advantage of

the test offer, they might suffer some indirect

disadvantages. Such fears must be avoided, however,

because this is the only way to dispel doubts about the

voluntariness of consent given the imbalance between

employer and employee

become.

The person responsible was also informed that according

to Art. 7 Para. 3 Sentence 1 GDPR, the employees must

be informed that their consent can be revoked at any

time and that in the event of a revocation the personal

data may not be processed further.

Technical-organizational measures, establishment

of a "trust center"

Due to the dependencies existing in the employment

relationship and any associated effects (such as

termination), which result from the

processing of health data can result

to place special requirements on data protection-compliant data

processing. Also with regard to the fact that the employer or the personnel

administration, in deviation from legal regulations and the right to ask

questions under labor law, gain knowledge about the specific health

conditions of employees, technical and organizational measures for

compensation are in return

to perform.

The responsible company was therefore informed that it was responsible

for the notified data processing within its

Personnel administration has to form an informationally isolated trust

point where the information

receive positive tests. This organizational unit must be described

transparently with regard to data processing and staffing and must be

managed according to Art.

37 GDPR designated data protection officer

become.

The number of trust center employees and their access to the test

health information received

ments must be minimized to the required level.

The health data collected must be processed independently of the

processing of other employee data. This means that this health data

may not be processed in the personnel file or in any other way. When it

is passed on to functional units for personnel deployment planning, the

person responsible must therefore develop a procedure in which the

identities of employees who have tested positive cannot be revealed to

shift supervisors, supervisors, etc.

test obligation

After at the beginning of the year employees were only tested for the

presence of an infection with SARS-CoV-2 in special facilities, such as

nursing homes, the Saxon legislator stipulated in the SächsCoronaSchVO

of March 5, 2021 that all employees ten and self-employed with direct

customer contact from 15.

March 2021 once a week a test for the Corona virus

rus SARS-CoV-2 have to carry out or are obliged to

to have this done.

From March 22, 2021, employers were obliged to offer their employees

who are present at their workplace the opportunity to carry out a free selftest at least once a week

wide.

My authority received a large number of inquiries about this as well

gen, which mostly included the question of whether this regulation entitles

the employer to record the test results.

I was able to inform those affected that the employer is not authorized to

process the positive or negative test result. Rather, this regulation only

obliges the employer to provide evidence that he offered his employees

the test.

Compulsory testing for people returning from vacation

With effect from July 26, 2021, the Saxon legislator then introduced a

test requirement for so-called “holiday returnees”. According to this,

employees who have not worked for at least five consecutive working

days due to vacation and comparable official or work exemption had to

submit a daily updated test to the employer on the first working day after

this work interruption or carry out a documented supervised test during

the course of the first working day.

If the work started in the home office, this obligation applied for the first

day on which the work takes place in the company or at other locations

outside of one's own home. The granting of inspection of the test or

vaccination certificates together with an official identity document in the

original should be sufficient for the documentation.

More information:

For this I have stated on my website that

ÿ sdb.de/tb2101

From a data protection point of view, the control of the test evidence

se by submission by the employees without them

Tests or controls with a personal reference are documented, are the

mildest means and accordingly

processing of this data is not permitted. Instead, employers can only

document that they have a process in place to carry out such controls.

The mere documentation of a corresponding control process seemed

sufficient in this respect, since Section 9 (1a) of the SächsCoronaSchVO

of July 14, 2021 only regulated an obligation for employees to submit,

but no specifications with regard to an obligation on the part of the

employer to provide more extensive documentation and the associated

processing of personal data dates met.

If employees were fully vaccinated against SARS-CoV-2 or had

recovered from a SARS-CoV 2 infection, Section 9 (7) of the

SächsCoronaSchVO in the version of July 14, 2021 stipulated that these

employees were not obliged to Submission of test evidence exists,

insofar as these prove that they have a full

are constantly vaccinated against SARS-CoV-2 or have recovered from

a SARS-CoV-2 infection.

This could also be taken into account in a corresponding control system.

However, the documentation of the vaccination or recovery status was

also subject to data protection law

From our point of view, not according to § 9 paragraph 1 a and paragraph 7 of the SächsCorona

SchVO of July 14, 2021, in particular the vaccination or proof of recovery

may not be copied.

Question from the employer about the

vaccination or convalescence status

After the vaccines against Covid-19 were no longer given as a priority

in the summer of 2021, but were available to large parts of the

population, and it was feared that the number of infections could rise

again in late summer and early autumn, the question increasingly arose

as to whether employers have the right to ask their employees about

their vaccination or recovery status. Until then, a legal regulation for

processing the vaccination and serostatus only existed for employees

of certain facilities, such as hospitals, according to § 23 a in conjunction

with § 23 In-

infection protection law. For all other areas, the general labor and data

protection regulations applied, which in practice often led to legal

uncertainties as to whether there was a right to ask questions or not. In

particular, it was discussed whether the vaccination status could be

queried with the consent of the employee.

Already on March 29, 2021, the conference of the independent

The data protection supervisory authorities of the federal and state

governments (DSK) published a resolution in view of these expected

DSK resolution : ÿ

sdb.de/tb2102

legal uncertainties, which called on the legislator to create corresponding clear legal regulations.

Processing of vaccination status on a consent basis

My authority then also received a request from an airline that wanted to clarify whether they were allowed to process the vaccination status of their pilots as part of a consent. The airline informed me that health authorities in other countries would not recognize the pilots' vaccination certificates (including international ones), but would insist on confirmation from the employer regarding the vaccination status. In some cases – according to the airline – entry regulations have been further tightened, so that pilots who have previously stayed in certain countries countries were only allowed to enter if they were vaccinated and had a PCR test carried out, or if they were not vaccinated, a three-week quarantine would be ordered. Due to these circumstances, the person responsible now wanted to process the vaccination status of the pilots as part of a consent in order to avoid quarantine and longer waiting times for the pilots in the airport area.

I first informed the responsible body that the data on the vaccination status was health

data within the meaning of Art. 4 No. 15 GDPR and thus special re categories of personal data within the meaning of Art. 9 Para. 1 DSGVO. The processing of special categories of personal data is generally prohibited under Art. 9 Para. 1 GDPR if the data specified in

GDPR are not relevant. The access of the employer to the health data of the employees is only possible to a very limited extent for reasons of privacy protection. In principle, there is no right to knowledge of health data. For example, the certificates of incapacity for work for the employer may not contain any diagnoses, cf. § 69 para. 4 SGB X.

Incidentally, there was no vaccination requirement in Germany at that time. Section 23a of the Infection Protection Act (IfSG) only provides for the processing of vaccination data by the employer for special reasons of pandemic control (for facilities according to Section 23 (3) IfSG, such as hospitals). This express legislative value decision to affirm and regulate a right to ask questions only in individual cases also makes it clear that a general authorization to process the information on the “vaccination status” is not to be assumed.

In this case, too, the only legal basis for the notified data processing was consent in accordance with Art. 9 paragraph 2 letter a GDPR, § 26 paragraph 2 in connection with paragraph 3 sentence 2 BDSG, since neither the SächsCoronaSchVO other legal provisions, apart from professional groups

expressly named by law (cf. § 23 a, § 23 para. 3 IfSG), provide for a processing authority and the associated documentation obligation of the employer with regard to the vaccination status. Accordingly, my authority has informed the responsible body that if the information on the "vaccination status" is processed by the employer on the basis of express consent in accordance with Article 9 (2) (a) GDPR, the specific requirements for the effectiveness of the consent would have to be observed in the employment relationship, in particular with regard to the voluntary nature (Art. 4 No. 11 GDPR). Furthermore, the requirements according to Art. 7 GDPR and § 26 Para. 2 BDSG have to be fulfilled. Despite the high requirements that are to be made of the consent and in particular the criterion of voluntariness in the employment relationship, this is

not excluded in the employment relationship.
Pursuant to Section 26, Paragraph 2, Clause 2 of the Federal Data Protection Act, voluntary work can be the case, in particular, if a legal or economic advantage is achieved for employees or if employers and employees are pursuing the same interests. In my opinion, in the case presented to me, the processing of the vaccination status by the employer on the basis of consent to avoid

having to “perform” an officially ordered quarantine or
longer stays in the airport building was equally
advantageous for both the employer and the pilot.
According to the descriptions of the facts presented to
me, this was not only advantageous for the employer,
especially with regard to his economic interests in
preventing quarantine-related absences. It was also advantageous
Arranging quarantine or long-term stays in the airport
building, which would reduce their rest periods,
to avoid.
The data protection-compliant query of the vaccination
status by the employer, based on consent, was therefore
an absolute exception. In addition to the high requirements
that are placed on consent that is effective under data
protection law, the legal basis for consent for the employer
is also a variant associated with considerable risks due to
the possibility of revocation of consent at any time. Priority
should therefore be given to examining whether other
legal bases could be considered.
I have also informed the responsible body of the
additional requirements for data protection-compliant
consent, which were already published in the 2019
Activity report 2019: ÿ
activity report. In this case, too, I have informed that the
sdb.de/tb2103
responsible office within their company has to set up an

informationally isolated trust center – which is separated
from the personnel administration office – to which
information on the vaccination status is received. The
health data collected must be independent of the
processing of other employee data. It would therefore
have to be ensured that the

sonally managing body does not receive any knowledge/information
as to who has given his vaccination status to the informationally
Schotten trust agency has revealed and who does not and
of course not about the actual vaccination status. That meant further
that these health
do not process the data in the personnel file or in any other way
may be tested. In particular, this data must not
be disclosed to superiors etc.
I have informed the responsible body that
this processing of employee health data requires a data protection
impact assessment in accordance with Art. 35 GDPR and the processing
of this health data is included in the list of processing activities in
accordance with Art.
30 GDPR should be included. It was recommended to reach a
corresponding agreement with the works council, which also has
normative effect and which takes into account the data protection
requirements described above (cf. Section 26 (4) BDSG).

§ 36 paragraph 3 Infection Protection Act

With Section 36 (3) IfSG, on September 10, 2021, the federal legislature regulated for certain facilities, such as schools and day-care centers, that in the event of an epidemic situation of national significance determined by the German Bundestag, the employer - insofar as this is to prevent of the spread of COVID-19 is required – may process personal data of an employee about his vaccination and serostatus in relation to the coronavirus disease-2019 (COVID-19), about the establishment of an employment relationship or about the nature of an employment to decide.

For all other employees, for whom the legal exemptions of Sections 23a, 23 and 36 (3) IfSG do not apply, the general labor and data protection regulations remained.

2G-Optionsmodell

Therefore, with the inclusion of a 2G option model in the Saxon Corona Protection Ordinance of September 21, 2021, the question arose again for many employers as to whether they should be allowed to inquire about the vaccination and

More information:

serostatus of their employees. My authority has a comprehensive position

ÿ sdb.de/tb2104

taken.

In certain areas, the so-called 2G option model made offers

exclusively for vaccinated and recovered people in which there
is no obligation to wear a face mask, no obligation to comply
with the distance requirement, and no restrictions on the
utilization of the maximum capacity. The prerequisite for the 2G
optional model was that all those present had proof of vaccination
or a proof of recovery. In accordance with Section 6 a (1)
sentence 2 SächsCoronaSchVO of September 21, 2021, this
did not apply to employees who have proof of a test and who
wear medical mouth and nose protection for the duration of the
event or the offer. If an employer wanted to introduce the 2G
option model, the question arose in practice as to whether the
employer should disclose the vaccination and recovery status
or the result of a test for the absence of an infection with SARSCoV-2 from their employees employees may request.
My authority is of the opinion that the introduction of the 2G
option model for his company does not regularly entitle the
employer to process the vaccination or recovered status of the
individual employee. Rather, it requires a clear statutory legal
basis. A special statutory permit within the meaning of Art. 9
Para. 2 Letters b, h and i GDPR for the processing
As already stated, the processing of data on the vaccination and
serostatus provides for Section 23a Sentence 1 IfSG for the in Section 23 Para.
3 IfSG listed employers in the healthcare sector (including
hospitals, rehabilitation facilities, day clinics, medical and dental
practices, outpatient nursing services, rescue services). The
processing of the vaccination status of the

Employees is therefore only permitted by the employers named in Section 23 (3) IfSG. The amendment to the IfSG of September 10, 2021 stipulated that for the duration of the epidemic situation of national scope and insofar as this is necessary to prevent the spread of the coronavirus disease 2019, employers from in § 36 para. 1 and 2 IfSG-designated institutions (e.g. day care centers, after-school care centers, schools, homeless shelters) may also process the vaccination and serostatus in relation to the coronavirus disease 2019 to decide on the establishment of an employment relationship or on the type of employment, see Section 36 (3) IfSG.

As part of the so-called 2G option model, which was mainly used by restaurants, bars and clubs, employers therefore have to check on the basis of the general data protection law basis whether there is a right to ask questions about the vaccination and serostatus and whether data processing is based on this can.

In the above-mentioned statement, my authority pointed out that in this case the processing of this health data of employees could not be based on consent. Section 26 (3) sentence 1 of the German Federal Data Protection Act (BDSG) is also generally not considered as a legal basis, since there is no legal obligation under labor law, social security law and social protection is recognizable, since the requirements for

the qualified necessity of processing the vaccination status
according to § 26 paragraph 3 sentence 1 BDSG are not given.
In my view, the newly created § 6a SächsCoronaSchVO in
the version of September 21, 2021 by the Saxon legislature
could not be used as a legal basis for the processing of the
vaccination or convalescence status or test results by the
employer within the framework of the 2G option model, since
Section 32 sentence 1 in conjunction with Section 28 (1)
sentences 1 and 2, Section 28a (1), (2) sentence 1, (3) and
(6) IfSG in the version of July 23, 2021 none

provided the Saxon legislator with appropriate regulatory
competence for this data processing.
Furthermore, the wording of § 6a SächsCoronaSch VO did
not provide for an obligation to present proof of vaccination
or proof of recovery. The employer was also not authorized
to process the result of a corona test to determine that the
employee was not infected with SARS-CoV-2.
As previously stated, the results are
of corona tests to include health data within the meaning of the
Article 4 paragraph 15 GDPR. The above statements on
processing the vaccination and serostatus apply accordingly
to the processing of this employee data.
The processing of this health data could not be based on §

6a SächsCoronaSchVO, either, as this only stipulated that employees must have proof of a test, which became an obligation to submit, deviating from § 5 Para. 3 SächsCoronaSchVO in the version of September 21 2021 (compulsory testing for people returning from vacation), currently not regulated.

For this reason, the employer's right to ask questions about the vaccination and convalescence status as part of the socalled 2G option model had to be denied. Furthermore, the employer regularly had no right to ask questions about the result of a test for the absence of an infection with SARSCoV-2. It was therefore up to the responsible health authorities to check compliance with the requirements of § 6a SächsCoronaSchVO.

Application help of the DSK

Since a large number of questions about the processing of employee data have to be answered in connection with the corona pandemic, the conference of the independent data protection supervisory authorities of the federal and state

DSK application help : ÿ sdb.de/tb2105

governments has published an application guide.

This includes, among other things, statements on the subject of whether employers check the vaccination status of employees in connection with compensation under Section 56 (1) IfSG (so-called quarantine compensation) ver

are allowed to work and which data protection issues or requirements result from § 28b IfSG in the version of November 22, 2021 from the so-called 3G regulation at the workplace.

Introduction of an obligation for employers to check the pandemic health status

According to § 28b IfSG, employers are now obliged to check whether employees who enter their workplace have been vaccinated, recovered or tested (duty to check).

For reasons of data minimization and data economy in accordance with Art. 5 GDPR, it is sufficient for the employer or employees or third parties commissioned by the employer to view the proof of vaccination, convalescence or test.

Proof can be provided digitally, for example using the CovPassCheck app from the Robert Koch Institute.

If third parties are entrusted with the fulfillment of these tasks, an order processing contract may have to be concluded. In particular, this should contain regulations on the non-disclosure obligation of the third party.

Employers who are deployed must also be made aware of the duty of confidentiality by the employer.

Employers also have the option of implementing simplified control processes for the “vaccinated” or “recovered” status. With an effective consent, the employer can record whether the employee has been vaccinated or recovered

and, if applicable, the end date of the respective status.

However, a copy of the vaccination or recovery certificate

is not required.

If employees provide 3G proof by means of a test

certificate, the above statements apply.

If proof is provided as part of operational testing or by

means of self-tests under supervision,

note that it only records that proof has been provided; the

negative test result must not be processed. If the test is

positive, it can be noted that the employee is not allowed

to enter the workplace. Additional reporting obligations,

such as

to the responsible health authority, may result from

further regulations.

Employers' obligation to document

Employers must document compliance with the

aforementioned obligations, Section 28b (3) sentence 1

IfSG. It is not clear from the wording of the law in what form –

in particular what degree of differentiation – the

documentation has to take place. Employers have

established processes to check the access requirements.

Regularly documenting these processes will therefore be

sufficient to fulfill the documentation obligation.

Also in 2022 I expect a large number of jobs

and data protection issues in the employee context in

connection with the corona pandemic.

1.2 Easier data transfer

within city administrations

under the GDPR?

ÿ Art. 6 para. 4 GDPR; §§ 3, 4 Saxon GDPR

The data protection officer of a large city administration

asked whether anything significant had changed with

regard to data transfers within a municipal administration

after May 25, 2018, i.e. after the applicability of the

General Data Protection Regulation (GDPR). He was

also interested in the continued validity of the principles

of necessity for the fulfillment of tasks, the ban with the

reservation of permission and the informational separation

of powers. The data protection officer received the

following reply from my authority: Art. 6 (4) GDPR also

gives public bodies the option of purpose-compatible

further processing, i.e. processing that is close to the

original purpose of collection, but is not congruent. There

are different views as to whether Art. 6 Para. 4 GDPR

applies to its function

some kind of compatibility test limited or beyond

also as a permit for a purpose-changing Wei

processing is to be classified. In my opinion, the history

of the origins, the system of regulations and the wording

of the provision speak in favor of a mere compatibility

test, so that I can state as a result that at least for the

public sector that adheres to the reservation

of the law, the compatibility alone does not allow further

processing that changes the purpose.

In my opinion, a purpose-changing processing, in

particular data transmission, in the public sector can only

be, in my opinion, only rarely permitted

ge consent or on a legal provision according to Art. 6

Para. 1 Letter c or e GDPR. as sole

Sections 3 and 4 of Saxony come with the legal provisions

Data Protection Implementation Act (SächsDSDG) into consideration.

In my opinion, Art. 6 Para. 4 GDPR – apart from cases of

consent and legally permitted further processing for other

purposes (cf. § 4 SächsDSDG) – plays a role for public

bodies in the following cases, for example:

• Use of personal data for purposes other than the

purpose for which it was collected in one’s own

area of responsibility (example: state judiciary cash

register: account data is collected when the debtor

of the court costs is paid for bookkeeping and any

payment reversal and in another, later enforcement

procedure against the debtor – both tasks of the

state justice fund – continues to be used; the purpose
of collection is different from the later purpose of
use. But both are administrative interventions and the
basis for authorization is the same.) • Transmission
to other authorities for the purpose of fulfilling their own
tasks (data is, for example, sent with a request for
notification whether the recipient has information that
the responsible requesting authority needs to fulfill
the task. Another case is enforcement assistance.)

As a result, I consider transmission by public bodies to other bodies
based on “compatibility of purpose” for the purpose of enabling the
recipient to perform their tasks with the transmitted data to be
inadmissible or inadmissible
for not compatible with the criteria of Art. 6 Para. 4 DSGVO.
Furthermore, further processing, in particular transmission, is of course
permitted on the basis and within the framework of special statutory
further processing regulations, in particular special transmission
regulations. The requirements of existing special transmission regulations
must therefore continue to be observed within the city administration.
According to Recital 50 Sentence 4 GDPR, no special authorization
should expressly be granted for “further processing for archiving
purposes in the public interest, for scientific or historical research
purposes or for sta

tistical purposes”.

Finally, I informed the requesting official data protection officer that the

principle of

friendliness - especially for public authorities - white

Furthermore, as follows from Art. 6 Para. 1 Letter b to f GDPR applies

(where Letter f does not apply to the processing carried out by authorities

in the fulfillment of their tasks). The principle of prohibition subject to

What should I

do? Public bodies must

permission also continues to apply in the public sector for every phase

check the admissibility of this

of processing, including transmission, i.e. a permission standard based

transmission every time it is

on Art. 6 (1) GDPR is still required. The same also applies to the principle

transmitted to another body,

even if the other body part

of informational separation of powers.

same city administration.

See also 2.2.9.

1.3 Creation of the dynamic

teaching aid database Saxony

The State Office for Schools and Education approached my authority in

the spring with the request that when creating a dyna

mix teaching aids database to advise. goal of the project

is to provide digital offers for all teachers in

Evaluate Saxony according to pedagogical aspects

and to demonstrate possible uses in the classroom. Of course, data protection also plays an important role.

Because with a large number of certainly interesting offers that are in principle well suited for school purposes, there was a problem, after a rough review of the products and websites available, especially there. My office

ganger gratefully accepted the offer to participate. I also think it makes sense to provide support for educators from a central location, instead of giving each individual teacher the task of checking their professional suitability and legal admissibility

ability to burden.

With the limited human resources of my agency

it is clear that my employees do not

can check every single offer of such a database. In several workshops, criteria were therefore developed with which the employees of the media education departments of the State Office for Schools and Education can carry out at least a cursory examination of possible offers without

becoming experts for themselves

having to become data protection.

No data transfers to non-European countries

Such an assessment is not easy, especially given the possible use in schools. The administrative regulation (VwV) for school data protection clearly formulates the requirements: "Only cloud computing services to

which EU law applies are permitted." This means that data transfers to non-European countries must be avoided. This not only affects the location of the actual provider of the app or website, but also the services integrated into the offer. And that's where the problem often lies, that many offers for analysis purposes and for reasons of simplification fall back on offers from mostly US companies and then usage data ends up there as well. Such offers are clearly unsuitable for school purposes and simply illegal.

Consents and Tracking

Another problem concerns consent to data processing. Even if it is now common practice to consent to all sorts of things when surfing the web privately or installing an app, special rules apply to such consent in the school context. If a learning material is made available (or in the case of teachers, a teaching material used for official purposes), consent is generally not possible. On the one hand, there is no voluntariness, on the other hand, many schoolchildren are not able to give their consent at all because they are not of the required age and their parents would therefore be asked. Websites and apps that require consent (“We need your consent” or similar) are therefore not suitable for school use.

Also when it comes to tracking or advertising, which the Ver

keep track of users on the Internet

follows, strict rules apply. Such observation of behavior is generally not compatible with the educational mandate or employee data protection.

Inspection tools for apps and websites

How can pedagogically trained employees create an app or a website in the foreseeable future on data protection review legal issues? In the first step, the data protection declaration is examined for any problems (permissions, transmission to third countries, comprehensibility and transparency). Unfortunately, this is not enough. In practice, it was often found that data processing that appears in the data protection declaration does not take place at all or, far worse, data processing took place that was not mentioned in the data protection declaration. All in all, unfortunately, it must be said that in many cases the data protection declaration does not cast the best light on the provider. A technical analysis must also be carried out.

DSK application help : ÿ sdb.de/

tb2105

This can easily be done with publicly available testing tools such as Privacy Score (privacyscore.org) or Webkoll

What should I do?

(webbkoll.dataskydd.net) or for apps Exodus Privacy (exodus-

When using digital teaching

and learning materials,

educational institutions must

privacy.eu.org) . With these instruments, the employees can make a

ensure that, in addition to the

requirements of the GDPR,

area-specific requirements

and that all data processing

is strictly aligned with the

educational mandate.

Minder's data protection

requirements

year-olds as well as teachers

is in a special way

decision and this

document.

Overall, the effort was worth it. The employees have internalized the

background to the decision-making process, and in cases of doubt, a

short shift has also been found

established away to look after sensitive cases at my authority

to seek advice. Cooperation with the State Office for

School and education can therefore be seen as a successful way to use

synergy effects for larger projects and to quickly achieve practice-oriented

to be fair.

results.

Chapter 1

Machine Translated by Google

2 Principles of data processing

2.1 Data Processing Principles,

Definitions

2.1.1 Logbook edition for a

company - data minimization

ÿ Section 31a paragraph 1 sentence 1 StVZO, Article 5 paragraph 1 letter c GDPR

In a consultation request of a larger craft

Operation is my office with the data protection law

1 sentence 1 of the Road Traffic Licensing Ordinance (StVZO).

A regulatory offenses authority had charged the company with (temporarily)

keeping a logbook and stipulated that every driver had to enter their home

address in addition to their name.

This in turn had the manager of the company as

disproportionate processing, because this would result in a collection of

addresses that a large number of employees would be able to see. He

turned

therefore seeking advice to my office.

Ultimately, my authority was able to convince the fine office that it is

sufficient as a (capable of summoning) address if the company address is

entered, possibly supplemented by the department, a personnel number

or the same, in order to rule out assignment errors. The corresponding is

sufficient for the official fulfillment of tasks.

And on the part of the authority it is also understandable that the

Responsible - the company - in relation to a

Activity Report 2021

| 47

Machine Translated by Google

has to restrict data processing, Art. 5 para. 1 letter c

GDPR.

In order to do justice to adequate and complete bookkeeping, the

companies affected have to

but also to include that any journeys made by third parties - for example

test drives in a repair shop - are to be entered.

practice note

In the logbook, which is usually limited in terms of space, it is not

necessary to enter the typical company address in full for every trip. A

simple internal reference ("according to page ...") is sufficient for the

correct filling in of the address field. The company stamp could be

entered on this page. With his signature, the driver making the entry in

the book also legitimizes the employer and those responsible in a second

step to disclose his home address to the police, administrative offenses

authorities, tax authorities and the public prosecutor's office, if sufficient

What should I do?

Ver

are in a company

to avoid reciprocal disclosures of

employee data that are not required.

To the

moments of thought give reason to do so. Understandably, administrative

information to be protected

the private ones also count in this respect

authorities have to ensure that simplifications do not turn into loopholes.

addresses of employees.

But there should also be no unnecessary disclosure of data and too

Also have public bodies

much data processing. In this respect, the sentence attributed to Albert

general data protection

Einstein applies that something can be made as simple as possible – but

requirements to which companies

are subject must be taken into

not simpler either!

account.

2.1.2 Artificial Intelligence in School:

Area9 Rhapsode

ÿ Art. 4 No. 1, 6 GDPR

In February 2021, the Saxon State Ministry provided information

to my authority for Kultus (SMK) that it intends to test the use of the

"Intelligent Tutorial System Area9 Rhapsode" at Saxon schools. The

special thing about this learning platform: It not only imparts content and

queries knowledge, but also recognizes the different

student status. Accordingly, it should help them on individual

learning paths until they have really understood a topic. In addition

to content-related answers, the users provide information about
their self-confidence from "I have that
understood" to "I'm not sure about that" to "I don't have any
Idea". If someone gives the wrong answer but ticks that they are
sure, the system recognizes an unconscious incompetence – and
vice versa. The system can be fed with content for all subjects,
school types and age groups. You can also create these yourself
but probably mainly - if they "play along" - come from the school
book publishers and are entered into the system. It is obvious that
this can be a promising way to independently expand knowledge,
especially in times of homeschooling.

For my authority, the decisive factors were initially those who were there
resulting data flows. The manufacturer to whom the SMK
referred to, assumed that no other personal data of the user would
be processed apart from user name, e-mail and password. All
other data collected is "learning data" from the user's interactions
with the system or non-personally identifiable 'technical information'
where data would only be collected and processed to recognize
and register the devices used to access Rhapsode.

My authority informed the manufacturer and the SMK that
that all of the aforementioned data can be assigned to a student
and should therefore be personal data in accordance with Art. 4
No. 1, 6 DSGVO. Their processing therefore requires a legal basis
- also for test purposes. This is also to ensure that data from
Saxon students is not outside
of the school context can be used, for example, to improve the

product. My authority expressly questioned the use of "AWS services", i.e. Amazon's cloud offer, since it cannot be fully guaranteed that all data will remain in Germany. The Questions from my authority remained unanswered.

Instead, a press release from the SMK dated July 8, 2021 stated that the test of the "Intelligent Tutorial System (ITS) Area9 Rhapsode" had started.

When I asked, my agency found out that Amazon's cloud service was being used for this. Despite this serious data protection violation, an instruction according to Art. 58 Para. 2 Letter f) GDPR - to stop the test operation immediately - was refrained from in view of the imminent end of the school year. The Minister of State informed my authority in a letter that the

The concerns expressed due to a lack of coordination between the various participants in the SMK had not been taken into account, and assured that for the future use of the "Area9 Rhapsode" system, data protection law Matters checked and granted in close cooperation with me be provided. This is also my impression from the discussions that took place with the SMK.

2.2 Legality requirements for data

processing

2.2.1 Art. 6 Para. 1 Letter e GDPR

in connection with a jurisdiction

regulation no legal basis for public

bodies

Occasionally, even in the fourth year of direct application

of the General Data Protection Regulation (GDPR), when

I ask an authority or other public body about the legal

basis for the processing of personal data carried out there,

I receive the answer that the processing is based on Art. 6

Para. 1 Letter e GDPR in connection with the relevant

statutory jurisdiction for the requested body.

This view is at least with regard to public position

Len of the Free State of Saxony inapplicable.

Machine Translated by Google

Because knowledge of the applicable legal basis for the

Lawfulness of official processing of personal data is essential and the

information to be given

affected persons according to Art. 13 Para. 1 Letter c GDPR

are mandatory, inaccuracies on this issue are acceptable.

Art. 6 Para. 1 Letter e GDPR does not form a legal basis for the processing

of personal data, even in connection with a statutory assignment of tasks

public bodies. Rather, a legal action is required

schrift within the meaning of Art. 6 Para. 3 Sentence 1 GDPR, which

explicitly allows the processing of personal data. It goes without saying
that this processing must be necessary for the public body to fulfill its
tasks (Article 6 (3) sentence 2 GDPR, cf. also recital 45 sentences 1 and
3 of the GDPR). Member State processing regulations as the legal basis
for encroachments on the fundamental right to informational selfdetermination in accordance with Art. 6 Para. 1 Letter e GDPR
must meet
the constitutional requirements for intervention norms for state bodies
(recital 41 of the GDPR). Even in connection with Art. 6 Para. 1 Letter e
GDPR, pure task assignments fail to meet the requirements of the
European Court of Justice (ECJ) and the European Court of Human
Rights (ECtHR) for the specificity and “foreseeability” of a norm affecting
fundamental rights, which according to the The will of the EU legislator
must be taken into account for "legal bases" within the meaning of the
GDPR (recital 41 of the GDPR). National constitutional law, which leads
to the same finding here, remains within the framework of Art. 6 para. 1
Letters c and e GDPR - with regard to these provisions, the GDPR, as
well as on individual other points,
Directive character and leaves the member states room for maneuver in conjunction with Art. 6 Para. 2 and 3 GDPR
unaffected according to
the will of the legislator (recital 41 of the GDPR), so that the requirements
formulated by the Federal Constitutional Court for the specificity of
overriding norms must also be met . That is

This is the case with explicit processing powers, but not

with pure task assignment norms.

Regarding the processing of personal data

by Saxon public authorities within the meaning of Section 2 Paragraph 1

In the Saxon Data Protection Implementation Act

(SächsDSDG), the legislator determined in § 3 para. 1

SächsDSDG that - unless the processing can be based

on overriding regulations in special specialist law processing is permissible if it is used to fulfill the

responsibility of the person responsible related task or in

the exercise of official authority that has been transferred

to the person responsible. If no area-specific data

processing regulation applies, § 3 SächsDSDG acts as a

sort of catch-all standard for data processing by public

bodies in the Free State.

The "recourse" of a public body in the Free State to

determine the relevant legal basis for its processing of

personal data is Art. 6 Para of the relevant national

legislation(s) or out of unwillingness to apply them –

What should I

neither permitted (see above) nor necessary. Saxon

do? Public Saxon authorities

public authorities are not entitled to disregard applicable

must know the legal basis for their

law and effective legal provisions addressed to them

processing of personal data, identify

and data subjects

inform about this. A return

access to Art. 6 Para. 1 Letter e

GDPR in connection with a legal

assignment of responsibility is

not to apply. Of course, there is no case of a possible

primacy of application of EU law.

excluded.

2.2.2 E-mail notice in the staff room

ÿ Art. 6 GDPR

A practice counselor who conducts careers guidance at

high schools informed my agency that she

private e-mail account had sent a message to the

headmistress's private e-mail address. In the message

she cited her child's illness as one of the reasons for her

absences. The Practice Advisor

later found out that this e-mail was posted in the staff room and therefore

both her private e-mail address and its content were visible to the entire

teaching staff.

The headmistress asked for a statement by my authority stated that the

petitioner's absences could be explained

had led to financial distress towards students and parents. That is why

she contacted the provider of the practice advice, which announced an email from the petitioner. Irrespective of the private

e-mail address used,

the school could therefore assume that this was an official connection.

However, it was not necessary for this e-mail to be posted in full in the

staff room. My authority therefore informed the headmistress that

information about “personal reasons” or blacking out the respective

passages would have been sufficient. Alternatively, the petitioner could

have been asked for a corresponding consent.

2.2.3 Data transmission of

a mobile phone number by the

retailer to a shipping service provider

ÿ § 242 BGB, Article 6 Paragraph 1 Letter b GDPR, Article 13 Paragraph 1 Letter e

GDPR, Article 14 GDPR

A customer of an online retailer complained that it was

ne mobile phone number intended only for the dealer

transmits this to the shipping service provider and this

him before the goods ordered arrive at the customer's

sent via SMS. Complaints of this kind, as far as data transfer is concerned,

my authority has not sel

to record.

The situation was complicated by the fact that the customer was able to

enjoy express delivery at no extra cost due to a seasonal bonus campaign

and regional availability. The customer may have either overlooked the

field (“Express”) that was already pre-assigned when ordering or

misjudged its mode of operation.

In this case, Article 6 (1) (b) of the General Data Protection

Regulation (GDPR) came into consideration as the legal basis for the transmission of the phone number to the mailing service provider due to the proper fulfillment of the contract. In the case at hand, consent was not required. The shipment had been part of the contract, and the customer had chosen free express delivery. It is also part of the obligation of the e-commerce customer to find out about the delivery conditions before concluding the contract, which in the present case, according to my findings, was easily possible and changeable by looking at the selection area on the website. The order page was ver understandable and in no way misleading.

When ordering the "express" shipping method, I am convinced that the customer should be informed in a way that he is able to take note of immediately, which is desirable on the part of the customer and necessary on the part of the company. In this respect, it also corresponds to Section 242 of the German Civil Code (BGB). Other forms of communication, such as e-mail notifications, would in too many cases, based on general experience, not result in the recipient being aware of the express delivery method owed in good time. In view of the interests involved, I assumed that it was permissible to transmit the telephone number to be entered by the customer in the ordering process to the postal service provider.

However, the company was responsible for the fact that

the transmission of the telephone number to the “Express”
shipping method was not explicitly mentioned in its data
protection information as a legal defect, Art. 13 Para. 1
Letter e GDPR. This was followed by the question of
whether this might affect the admissibility of the data
transmission. As a result, I again denied this. The following
considerations were decisive for me:

According to recital 47 of the General Data Protection Regulation,
even an assumed legitimate interest must be measured by whether
a data subject can reasonably expect processing in the given
situation.
This is especially true in contractual relationships.
A requirement that was not sufficiently clearly communicated in advance
approach would be generally suitable for influencing expectations
towards the exclusion of processing; however, this does not apply
across the board, but must be considered on a case-by-case basis.
Ultimately, this is also supported by the fact that Art. 13 GDPR itself
makes no statement about the possible legal consequences of the
violation of the information obligation.
No special circumstances could be inferred from the individual case
to be examined. This leaves the check of the typical expectations
(particularly for the product group) on the part of the customer. Here
I came to the conclusion that successful delivery using all available

communication channels can and must be regarded as common

practice, at least in the case of express shipments. The passing on

of contact data that goes beyond the name and address to the

postal service provider is ultimately also subjectively to be expected

by the customer in the case of express deliveries. From the lack in

data protection

information could for the facts described

no exclusion of data transfer can be derived.

What should I do?

However, my authority pointed out to the company that the data

Especially in the area of trade

especially with e-com

protection information was misleading in relation to the specific

merce, those responsible should

circumstances and suggested a clarifying wording. The corresponding

comply with the information

data protection declaration was then adapted.

obligations, if only out of their own interest

Art. 13 and 14 GDPR complete

fulfill dig. If necessary, expert advice

It would be unrealistic, comprehensive, complete and completely

should be obtained.

correct data protection information in accordance with Articles 13 and 14

Disputed transfers of data within

GDPR of data processing companies and others

the framework of contractual

relationships are also under Ein

jobs to be expected. As far as the General Data Protection

relationship of the general clause

Regulation and the interpretation of the standards are concerned,

of § 242 BGB, according to trust and

the development of the law is far from complete; Not to mention a

Believe with respect to the

Traffic custom with regard to

coherent Europe-wide application of the provisions. To the extent

assess their admissibility.

that those responsible for the shutdown of Infor

If I work cooperatively with the lack of information, I also recognize my

work as fruitful. But I also advocate

that responsible persons contact each other when necessary and in cases of doubt

Contact a knowledgeable data protection advisor at an early stage.

Structural recurrences and attempts to cover up misconduct weigh

more heavily than uncertainties and mistakes. The same applies if

necessary

sanction.

2.2.4 Video surveillance to

analyze the driving behavior of e-scooters

ÿ Section 15 (4) eKFV; Article 6 paragraph 1 letter f GDPR; Art. 9 para. 1, 2 GDPR; § 27 paragraph 1 BDSG;

Art. 25 and 32 GDPR

Since the release of the small electric vehicles (eKF) - better known as e-scooters - on public roads is the The number of accidents involving these vehicles has risen sharply. Scientific monitoring of the participation of eKF in road traffic was already suggested when it was approved (§ 15 Para. 4 Small Electric Vehicles Ordinance - eKFV), which was carried out by the Federal Highway Research Institute (BASt) with the research project "Scientific Monitoring of the Participation of Small Electric Vehicles in Road Traffic". was brought to the way. The BASt has commissioned the traffic accident research at the TU Dresden GmbH (VUFO) together with various partners to carry out the research project in order to ultimately shape the discussion about the vehicles on an objective basis with correct argumentation in the future.

Research goal and concept

Against this background, the VUFO approached my office with a data protection concept that encompassed the data protection aspects of the research project. An essential part of the research was the analysis of the driving behavior of e-scooters, which the VUFO wanted to investigate more closely by means of video observation in real traffic situations (limited route section). As places

for traffic observation, streets were both in Both Dresden and Berlin are planned, with the choice of location being based on the frequency of eKF transits, infrastructural aspects and a

possible high number

conflict oriented.

For this purpose, a camera box should be installed at a height of 4 meters (Mobile observation box) with a recording device in which the video sequences are stored in encrypted form to protect against unauthorized access.

The evaluation of the video material should take place at a specialized company in Vienna, since automated processing on site was not possible for reasons of space and security. The access

on the video recordings and the selection for the for

Research projects for relevant sequences should only take place automatically and the remaining video material – after evaluation and pseudonymization – should be deleted immediately afterwards. Already by reducing the image quality, the identification of natural persons complicated and also by a weekly location

longer, continuous recording times are avoided

become.

Both the users of eKF and those involved in the conflict, as well as uninvolved persons who happened to be present and observed, were potentially affected by the video surveillance. The data was processed on the basis of algorithms that automatically recognize eKF in road traffic based on their special appearance and use this to create a driving line (trajectory). There was neither a "recognition" of users nor a manual review

of the video material provided. The aim of the video observation was to use the chronological order of the image sequences to understand and

present driving movements and speeds in order to gain insights into the speeds driven, the distances maintained and the traffic areas used. In addition, an accident-analytical assessment of any conflict or accident situations that may have arisen should be carried out. Even if in contrast

to avoid influencing traffic behavior as far as possible during a laboratory test, the data protection concept – by necessity – provided for appropriate signage.

processing of health data

was essential for the success of the research project

in particular, knowledge of the nature and severity of Ver

injuries in an accident involving small electric vehicles. Indirect conclusions about the state of health of the persons involved in the accident could thus be drawn from the observed (accident) events pull. Ultimately, this is health data

(special categories of personal data, Art. 4 No.

15 GDPR) for which there is a legal ban on processing (Article 9 (1) GDPR). With the Federal Data Protection Act (BDSG), the national legislature has of the in Art.

9 Para. 1 Letter j GDPR used and specified there in § 27 for the purposes of science and research under which conditions the basic processing ban of Art.

9 Para. 1 GDPR does not apply in exceptional cases. According to

§ 27 paragraph 1 BDSG, the prerequisite for this is that

• the processing of special categories of personal data is necessary

for the stated purposes and

• exacerbated to the general weighing of interests of

Art. 6 Para. 1 Letter f GDPR the interests of the Ver

responsible with the processing to the privileged

Purposes the interests of the data subject significantly

predominate.

Art. 9 GDPR and Section 27 BDSG alone do not form an independent

legal basis for the processing of personal data. Because the assessment

of the legal admissibility for the processing of health data can only be

made together with a provision of Art. 6 Para. 1 DSGVO. The

admissibility of traffic monitoring under data protection law and the

associated processing of personal

I saw the legitimate interests of Art. 6 Para. 1 Letter f GDPR in conjunction

with Art. 9 Para. 2 Letter j GDPR (in conjunction with Section 27 Para. 1

BDSG) as justified.

My authority was able to agree with the risk assessment carried out by

the VUFO and came to the conclusion that the numerous precautions

and measures taken by the VUFO ultimately involved only minimal legal

interference. In any case, there was no indication that the interest of the

road users operating in the observation area outweighed the research

interest.

Data protection compliant implementation

The subject of the consultation was the examination of the data
protection legal focal points of the research concept. In this respect, my
authority has communicated its comments to the VUFO on the presented
concept, which have been implemented accordingly. In the bilateral
exchange, the data protection law implied by the research project
common principles discussed and concurring feast
decisions on this and reached an agreement on fundamental positions.
It was important to inform the public in advance. As well as
in the press as well as on the websites of VUFO and mei
Information about this was published by an authority. The VUFO has
on the affected road sections before entering the
What should I do?
video-monitored area also protects data
Depending on the purpose,
video surveillance in generally
specifications corresponding complete information sheet attached. In
accessible areas is permitted
addition, I have instructed VUFO to ensure that technical and
minimize, pseudonymize and
organizational measures are taken in accordance with Articles 25 and
promptly anonymize. These are in
practice
32 GDPR.
only in exceptional cases
It is not possible to say exactly whether it was ultimately due to the large-
comprehensive consideration of interests

scale public relations work or the professional implementation on the part

justifiable. Automated methods, on

the other hand, allow the instantaneous

of the VUFO, but my authority did not receive a single request or

conversion of the recorded video

submission for traffic monitoring. As a result, the data obtained with the

recording

participation of the Dresden road users made an important contribution

data in information that can no longer

as a basis for an evaluation of the e-scooter driving behavior based on

be assigned to individual individuals is

to be given preference.

this, the future participation of the

Making e-scooters safer on the road. One may

be curious how and in what form the won He

Knowledge of the by the Federal Ministry of Transport

and digital infrastructure for amending the eKFV.

2.2.5 Limits of Video Surveillance

of Private Property

ÿ Article 2(2)(c) GDPR, Article 6(1)(f) GDPR

Private camera operators often think they are in line with

data protection law when they turn off their video cameras

eventually align to their own private lots. In most cases I

am against this as well

no objection. Because data protection law applies to

Video surveillance does not apply if it is carried out by a

natural person to carry out exclusively personal or family

activities and thus has no connection to a professional or

economic activity, see the so-called household exception

in Article 2 Paragraph 2 Letter c data protection General

Regulation (GDPR). However, this does not justify video

surveillance if a business with customer traffic is (also)

set up on the private property or if there is an apartment

building. The recourse to the household exception also

does not apply to private property areas in which other

people enter

have a right of ownership, right of use or right of residence.

Occasionally, residents of a back-lying property turn to

me. Because if you buy a property that does not have its

own road access, you can only do so via the neighboring

property. Experience has shown that this is often the

starting point for a neighborhood dispute, for example

about who should

Wear and tear or damage will be charged for the cost of

repairing the trail. This was the case in a case that became

known to my authority. The background was alleged damage

to the path, which the person lying behind is said to have caused.

The neighbor brought a video to document it

camera an.

Due to the non-applicability of the budget exception mentioned,

admissibility could at best result from legitimate interests, Article 6 (1)

(f) GDPR.

However, it is not possible to use this to legitimize the video surveillance

of the access area secured by land register law, even if this is on the

camera operator's own property. Of course, if the requirements of Art. 2

Para. 2 Letter c GDPR are met, the property owner may permissibly

monitor all other areas not covered by the right of way. However, this

no longer applies to the path area covered by the land register entry there the legitimate interests of the users of the right of way (locators

behind, visitors, craftsmen, postal service providers, etc.) not to be

monitored by the owner via video during the unavoidable passage of

this path prevail there .

I get the same result when the property owner monitors his private road.

This is what happened in another case brought to my attention, in which

the private road was owned by several residents.

Although the owners of the private road agreed on video surveillance

there, this did not change my legal assessment. In this case, too, the

circle of those affected is much broader, especially since the circle of

Local residents expanded and these no stake in the private

have a street, but have to use this access road to reach their property.

Ultimately, for purely practical reasons, video surveillance can hardly be

based on the consent solution in any conceivable case, since this would

require the informed and voluntary consent of all persons affected, Art. 6 Paragraph 1 letter a GDPR.

In another case, a citizen contacted my agency because he spotted a video camera on a public footpath. As it turned out during my investigations, this was on private property, but it was

Path dedicated several decades ago as a limited public path by the municipality. In this respect, the property owner is restricted in the use of his private property and may not permanently monitor the hikers and walkers using the path.

As far as wildlife cameras in private forest areas are concerned, I also get input and inquiries about this from time to time. My predecessor in office dealt with this in the 7th activity report (No. 8.1.2), but at that time under the old Federal Data Protection Act and thus the legal situation before the application of the General Data Protection Regulation. However, even under the current legal situation, nothing has changed in the data protection assessment at that time. Section 6b, paragraph 1, number 3 of the Federal Data

What should I do?

property owners and

Camera operators should before In

Protection Act has been replaced by the provision of Article 6, paragraph 1, letter f of the GDPR, which in the same way

operation of video technology

requires a decision to weigh up the existence of legitimate

first check whether third

interests, which in the case of private forest areas is generally

parties could be affected

in favor the forest users (hikers, mushroom pickers, etc.) are absent.

by the detection range of

the intended video cameras. Is

As a result, the reasoning of the Federal Court of Justice of

this is the case and it is

April 25, 1995, Az. VI ZR 272/9, for the illegality of private

an area accessible to

third parties should be

video surveillance in public traffic can be applied to the cases

Measure to be refrained from,

as far as effective

Consent from all those

affected – as in these cases

regularly – will not be

catchable.

presented. Even in the case of publicly accessible privately

owned property areas, the interests of those affected that are

worthy of protection generally outweigh the surveillance

interests of the camera operator.

2.2.6 Curious and strange things

about videography

ÿ Art. 6 Para. 1 Letter f GDPR

Time and time again, during my investigations, I experience

how little thought some camera operators give to the limits of

video surveillance and that they violate the informational selfdetermination rights of the people being observed if they

have innocent fellow human beings under constant

surveillance. It amazes me all the more which ones

Arguments that those responsible sometimes use to justify the use of

cameras; Justifications that are also obviously not suitable as a

justification for processing based on a legitimate interest pursuant to

Article 6 (1) (f) of the General Data Protection Regulation (GDPR).

Alternative to the TV program

In one case, for example, the municipal security service in a Saxon city

contacted my authority because it

Window sills on the third floor of a residential building meh

rere video cameras. The camera operator let the

municipal officials unabashedly look at the video surveillance and

willingly provided them with information on this. He had positioned the

cameras to face the sloping street in front of the apartment building,

but because of the camera angles he could also see several apartment

buildings opposite.

The municipal employees were probably amazed

when the camera operator justified the cameras he installed with

entertainment purposes, especially in winter when fresh snow had fallen

and motor vehicles had problems on the road slope. Although no video recording took place due to the outdated technology used, the apartment owner transmitted the live images from the cameras to his analog TV set in order to add an (additional) add live channel. It can only be assumed that he was probably not completely satisfied with the range of programs offered by conventional TV stations.

control of public infrastructure

In another case, a citizen police officer described to me the difficulties she was having with a private property owner. After she had the suspicion that he was also observing the public traffic area beyond the property fence with the camera on the house pointing in the direction of the entrance gate, she spoke to the camera operator. He frankly admitted that

he actively operates the camera and cited the reasons for the Video surveillance indicates that cyclists and municipal building yard workers are constantly being used during clearing and gritting work, but also postal and newspaper deliverers would drive their vehicles on the sidewalk in front of the residential property. He already has a team of horses on it see driving. In addition, the lawn would be in front of the reason piece not maintained regularly. That's why he meant this would have to be checked and obviously saw itself

appointed for this. In the course of further investigations, it became known that he once even contacted the responsible building yard manager because of what he considered to be the poor quality of the winter service and presented video recordings from his camera as evidence of this.

In the first case, I was able to persuade the camera operator to completely dismantle the video cameras. In the other case, the homeowner showed me that he had the camera alignment changed it at my request in such a way that only his private entrance to the property was still included.

Due to the seriousness of the legal violations, I could not avoid issuing a warning to the camera operators in both cases.

2.2.7 Provision of billing documents within a homeowners association

ÿ § 18 Para. 4 WEMoG, Art. 4 No. 1 and 2 GDPR, Art. 6 Para. 1 and 3 GDPR, Art. 32 GDPR

Due to the contact restrictions associated with the fight against the corona pandemic, the shift of services to the Internet has received an impetus.

Last but not least, this poses new challenges for those responsible, who have to take increased measures, especially in the digital processing of personal data, in order to do justice to data protection. Because he has exercised his right to informational self-determination through the

faithful housing management saw hurt, an apartment owner turned to my authority with a petition.

The property management had sent all co-owners an e-mail with which they could read about the annual statement for

the year 2020 were informed. The email contained next to

A link to an internet portal also directly accessible PDF documents, each of which was labeled with a consecutive number and the respective owner's name. After registering on an internet portal, each of the more than 60 owners could access them and granted access to all billing documents (individual bills plus heating and water bills) of all apartment owners of the residential property in question.

The housing administration justified this approach with the fact that the exact design of each owner

entitled right to inspect the administrator and thus

the billing documents are also her sole responsibility. She was of the opinion that the personal data of the owners and tenants contained in the individual invoices were not subject to the General Data Protection Regulation.

After explaining the facts with reference to the increase

The current provision of documents by owner associations in digital form was of fundamental importance for a large number of management companies, my authority presented the issue to the responsible working group of the data protection supervisory authorities in order to achieve a coordinated legal opinion there.

legal basis sought

But first to the question of the applicability of data protection law within

a homeowners' association, specifically with regard to the disclosure of billing documents. In addition to owner and Tenant names also individual consumption values and thus Undoubtedly personal data within the meaning of Art. 4 No. 1 General Data Protection Regulation (GDPR). The processing - here in the form of disclosure (Art. 4 No. 2 DSGVO) - is to be assessed according to the data protection regulations.

The property manager obviously failed to notice that the federal legislature also expressly made it clear in the explanatory memorandum that with the statutory right of inspection in Section 18 (4) of the Housing Ownership Act (WEG), which will apply from December 1, 2020, “of course, mandatory data protection requirements must be observed”. (Bundestag printed paper 19/18791 on Section 18 (4) of the Home Ownership Modernization Act – WEMoG). Accordingly, a legal basis pursuant to Art. 6 (1) GDPR would have been required for a permissible data disclosure. In the absence of a legal obligation to pass on data, processing based on Article 6 (1) (c) GDPR was ruled out. According to this, the processing of personal data is only lawful if it is necessary to fulfill a legal obligation to which the person responsible is subject. The processing purpose must be expressly defined as such in the legal basis, Art. 6

Para. 3 Sentence 2 GDPR.

However, the provision of Section 18 Paragraph 4 WEG (formerly derived from Section 24 Paragraph 6 Sentence 3 and Paragraph 7 Sentence 8 WEG in conjunction with Sections 675, 666 of the Civil Code in conjunction with the management contract) contains only one individual claim

“The public has an
insatiable curiosity to
know everything but not
the worth knowing.”
Oscar Wilde

apartment owner to inspect the administrative documents and thus also the records and billing documents as well as the individual bills of the other apartment owners. The right of inspection is intended to enable the apartment owner to check the administrative activities and, in connection with the annual accounts, to check the correctness of the accounts relating to him. All that is required for this is an application without the authorization of the other apartment owners, without a prior resolution in this regard being passed by the owners’ meeting and without the presentation of a (legal) interest (see Bundestag printed paper 19/18791 on Section 18 (4) WEMoG). This is offset by the obligation of the property manager, with the exception of the abusive or vexatious exercise of rights, to grant access to the manager's documents.

Chapter 2

Machine Translated by Google

A requirement for the disclosure of the administrative
documents is therefore a relevant application by the
owner. Authorization for the complete and applicationindependent disclosure of accounting documents (here:
annual accounts including individual accounts as well as
documents for utility bills, esp.
Heating and hot water bills) as part of the administrative
documents for all owners - in anticipation of individually
asserted rights of inspection - cannot be derived from this,
however.

Legitimate interest no reason

The property manager could not invoke legitimate
interests either, cf. Article 6 (1) (f) GDPR.
According to this, the processing is only lawful if it is
necessary to protect the legitimate interests of the person
responsible or a third party, unless the interests
sen or fundamental rights and freedoms of those affected
persons who require the protection of personal data
prevail. These conditions were also not met in the present
case.
My authority already recognized no legitimate interest
on the part of the house manager. With a benevolent Be
At best, this could consist of a reduced amount of time
and work required to process individual inspection claims.

If one wanted to see a legitimate interest in this, then there was no need for the unsolicited provision of all billing documents from all property owners independently of the application. The pandemic-related (preferably) electronic provision of documents could not change anything here. The legislature gives the administrator the choice of the form in which he makes the billing documents available to an apartment owner who contacts him with a request for inspection, i.e. whether in the conventional way with physical provision on the business premises or in digital form. However, the latter in particular should save time and money

possible, for example by assigning appropriate rights when accessing an Internet portal or in the form of an encrypted transmission of billing documents, these can be sent to specific recipients and without great effort. Also with regard to the additional disclosure of tenant data, even if only the names, I could not see any necessity.

Disclosure not lawful

Ultimately, the consideration to be carried out in the second stage also showed that owners do not have to accept the unsolicited and unfounded disclosure of all

billing-relevant data to other owners. Otherwise, the data protection fundamental right of the affected owners – especially in the internet age – could be undermined across the board and virtually without barriers with reference to reasons for cost savings and advancing technical possibilities. However, the mere fact that many services have shifted to the Internet, not least as a result of the experiences from the corona pandemic, does not imply an (autom Withdrawal of the basic data protection right of the persons concerned Persons.

DSK working group shares opinion The responsible working group of the data protection conference (DSK) confirmed my legal opinion and there was agreement that the unsolicited disclosure of the individual bills within a homeowners' association violates Art. 6 GDPR, unless the prior informed consent of the persons concerned owner exists. When asserting the individual right of inspection, however, all individual bills and billing-relevant consumption values must be disclosed to the applicant in full – with the exception of any tenant data.

Otherwise, from a data protection point of view, there are basically no objections to the outsourcing of billing data to an internet portal, provided

that the security of the processing is ensured by technical and

organizational measures (Article 32 GDPR). This can be made possible

with a staged disclosure of the accounting documents, for example by

restricting access (depending on a request for inspection) depending on

What should I do?

the content and type of the documents stored there. Ultimately, according

The administrator can also

to the intention of the legislature, an expressly formulated request by the

provide billing documents within a

owner is required for inspection ("Every apartment owner can […] request

homeowners association digitally by

inspection of the administrative documents.", see Section 18 (4) WEG).

means of a retrieval. The are available

for inspection

The right to inspect receipts does not imply any obligation or authority

on the part of the property manager to transmit all individual bills to all

apartment owners without being requested to do so. In contrast,

only provide authorized persons with

the documents permitted under data

protection law.

anticipatory disclosure would be an imposed flood of information that not

every homeowner wants.

on the part of the person responsible

According to Art. 32 GDPR, it must be

ensured that the data is kept available

in accordance with information security.

2.2.8 Core area of private life also protected in the visa process

ÿ § 86 AufenthG, Art. 2 Abs. 1 GG in connection with Art. 1 Abs. 1 GG

I was contacted by a petitioner who was a husband ner still living abroad from a Saxon woman Immigration Office was requested by email, im Rah of his wife's visa procedure for further examination ing the proof of contact, the chat history on WhatsApp or the medium the petitioner used with his wife uses to submit, whereby this also applies to correspondence include how sent image files and the common me call log. This e-mail from the Immigration Office was a This was preceded by a formal letter from the authority asking the petitioner to provide all evidence of contact with his wife (e-mails, chat histories, call logs and the like).

inviolability of privacy

My office asked the competent authority for a statement and pointed out that they considered the official request for the transmission of "all contact records" and complete private chat histories to be inadmissible. The request for the submission of complete private chat histories represents a serious official intervention in Article 2 (1) of the Basic Law (GG) in conjunction with Article 1 (1) of the Basic Law and requires a constitutional

legal basis from which the requirements and the scope of the Restrictions are clear and recognizable for the citizen and thus corresponds to the rule of law requirement of norm clarity. However, the Residence Act (AufenthG) does not contain a special basis for authorizing such a far-reaching survey measure. Section 86 sentence 1 AufenthG merely represents a basic act of authorization to collect data, which does not include particularly in-depth collections of sensitive data. In addition, the foreigners authority has to observe the inviolability of the spouses' privacy at all times during the review (Administrative Court of Hesse, March 21, 2000, Az.: 12 TG 2545/99). At least parts of private chats between spouses, including image files that have been sent, will regularly fall within the core area of private life.

The authority announced that an official right to order the submission of certain documents also from view

the foreigners authority does not exist. This is also in the

been recognizable from official letters. Also in

inform the immigration authorities about those affected

personal visits, regularly orally, that the selection decision for the submission of suitable evidence lies with the persons concerned themselves. Insofar as the evidence is intimate or insidious, the person concerned is free not to submit the data. If no suitable evidence is provided, the immigration authorities can only decide on the basis of the files. Around

to avoid misunderstandings in the future - in particular due to the lack of

personal visits by the person concerned

the corona pandemic

– the immigration authorities suggested

drafting a corresponding information sheet for those affected and handing

it out to them. Nevertheless, from the point of view of the foreigners

authority, the verifiable description of the organisational, emotional and

mental Ver

bond between spouses in suspected cases does not work

without touching the core area of privacy and the right to informational

self-determination.

No obligation to disclose highly

personal circumstances

My office then has the immigration office

pointed out that the official letters sent so far did not contain any clear

indication of the extent of sufficient proof of contact or the voluntariness

of the submission. The official letter only stated that the documents were

“required”, stating a deadline for submission. Also the indication that

circumstances not asserted in a timely manner are not taken into account

in the decision-making process by the authorities did not correspond to

the general understanding of voluntary participation.

The notice from the foreigners authority that the

I clearly objected to the fact that the organisational, emotional and

intellectual ties between spouses, which is to be examined under verifiable

circumstances, cannot be carried out in full without touching on the core

area of the private sphere.

The core area of private life is absolutely protected and, according to the established case law of the Federal Constitutional Court, is without exception withdrawn from any state access. Even overriding interests of the general public cannot justify an intervention in this absolutely protected core area of private life (BVerfG, 03/03/2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99). For the development of personality in the core area of private life

design includes the possibility of internal processes such as To express sensations and feelings, as well as reflections, views and experiences of a highly personal nature, without fear that public authorities will do so monitor and evaluate. Also included in the protection Expressions of feelings, expressions of unconscious experience and forms of expression of sexuality (BVerfG, March 3, 2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99). Against this background, the foreigners authority must ensure that in future requests for proof of contact for the examination of living conditions by the foreigners authority that the affected a person avoids the impression of communication including sent pictures are completely open (keyword “chat histories”).

Clear notices to affected individuals

I expressly welcomed the creation of the information sheet

advised by the immigration authorities and suggested that

corresponding information on voluntariness and the protection

What should I do?

of the core area of private life should be included.

The core area of private life

is absolutely protected and

After the content of the immigration authority, the responsible

without exception withdrawn

data protection officer and my authority had been coordinated,

from state access.

the immigration authority has been handing out what I believe

Authorities are not allowed to do this

data from the area

to be a successful information sheet to those affected for a few

raise.

months.

2.2.9 Use of account details for

future proceedings by the State

Justice Fund

ÿ Art. 6 Para. 4 GDPR, Art. 13 Para. 3 GDPR

One petitioner reported that the Landesjustizkasse (LJK) had

issued a seizure and bank transfer order against the bank that

held her account. She wondered how the LJK knew her bank

details.

At the request of my authority, the LJK, a department of the

Higher Regional Court (OLG) Dresden, reported that the bank

details from a previous cost

drawing proceedings against the petitioner was known.
This had arisen from one of those affected using About
payment caused by the instructions. The collection and
processing of the payment data serves to fulfill the tasks of
the LJK as an enforcement authority.
The original, first use of the account data relates to the
specific process for which the data was originally collected
had been or in which the data - here by the of
transfer initiated by the party liable for costs – became
known. The continued use in any other, later procedures
represents a change of purpose, which is permissible under
Article 6 (4) of the General Data Protection Regulation (GDPR).
Permitted repurposing use
I consider this practice of further processing the account
connection data in a different procedure, according to
which my predecessor had considered such processing for
other purposes to be permissible even before the GDPR
came into force and under the old legal situation, to be
permissible under the current provisions of the GDPR. The
purpose-changing further processing is in accordance with
the requirements of Art. 6 Para. 4 GDPR. The regulation
describes the conditions under which processing of personal

data for a purpose other than that for which the data was originally collected is permissible.

Also up for discussion was the question of whether, according to the criteria specified in Art. 6 Para or any other procedure) can be used against this debtor. Recital 50 of the GDPR explains that – in addition to the category of data concerned and the consequences of further processing for the data subject – it must also be checked whether, taking into account the relationship between the data subject and the person responsible (LJK), they can reasonably expect this must or can that the data be used in other ways. It's up to me

Eighth, it is reasonable to expect that account connection data disclosed to the LJK will also be used by the LJK for the purpose of its enforcement task, as long as the data is lawfully stored and available to the LJK.

Less intrusive than new third-party data collection

In the context of the necessary consideration, it must also be taken into account that it is less intrusive in terms of data protection if the LJK uses account details that are known to it again in a future case than if it sends a query to the Federal Central Tax Office regarding the existing bank details of the debtor (cf. Section 802l (1) of the Code of Civil Procedure) and in this context would process more of

the debtor's data and even involve a third party.

However, according to Art. 13 Para. 3 GDPR, the LJK is obliged to

inform the data subject comprehensively about the change in

purpose before further processing

ren. Even before the GDPR came into force, the LJK had to

Coordination with my authority since 2013, together with the request

for payment, using a form, that the transferred transfer data will be

stored and, if necessary, used in further procedures. Unfortunately,

this notice was missing in the current case of the petitioner, so that

she was not informed about the further processing for another

purpose in accordance with Art. 13 (3) GDPR. The Higher Regional

Court announced that the reference to a possible use of the transfer

data was also missing in other procedures for payment requests

that were made in a period of a few months after the

June 2018 sent. With noticing the error

What should I do?

the payment requests were immediately supplemented with the

The state justice fund has

Point out to those liable for costs

reference. With regard to the debtors for whom the information had

that after transfers the account

not been provided in the form, the OLG Dresden requested the LJK

details are stored and, if necessary,

to provide information in accordance with Art. 13 (3) GDPR before

also in further procedures

using the transmitted bank data for other purposes, such as

be used.

enforcement.

Machine Translated by Google

2.2.10 Vaccination

advertising by the Ministry of Social Affairs

One petitioner contacted my authority during the reporting period

de, because he feared that the Saxon State Ministry for Social

Affairs and Social Cohesion (SMS) was misusing personal data

for "vaccination advertising in the Erzgebirge district" and

requested that this be checked. In his complaint, he referred to

an interview with the “Freie Presse” on August 24, 2021. In it,

Minister of State Petra Köpping said that, according to a study

by the Technical University of Dresden, younger AfD voters with

low incomes in particular reject the vaccination. These should

now be specifically addressed.

With regard to “vaccination advertising in the Erzgebirge district”,

the SMS reports that the Office for Strategic Advice Hitschfeld in

Leipzig has been commissioned to develop an information

campaign aimed specifically at the population groups in the

Erzgebirge district that are particularly skeptical about vaccination.

No personal data was made available to the company for this purpose.

The relevant population groups have already been identified in

a microgeographical analysis. The basis was the study "Covid-19

in Saxony" by the Mercator Forum Migration and Democracy

(MIDEM). Based on the order results, SMS had information

flyers delivered via Deutsche Post to entire delivery districts of

specific municipalities in the Erzgebirge district.

A use of personal data did not take place.

More information:

The above study is posted on the MIDEM website.

ÿ www.forum-midem.de

2.2.11 Information from archived population

register data

ÿ SächsArchivG

My authority received an inquiry as to whether the requirements for

information on population register data had changed according to their

Archiving (once the retention period has expired) after

Archive or continue to determine according to reporting rights. While

The latter in accordance with Article 44 of the Federal Registration

Act (BMG) enables so-called simple registration information without

further requirements, in the case of the former until the expiry of

protection periods (which, in accordance with Article 10, Paragraph 1

of the Archives Act for the Free State of Saxony {SächsArchivG}, are

between 10 and 100 years can) no information possible.

This protection period can be shortened with consent or according to

§ 10 Para. 5 SächsArchivG, but the latter is mandatory

legitimate interests that outweigh the legitimate interests of the person

to whom the archive material relates.

Section 11 (5) of the Federal Archives Act contains a regulation according to which protection periods do not apply to federal archive material if it consists of documents that were already open to information access under an Information Access Act before they were handed over to the Federal Archives. On the one hand, the wording “Information Access Act” does not include the Federal Registration Act. On the other hand, the BArchG does not apply to Saxon registration registers, and the SächsArchivG does not contain any

Regulation comparable to Section 11 (5) No. 2 BArchG.

The Saxon State Ministry of the Interior, which was asked for an opinion, informed my authority that the result of the archiving of registration data is actually an additional threshold for information that was not originally provided for under § 44 BMG for records see was.

2.3 Consent questions 2.3.1

Data protection in offender-victim mediation

ÿ Section 155 (2) StPO

At the beginning of last year, a petitioner contacted my authority with a complaint that her statements made as part of a victim-offender mediation (TOA) were sent by the social service of the judiciary to the social-psychiatric service of the local health authority responsible for the petitioner were disclosed, although the petitioner

repeatedly mentioned to the employee responsible that she did not want any contact with the social psychiatric service. Nevertheless, after the interview within the framework of the TOA, the petitioner had received a telephone call from the social psychiatric service of the health department, in which their statements in the context of the TOA were addressed.
My authority asked the social service of the judiciary, which is set up at the regional court (LG) and whose employees are subject to the supervision of the president of the LG, to comment. I pointed out that according to § 155 b paragraph 2 sentence 2 of the Code of Criminal Procedure (StPO), the body commissioned to carry out the TOA - in the case of adult suspects the social service of the judiciary, commissioned by the public prosecutor (StA) - personal data only may process, insofar as this is necessary for the implementation of the TOA or the compensation for damage and the data subject has consented.
The provision is intended to ensure that the
The processing of personal data required by the TOA does not take place without the will of the persons concerned (injured persons as well as suspected perpetrators). The processing of personal data also includes the transmission of this data to third parties. The consent of the person concerned is therefore not only required for data collection, but also for data transmission. In the present case, the petitioner had

expressly opposed the transmission of information concerning her to the health department.

Without the consent of the person concerned, the body commissioned to carry out the TOA – i.e. the social service of the judiciary – may only report to the StA or the court to the required extent in accordance with Section 155 (2) sentence 3 StPO after completion of the activity. The fact that reports are only to be made “to the extent necessary” means that the social service itself only discloses procedurally relevant information to the public prosecutor or the court, but not all of it that suspected perpetrators or injured persons have disclosed within the scope of the TOA.

This strict earmarking of data processing is intended to Promote willingness to TOA because they give those involved the It will make it easier for the decision to disclose itself to the body responsible for its implementation, also with regard to circumstances in which secrecy is fundamentally a concern special interest exists.

In the present case, the social service of the judiciary was not commissioned by the StA to transmit specific information about the petitioner (of which the StA was not even aware) to the social psychiatric service of the health department. Section 13 (2) in conjunction with Section 17 No. 3 of the Introductory Act to the

Courts Constitution Act (EGGVG) could not justify the transmission by the social service either. Only the courts and the StA to. If statements are made within the scope of the TOA which the social service of the judiciary sees as a (concrete) danger to public safety, the social service of the judiciary can inform the police authorities of an acute risk situation.

In the present case there was no legal basis for the transmission of the information from the TOA concerning the petitioner to the social psychiatric service of the health authority; the transmission violated data protection regulations. The president of the regional court responsible here took the opportunity to instruct the employees of the social service of the judiciary at the regional court about the application of data protection regulations for the processing of orders for the TOA, and asked my authority for appropriate expert advice.

Validity of the GDPR for TOA positions

First of all, it had to be clarified whether TOA bodies are subject to the scope of the General Data Protection Regulation (GDPR).

I am of the opinion that TOA bodies operate within the scope of the GDPR. Even if one takes the view that the TOA, with its anchoring in the

Since the Code of Criminal Procedure serves criminal prosecution in the broadest sense and thus falls within the scope of Directive (EU)

2016/680 (JI Directive), the TOA procedure relies from the outset on the voluntary cooperation of those involved and is therefore similar to the GDPR .

Compulsory enforcement of this measure, which the directive issuer sees as a matter of principle when performing tasks within the framework of the JI Directive, is out of the question because the TOA is required to be voluntary by law. In addition, there is the fact that when the order to carry out the TOA is issued, the investigative procedure pursuant to Section 153a Paragraph 1 Sentence 1, Sentence 2 No. 5 StPO is temporarily suspended, i.e. no criminal prosecution takes place during the TOA.

But the TOA office also occupies a certain special position in the scope of the GDPR, since it is neither clearly a processor nor a person responsible for the data

protective sense can be considered.

A prerequisite for order processing within the meaning of Article 4 No. 8 GDPR is that the order processor processes personal data on behalf of and on the instructions of the client. Although the social service of the judiciary is commissioned by the StA or the court to carry out the TOA procedure, the TOA office is not sufficiently bound by instructions. In the case of order processing, the client determines the type of processing. The processor receives a "route", i.e. forward, from the person responsible

gave or just instructions what exactly he has to do. However, the TOA office is not subject to the instructions of the StA or the court with regard to the implementation of its task. With § 155 b paragraph 2

sentence 2 StPO, the legislator assumes that, in addition to those of
the StA and the court
communicated personal data, further personal information is only
collected in the context of the implementation of the TOA by the
responsible body.
In order to be able to do justice to their task and presumed perpetrators
and victims an understanding, one

In order to enable compensation, the TOA office will regularly have
to find out other (living) circumstances of those involved that have
not yet been determined
and court or StA are unknown.
Another feature of order processing is the right of the person
responsible vis-à-vis the order processor to determine the deletion
of the data processed in the order or their return. This is already
opposed to this in the TOA by Section 155 b (4) of the Code of
Criminal Procedure, which only applies to the TOA office, but not
to the StA or the court
contains. In addition, the person concerned can restrict their
consent in accordance with Section 155 b (2) sentence 2 StPO,
so that the reporting obligation of the TOA office (even to the
Public Prosecutor or the court) is limited. The TOA office thus acts
at least partly under its own legal responsibility.
However, the TOA office does not act as its own controller within

the meaning of Art. 4 No. 7 GDPR; she doesn't decide

only about the means and purposes of data processing, but is

commissioned to fulfill a specific task in accordance with the legal

requirements. The TOA is the responsibility of the social service

of the judiciary, which is integrated into the administrative structure

at the respective regional court and is therefore a responsible but

dependent body of the regional court.

TOA office obtains the consent of the person concerned

As a result, the question arose as to who had the consent of the

Obtain data subject according to § 155 b Abs. 2 Satz 2 StPO

has – the body commissioned with the TOA (the TOA body at the

social service of the judiciary), the regional court where the social

service is set up, or the commissioning body (StA or court)?

In fact, consent must be obtained from the TOA body. In

accordance with the administrative regulation for offender-victim

compensation (VwV TOA), the mediation center immediately

contacts the parties involved after being commissioned by the

public prosecutor or the court and clarifies their willingness to carry

out the TOA. This already starts the examination of the suitability of the

Process for a TOA according to § 155 a StPO (the conflicting

will of the injured party precludes suitability) is the responsibility

of the TOA office. There is no legal objection to this, because

the law does not regulate how the suitability test is to be carried

out. However, if the TOA office already discusses the suitability

of the matter for the TOA with the parties involved, it is also

responsible for obtaining the required consent under Section

155 b (2) sentence 2 StPO due to this factual proximity. In

addition, Art. 4 No. 11 GDPR requires that the consent must be

given in an informed manner, i.e. the data subject must be

informed comprehensively and sensibly about the data

processing so that the consent can be formulated in a sufficiently

specific - or correspondingly limited - way. But since neither the

StA nor the court have insight into the implementation of the

TOA, only the TOA office can only

What should I do?

The body responsible for the

TOA acts within the scope of

there an "informed" and thus legally effective one

the GDPR.

consent to be obtained. This is also the only solution that makes

You must obtain the consent

sense with regard to the effect of consent. Because the consent

of those involved in the processing

of your data. Without

of the person concerned determines the scope of the processing

After completion of the activity,

of their data in the TOA and – by way of transmission – beyond

the commissioned TOA office may

the TOA. However, data processed in the TOA is only available

only give the consent of the person

concerned and only if necessary

report to such an extent to the StA

to the TOA office, so that only this office is able to implement

the consent and restrict the processing accordingly.

or the court.

2.3.2 Internet publication of

competition results in youth golf

ÿ Article 5 (2) GDPR, Article 6 (1) GDPR, Article 14 GDPR, Article 17 GDPR

A citizen who is a golf enthusiast had set himself the task of

collecting all the results of competitions and tournaments from

youth golf and presenting them in one website. There he also

created a player portrait for each youth player and assigned an

individual rank to each one. After registering in a protected area,

he offered parents and others interested in golf not only extended

There is also the option of adding a picture of the young golfer to the

player portrait.

Assertion of a right to erasure of personal publications

After a father obviously with the one from the side berei

About the determined ranking value for his two underage sons, he first

tried to delete all data concerning his children with reference to Art. 17

General Data Protection Regulation (GDPR), which the person responsible

with reference to the publicity of the held tournaments and competitions.

As a last resort, the parent with custody turned to my authority and asked me for help in enforcing this site operator.

Consent Requirement

It is true that sporting competitions are generally held in public, so that a tournament host or event organizer is also entitled to present the results on their website. Sports competitions are always carried out on the basis of sport-related competition regulations. In order to take part, the respective athlete must be registered in the license register of the sports association in advance, and by taking part in the competition, the parents also give their consent to the processing of their children's data.

In the present case, however, the site operator was unable to produce the consent of the legal guardians. Rather, he obtained the game data and thus also information about the participating young athletes from both publicly available result lists and from the tournament association tournament data sent to him by organizers. So could he only refers to the legitimate interests of Art. 6 Para. 1 Letter f GDPR. According to this, the processing is only lawful if it is used to protect the legitimate interest food of the person responsible or a third party is required

is provided not the interests or fundamental rights and reason freedoms of the data subject, which require the protection of personal data, prevail, especially if

these are children.

Hobby as legitimate interest?

The person responsible explained his actions to me with a "hobby project" and drew attention to the possibility of comparing the performance of the individual players. However, his interest differs from that of a pure tournament organiser/host, who wants to draw attention to himself and his event with the presentation of the results and wants to promote interest in golf. In addition, the organizers
or organizers cannot find a rank or point value expressing the respective playing strength. Based on this, my authority saw no need or necessity to offer interested website visitors a player portrait with an individual ranking value in addition to the results of the organizing clubs and sports associations that can be called up on the Internet. In addition, the person responsible placed the information he had collected in new contexts.

The special protection of children

The inadmissibility of data processing becomes even clearer when the mutual interests are weighed. From the textual formulation it is already clear that
that the protection of children has a high priority.

The legislator has also emphasized this special protection in the recitals (recital 38 to the GDPR). This is only opposed to the hobbyist interest of the site operator. In the case of an Internet publication, it is particularly important that the personal data of the children and youth players presented is publicly accessible to everyone and can be distributed practically without limits via the Internet. Particularly problematic in the case presented was the individual rank value, which according to

position of the person responsible should express the playing strength of the respective player and thus ultimately enable comparability and ranking. If you only take the different pitch or weather conditions, I doubt that an objective comparison value that expresses performance can be determined at all, especially since not every youth player took part in all events and tournaments and the result lists presented were sometimes incomplete.

Ultimately, the method used to determine the point value also remained completely opaque. The page FAQ contained only very general information on the criteria that were included.

summary

In order for the competition results of children and youth golfers to be presented in compliance with data protection regulations, the responsible website operator would have had to show the consent of the legal guardian (Art. 6 Para. 1 Letter a in conjunction with Art. 7 and Art. 4 No. 11 GDPR). , as well as for the player portraits (first name, surname, photo, age group, ranking). After my authority pointed this out and he obviously had no consent, he took the website offline and also proved to my authority that all player-related personal data of the children

What should I do?

and young people had been deleted. did

Internet presences operated as a

hobby are also included, provided

they are not exclusively personal or

actually, the controller had the data subjects

family-related – cf.

not even about their inclusion on his website

Art. 2 para. 2 letter c GDPR

– under the scope of the GDPR. This

also applies if information is partly

bid informed (Article 14 GDPR).

In addition, a person responsible is always obliged to prove

that the personal data processed by him/her are processed in

have been compiled from

generally accessible sources.

a lawful manner (accountability, Art. 5 Para. 2 DSGVO). In the

Are third

case of processing based on consent, this requires that the

Persons and minors are affected,

person responsible has this (in writing) and that it is

consent is required, especially if

images are to be distributed.

their content also to the data protection law

specifications oriented.

2.4 Sensitive Data, Special Categories of Personal Data

2.4.1 Corona at school

ÿ Art. 6 GDPR, SächsCoronaSchutzVO, SchulKitaCoVO

My authority received numerous submissions in connection with the regulation in the Saxon Corona Protection Ordinance (SächsCoronaSchVO) and in the later school-specific school and daycare Corona Ordinance (SchulKitaCoVO) of the Free State of Saxony, according to which access to school is only permitted with testing is permitted. The complaints related to testing in class groups and the resulting possibility of mutual knowledge of the test results. As a result, however, my authority had no objections to carrying out these tests.

If the test result is positive, the person who tested positive must isolate themselves immediately; underage pupils Students are excluded from the rest of the class separate and collect from the person with custody. This is absolutely necessary and the inevitably associated processing of personal data is lawful accordingly. In this context, it makes no difference whether a positive test result is already determined in the test in the class association.

Decision OVG Bautzen:

With a decision of April 9, 2021 (Ref.: 3 B 114/21), the Saxon

Higher Administrative Court (OVG) issued a statement on related

data protection issues and the compatibility of the test regulation

with the GDPR. In this decision, based on Art. 6 and 9 GDPR,

the OVG examines the disputed regulation in the

SächsCoronaSchVO of a sufficient legal basis for authorization

Art. 6 Para. 1 Sentence 1 Letters c and e GDPR. Also standing

Art. 9 Para. 1 GDPR does not prevent the collection of personal

data. According to Art. 9 Para. 2 Letter h GDPR, paragraph 1 of

the provision does not apply, among other things, if

if the processing is for health care purposes

- as here - is required.

The SächsCoronaSchVO (or later the SchulKitaCoVO) also provided for

the obligation to wear a medical face mask (surgical mask), an FFP2

mask or a comparable breathing mask. You could be exempted from this

obligation with a medical certificate. Also

my agency received numerous petitions on this. Included

was the practice that can often be observed that headmasters only At

initially not covered by the regulations. This was finally "adapted to

practice" and contained these content-related requirements for the

certificates. After it was determined that anyone who has access to these

certificates has to maintain secrecy about the health data contained

therein

I have no serious concerns.

There were also other petitions to document this At

test. The SächsCoronaSchVO initially left a credible

making by granting inspection is sufficient.

The copy, which was nevertheless often made, was therefore permissible

at most with consent. Here, too, an authorization was finally included in

the SchulKitaCoVO to make an analogue or digital copy of the medical

certificate for exemption and to keep it. This must be secured against

unauthorized access and deleted or destroyed immediately after the

period for which the certificate is valid has expired, but no later than the

end of 2022.

Finally, with the enabling of a corona vaccination for young people from

the age of 12, this was included in the SchulKitaCoVO as an exception

to the mandatory test.

Here, too, initially only inspection of the convalescent or vaccination

certificate was regulated, despite experience with the certificates for

mask exemption; however, there is no corresponding documentation.

The result of this would have been that without the appropriate consent,

this evidence would have been presented again for each test.

the must. My predecessor in office therefore strongly

suggested to the legislator that a corresponding regulation

be made here as well. In the end, that was agreed.

Schools can now record and document the day on which

inspection of the vaccination or recovery certificate was

granted.

2.4.2 Biometric access

control in leisure facilities

ÿ Art. 6 (1) b and f GDPR, Art. 9 (1) and (2) f GDPR,

Art. 22 GDPR

A large leisure facility had introduced a mandatory

biometric access control system based on face recognition

to speed up its admission control. The long-term

customers had received a corresponding information

letter in which they were given the no alternative

change of the access control system had been

communicated. On their next visit to the facility, a digital

recording of them would be taken at the turnstile and

then stored (actually only as a non-recalculated template).

From then on, at each further visit, a new recording

would be made and compared with the first recording.

Insofar as customers had complained to the operator of

the leisure facility in this regard, the legality of the

associated processing of personal data was upheld with

Art. 6 Para. 1 Letters b and f General Data Protection

Regulation (GDPR) on the one hand and Art. 9 Para. f

GDPR justified on the other hand.

examination of the facts

The person responsible has the processing personal

ner data of his regular customers rightly first

based on Art. 6 Para. 1 Letter b GDPR (performance of

a contract concluded with the data subject) and also

correctly recognized that he - because of the processing bio

metric data - also a right

based on Art. 9 GDPR required. his assessment,

in this respect referred to Art. 9 Para. 2 Letter f GDPR

can, but was wrong.

According to this provision, the processing of biometric data

would be permissible if it is necessary for the assertion, exercise

or defense of legal claims or for court actions in the context of

their judicial work. In the present case, however, these

requirements were not met; the justification of the person

responsible that the biometric access control system can be

used to effectively rule out the repeated attempts at fraud with

the season tickets (use by third parties despite the exclusion of

transferability) and to be able to use such an identity check to

protect his contractual claims in the run-up to a possible legal

dispute,

was understandable, but not of Art. 9 para. 2

Letter f DSGVO covered.

A legal conflict, Art. 9 Para. 2 Letter f GDPR

could be applied does not already exist at the time the contract

is concluded or if the contractual relationship is undisturbed.

Only if there are irregularities in the fulfillment of the contract,

for example if one of the contracting parties does not fulfill his

obligations in this regard, especially if there is a suspicion of

abuse, and as a result

Legal dispute arises in which the person responsible

must assert or defend claims, this provision applies. This results

both from the wording of the provision itself, from recital 52 (last

sentence), and from the relevant commentary literature.

The rights referred to in Art. 9 Para. 2 Letter f GDPR

Although claims can arise from contractual regulations, for

example from damaging actions leading to claims for damages,

the existence of such a legal relationship alone is not sufficient

to justify the processing of biometric data.

Rather, this must first have resulted in a conflict that forces the

claimant to take procedural action to enforce the claim (Kuhling/

Buchner/Weisert, 3rd edition 2020, DS-GVO Art. 9 No. 84). Only

Art. 9 Para. 2 Letter f GDPR can be used to process data previously

processed on another legal basis, for example on the basis of consent,

in accordance with Art. 9 Para. 1 GDPR also to enforce these legal claims

che to use.

Art. 9 (2) (f) GDPR covers the use of special categories when enforcing

such legal claims, i.e. in the context of the respective dispute, but does

not create a legal basis for their processing in the underlying legal or

contractual relationship. Because then processing in this way would be

justifiable in any contractual relationship - after all, there can be

disruptions and abusive actions in every contract. If the legislator had

actually intended this, he would have had an Art. 6 para.

1 letter b GDPR comparable permission in

Art. 9 GDPR. The privacy reason

Instead, the regulation differentiates conceptually but clearly between the

processing of a contractual relationship (Article 6 (1) (b) GDPR) and the

enforcement of claims (Article 9 (2) (f) GDPR). It is therefore not justifiable

to use the exception in Art. 9 Para. 2 Letter f GDPR when processing

sensitive data to fulfill contractual relationships. The inclusion of out-ofcourt dispute resolution in recital 52 sentence 3 is

reinforced in view of

the wording there

the requirement of a legal conflict. Should be sensitive

If the data becomes the subject of the contract, an independent exception

is required, for example consent in accordance with Art. 9 Para. 2 Letter

a GDPR.

Face recognition only with consent

It follows from all of the above that the application scenario presented,

specifically the use of a biometric procedure to fulfill the contract (here:

granting access), cannot be based on Art. 9 Para. 2 Letter f GDPR. As a

result, the solution to the processing problem is already shown. Securing

access for permanent

Customers by means of face recognition is (only) possible if the consent

of the persons concerned has been obtained and is thus based on Art.

9 Para. 2 Letter a DSGVO

becomes.

In order for such consent to actually be given voluntarily, detailed

information is required

the responsible on the one hand and also one without the

Processing of biometric data coming from Alterna

tive for access control on the other hand. In addition, the

Responsible in relation to the granting of consent in the obligation to

provide evidence (Article 7 (1) GDPR).

I do not share the irrelevant objection that the consent solution is difficult

to implement, nor do I share the objection that the organizational effort

in the event that consent is not granted or in the event of a revocation is

technically, personnel and financially unfeasible. In any case, alternative

solutions must be planned and made available in the event of a system

failure of the biometric access control. If consent is revoked, it should be

possible to block the customer concerned in the reference database or

remove the template assigned to him with just a few clicks.

What should I do?

For the sake of completeness, Art. 22 GDPR – Automated decisions in

The use of a biometric

individual cases (here: granting access) – should also be referred to.

face recognition method

According to Art. 22 Para. 4 GDPR, such decisions may not be based

9 para. 2 lit.

on special categories of personal data according to Art. 9 Para.

1 GDPR, unless the data subject has consented to this or a substantial

f DSGVO are supported.

The person in charge has one

to obtain the explicit

consent of the persons

concerned.

public interest can be asserted. In any case, Art. 9 (2) (f) GDPR is not

mentioned in the relevant exceptions.

2.4.3 Engagement of an

external expert by a social

security authority

ÿ SGB X

The transmission of the applicant's documents to an institution

that acts as an expert on the part of the competent authority

in accordance with Section 21 of the Tenth Book of the Social

Code (SGB X) is permitted under data protection law.

The commissioning of an external expert, in this case to

prepare an opinion from a health care provider on an application

procedure pending at the authority, by the competent authority

is not dependent on the consent of the applicant having to be

obtained in advance, but falls within the decision-making

authority of the authority. The same applies if the administrative

procedure is pending before a court.

The selection decision, i.e. which external expert the authority

specifically selects as an expert to make a decision on the application, is not subject to the applicant's consent requirement, but falls within the discretion of the authority.

For a meaningful opinion from the medical officer, I also consider it permissible for the external expert to submit the documents consulted to the authority for inspection and therefore to be sent, since otherwise it is not possible to draw up an expert opinion - especially one that will stand up in court. The expert, as a helper and adviser to the authority, has the task of examining facts to be determined and assessed by the authority. The expert must be impartial, there may be no grounds for exclusion or partiality.

He must also have special expertise. The reports obtained in the administrative procedure are also to be used in the social court procedure, since they are not private reports (so Vogelgesang overall in: Hauck/Noftz commentary on SGB X § 21 marginal no. 18).

2.4.4 Measles Protection Act: Abnormalities in medical certificates

ÿ GDPR, IfSG, StGB

From the inquiries and complaints I have received regarding measles protection, it can be inferred that the management

of day care centers or other community facilities are increasingly being presented with so-called certificates of incapacity to vaccinate as proof of adequate vaccination protection against measles.

In the 2020 activity report (2.2.9, page 589), my predecessor had already commented on the Measles Protection Act.

At that time there were several cases in which parents had complained that the management of the day care centers copied proof of sufficient vaccination protection in order to add a document to the files. As stated, this was inadmissible.

The Infection Protection Act (IfSG) regulates compulsory vaccination against measles. If a child attends a community facility within the meaning of Section 33 No. 1 to 3 IfSG, e.g. a day-care center or school, then according to Section 20 (9) IfSG, evidence must be presented to the management of the facility that there is adequate vaccination protection against measles. This proof can be in the form of vaccination documentation (vaccination card or medical certificate), a medical certificate of immunity against measles or the existence of a medical contraindication or confirmation from a government agency or the management of another institution that the proof has already been provided, be led.

In my opinion, the vaccination card or a doctor's certificate may not be copied for data protection reasons, as these contain data other than that required by law - the principle of data minimization. § 20 paragraph 9 IfSG only requires

the submission of proof. Therefore, as explained in the

activity report mentioned above, copying of the evidence is

not permitted.

The "vaccination certificate" is a medical certificate that

certifies that in

there is a permanent "vaccination ban" of any kind on the affected child

due to a medical contraindication. A vaccination certificate can be a

reference point for a courtesy certificate.

The Saxon State Ministry for Social Affairs and Society

Social Cohesion (SMS) received the technical supervisory instruction

(decree) on the implementation of the Measles Protection Act for the

state in a letter dated September 7, 2021

Directorate of Saxony and the health authorities of the Free State

Saxony enacted. The appendix to this decree states that the certificate

does not have to be recognized if the management of the facility has

indications that it could be a courtesy certificate or if there are other

justified doubts as to the correctness of the certificate. This can be the

case, for example, in the case of a blanket denial of any vaccination

suitability with reference to an unspecified contraindication.

More information:

On the joint website of the Federal Ministry

ÿ www.masernschutz.de

for health with other public institutions

under the keyword "Heads of facilities, medical profession including

public health service" to the

Question "How to prevent incorrect vaccination documents/certificates

from being used?"

"Documents in another language, obviously forged documents or

obvious courtesy at

tests do not have to be recognised. In these cases is

notify the health department. The issuance and use of incorrect

health certificates for submission to an authority is punishable

under Sections 278 and 279 of the Criminal Code (StGB). This

also includes vaccination documentation. The issuing physicians

also face consequences under professional law."

(www.masernschutz.de/leitungen-und-aerzteschaft.html)

In my opinion, in these cases § 20 Paragraph 9 Clause 4 IfSG applies,

since the proof was not provided. The

The health authorities are to be notified and personal information is to be

transmitted.

What should I do?

In the meantime, the legislature has reacted to the compliance

There are doubts about the authenticity

certificates and when the IfSG was amended by the

or the correctness of the content of

Law of December 10, 2021 § 20 para. 9 to 12 new

the submitted proof of sufficient

drafted and a paragraph 9a inserted. It is regulated, as in the

vaccination protection against measles,

the management of the facility

according to § 20 para.

9 sentence 2 IfSG to notify the

responsible health authority

immediately. In this case, personal

data must also be transmitted.

case of doubts about the authenticity or correctness of the content

of the evidence is to be proceeded. According to § 20 paragraph 12 IfSG

For example, the health department has the option of asking

people who are cared for in community facilities to provide proof

in accordance with paragraph 9 sentence 1 IfSG

to submit.

2.4.5 Use of police officers for home

quarantine checks

ÿ GDPR, IfSG, IfSGZuVO

In early 2021, a petitioner contacted my authority and

requested the use of police officers for the control

to check its secretion. At the time of the check, he was in isolation

(home quarantine) as a category 1 contact person for a person

suffering from Covid-19. During his seclusion he was several times

been controlled. One of the control teams consisted of

two police officers. The complainant feared

that the health department had passed on his personal data or

health data to the police and asked me to check this.

The public health department of the district-free city confirmed

that the control measures had been carried out on the petitioner

and reported that the police officers within the framework of the office

were seconded to the municipality during the period in question.

They were used in the implementation of control measures like

municipal officials. They used civilian vehicles for the control

actions. They appeared in uniform.

The persons to be controlled were chosen at random. In the

present case, this led to the checks being carried out at the

petitioner's premises in quick succession.

The authority to order domestic quarantine and to check whether

this is being observed results from Section 28

Chapter 2

Paragraphs 1 and 3 of the Infection Protection Act (IfSG) in

conjunction with Section 30 Paragraph 1 Clause 2, Section 16

Paragraph 2 IfSG. Accordingly, the competent authority must take

the necessary (infection) protection measures to the extent and for

as long as it is necessary to prevent the spread of communicable diseases.

The districts and independent cities are according to § 1 Infek

tion Protection Act - Competence Ordinance (IfSGZuVO) the

responsible authorities.

The health department informs according to § 27 paragraph 1 IfSG ins

particularly in the cases of Section 25 (1) immediately the

competent authorities and transmits to them the information

required to fulfill their tasks. The information about who is in

quarantine at home could therefore be transmitted from the health

department to the public order office of the district-free city. The

purpose of the legal basis also includes monitoring the ordered

quarantine. According to Art. 6 Para. 1 Letter e,

Para. 3, Art. 9 Para. 2 Letter i GDPR permissible, as there is a

legal basis for this in the IfSG.

What should I do?

The use of the police officers during the secondment is carried out

It must be ensured that police

officers who are deployed as part

by the district-free city. The police officers perform tasks of the

of a delegation from a district-free

district-free city. During the secondment, the police officers do not

city do not transmit any personal data

perform any tasks of the police enforcement service. In doing so,

to the police enforcement service

without a legal basis.

no data may be "flown" to the police enforcement service, unless

there are statutory transmission bases.

2.4.6 Transmission of personal

data by rescue control centers to

the police for the purpose of criminal prosecuti

ÿ SächsBRKG

A rescue association described to my authority that courts, public

prosecutors and, on their behalf, police stations often required

information in connection with criminal investigations as to which

doctors and which non-medical staff were working at be

agreed to be involved in order to witness them

hear. In addition, there were inquiries about assignments; for example,

whether there was an operation due to bodily harm on a certain day at a

certain time and

who was treated as a patient or whether a be

right person was treated as a patient.

The Saxon State Office contacted by my authority

The Ministry of the Interior (SMI) reported that the transmission of

personal data, which the rescue coordination centers process as part of

their tasks under the Saxon law on fire protection, rescue services and

disaster control (SächsBRKG), to the police for the purpose of criminal

prosecution is inadmissible. The rescue coordination centers collect the

data in accordance with Section 72 (1) SächsBRKG. Transmission of the

data for other purposes, including criminal prosecution under Section 161

of the Code of Criminal Procedure (StPO), is excluded by Section 72 (2)

SächsBRKG. This legal regulation is also appropriate, since the personal

data of those cared for in the context of an emergency service operation

are patient data. This only applies if there is a corresponding declaration

of release from confidentiality.

The rescue coordination center does not have access to the personal

data of employees involved in a rescue service operation for police purposes. According to Section 28, Paragraph 2, Clause 2 of the SächsBRKG, it is the responsibility of the statutory health insurance companies to draw up the duty rosters for emergency medical services. On the other hand, the service providers according to Section 31 (1) sentence 2 SächsBRKG or the locally responsible rescue service providers (county, district-free city or rescue association) draw up the duty rosters for the needs-based staffing of the rescue equipment. In this respect, the police should contact the person responsible for human resources for information, for whom the general data protection regulations for handling employee data apply.

3 rights of data subjects

3.1 Specific Obligations of the Controller

3.1.1 Data protection information for citizens' requests

ÿ Article 13 GDPR

The initiators of a citizens' initiative asked in what form the information obligations when collecting personal data according to Article 13 of the General Data Protection Regulation (GDPR) can be fulfilled. They pointed out that corresponding signature lists do not offer unlimited space for additional information.

The Saxon State Office contacted by my authority

nisterium des Interiors (SMI) first referred to the note

se on data protection in the 2019 local elections

Comparable topic of collecting supportive signatures for election

proposals had been recommended,

the information sheet on data protection in the area of the municipal association

administration, in which the signature lists are laid out, to be posted and

to offer further copies to take away.

When asked, the SMI also agreed with me that it is sufficient to provide

the information sheet separately in paper form

and also to availability on the internet

point out (insofar as the persons of trust want to create such a website).

In addition to a reading copy, there should be several copies to take

away. Appropriate notice should be given. A "up

urge" of the info sheet to the effect that this must be given to everyone

before signing, is not he

conducive.

3.1.2 Video Surveillance

Information Obligations:

Purpose and Legitimate Interests

ÿ Art. 6 Para. 1 Letter f GDPR, Art. 13 GDPR

In the course of supervisory dealings with video surveillance systems,

the fulfillment of the information obligations under Article 13 of the

General Data Protection Regulation (GDPR) is also a regular issue. In

the 2019 activity report, my predecessor in office presented the two-stage information concept recommended by the German supervisory authorities and also shared by the European Data Protection Committee under point 3.1.1 (page 71ff.).

The differentiation between the purpose of the data processing to be stated under Article 13 (1) (c) GDPR on the one hand and the legitimate interests under Article 13 (1) (d) GDPR regularly causes practical problems GDPR on the other hand.

In fact, both pieces of information are difficult to tell apart to delimit. The commentary literature mostly does not go into a distinction and happily uses relevant formulation examples both for the purpose of data processing and for the interests pursued with the processing. Since, as is well known, video surveillance is not specifically regulated in the General Data Protection Regulation, there are no special specifications or examples for the fulfillment of the information obligations for this area of application anyway.

The problem is at least touched upon by Bäcker (Kuhling/Buchner, 3rd edition 2020, DS-GVO Art. 13 No. 27), who explains that the information obligation under Art. 13 para.

1 letter d GDPR partly with the obligation from Art. 13 para.

1 letter c GDPR overlaps, since in the cases of Art. 6

Paragraph 1 letter f GDPR the legitimate interest at the same time

forms the purpose of the data processing. Their independent content

results from the fact that a legitimate interest of the person responsible or a third party only justifies data processing if it outweighs the conflicting interests and rights of the person concerned. According to Art. 13 (1) (d) GDPR, the person responsible is obliged to present the relevant aspects for this balancing of interests in such a way that the data subject can understand the balancing and, if necessary, raise substantiated objections against it.

OH video surveillance:

ÿ sdb.de/tb2107

Statements on this topic can be found in the video surveillance guide of the data protection conference

under points 2.1 and 2.2.1:

“Before a video camera is activated, the purpose of the video surveillance must be clearly identified and defined for each processing operation. Video surveillance can be used, for example, to protect against break-ins, theft, vandalism (property protection) or attacks (personal protection). […] Therefore, if the video surveillance is intended to protect against burglaries, theft or vandalism, this can generally be seen as a legitimate interest. The same applies to interests such as preserving evidence for enforcing legal claims, preventing fraud, misuse of services or money laundering.”

In the same way, the EDPB Guidelines 3/2019 on the processing of

EDSA Guidelines 3/2019: ÿ

sdb.de/tb2108

personal data by video devices, version 2.0, mix these two terms. In

para. 19 of the paper states:

"The purpose of protecting property from burglary, theft or

vandalism can represent a legitimate interest in video surveillance

if there is an actual risk situation."

In this respect, a conceptual identity is also assumed there. This also

changes with the involvement of in

item no. 15 of the guidelines or the examples of purposes listed

in para. 18 made statement that legitimate interests of a person

responsible or a third party are more legal

can be of a physical or immaterial nature, nothing.

"Video surveillance can serve a variety of

purposes, such as protecting property and other assets,

protecting the life and physical integrity of individuals,

gathering evidence to enforce civil claims."

EDPB Guidelines 3/2019 on the processing of personal data by video devices, para. 15

The conceptual meaning of the word purpose - generally

understood as the motive for a targeted activity - does not allow

a clear distinction to be drawn from legitimate interests, rather

this also leads to the assumption that the legitimate interests

are largely congruent.

In practice, against this background, I can only give a rough

recommendation that it should generally be sufficient to choose

a rather general, catchphrase-like statement (overriding goal)

when stating the purpose, while the presentation of the

legitimate interests should then be more specific and detailed

in order to enable the data subjects to understand the weighing

of interests carried out in accordance with Article 6 (1) (f)

GDPR. Ultimately, it is important that the addressees as a

whole, i.e. from both statements together, are aware of the –

legitimate – reason for which the video surveillance system is

being operated. Conceivable indications of purpose would

therefore be, for example, information such as

• Protection of property (burglary, theft, vandalism) •

Personal protection (protection of physical integrity) • Exercise

of the duty of supervision • Exercise of domiciliary rights

• Traffic monitoring/traffic coordination • Billing (e.g.

when using

parking areas)

while in the case of legitimate interests, further explanations such

as

• Deterrence of potential criminals •

Investigation of criminal offenses/preservation of

evidence • Enforcement of civil claims/

Preservation of

evidence • Securing/monitoring of danger areas •

What should I do?

In order to fulfill the information

obligation, the purposes of the data

processing must be specified. The

purposes of

Data processing on the one hand

and legitimate interests according to

Prevention and prosecution of theft, vandalism

and burglary

• Determination of downtimes (for example on

parking areas)

• Entry and exit control

• Examination of access authorization

Art. 13 Para. 1 Letter d

DSGVO are to be distinguished.

Supports the person in charge

could be made. Insofar as controllers already provide sufficiently

detailed information under the purpose, it should nevertheless also

to legitimate interests, he must also

provide information according to the

regulation.

be legitimate to simply refer to the purpose in the case of legitimate

interests.

3.1.3 Operation of a customer center

by a contractor of the controller

ÿ Art. 13 Para. 1 Letter e GDPR, Art. 28 GDPR

A customer of a funeral home (responsible person) complained

that this was a subcontractor

used as the operator of a "customer center" and there the

would have passed on the customer data required to prepare a

customer account. The data subject also complained that the data

protection information and

- do not indicate the commissioning and data transfer

would have been set forth.

First, as part of the data protection control, my

On the one hand, it had been determined that order processing

within the meaning of Article 28 of the General Data Protection

Regulation (GDPR) was to be affirmed. The information obligation of

responsible to the data subject in accordance with Art.

13(1)(b) GDPR should therefore also have contained

specific information about this (already known) processor,

which, according to the complainant, was not

had been the case.

It was confirmed that data processing processes, such

as the procedure carried out for the complainant to

prepare a customer account, including sending a

registration link to his e-mail address, were not included

in the funeral home's data protection information.

However, this subcontractor was named in other contexts

in the data protection information with full details. It was

shown that it should be commissioned to "carry out and manage online deregistration and to regulate digital inheritance". In addition, setting up a “memorial portal” for the deceased – albeit to be commissioned separately by the customer – was mentioned as a task for the subcontractor. The detailed services were to be regarded as relatively complex and the associated data processing as multi-layered.

Nevertheless, responsibility remained as a reproachable omission

The missing reference to the fact that the preparation of the customer account should already be carried out by this very service provider. In this respect, the declaration was deemed incomplete within the meaning of Art. 13 Para. 1 Letter e GDPR value.

However, the activity of the service provider as a contractor was not concealed in this case, since the corresponding commissioning for the “implementation and administration of online deregistration and for the regulation of the digital inheritance” was agreed with the customer in an individual contract had been. Nor was any extra or onerous Data processing with the activity of the contractor tied together.

Taking into account the overall circumstances, my authority assessed the lack of granular data protection notices as not comprehensive. The

Chapter 3

Machine Translated by Google

I have completed the process with general information to those

responsible.

What should I do?

I advise those responsible to comply

In general, it can be summed up that customers should better ask more

with their data protection notices

about data processing and services in advance than too little, and as

Art. 13 and 14 GDPR

soon as they have gained clarity, they should also fix desired special

to group processing purposes

features or deviations from the usual contract content with a wording

and to deal with these purposes

in full in each case.

that is accepted by both parties.

Should the data protection information

are not overburdened by a

description of all conceivable

processing variants, the persons

Those responsible should note that turn together

comprehensive or summary representations of processing processes

concerned are also to In

can lead to loss of information. It is also important to map profoundly

information, if necessary, to make

individualized contract designs in the information according to Art. 13

available a supplement or amendment

and 14 DSGVO in a data protection-fair and transparent manner, Art. 5

tailored to the concluded contract.

Para. 1 Letter a

GDPR.

3.1.4 Processor as recipient

according to Article 13 GDPR

So that data subjects can exercise their rights under the GDPR

they need meaningful information about the fact that and how their

personal data is being processed. Therefore, the GDPR provides for

information obligations for those responsible. The recipients of the

to name data from the person responsible.

According to the prevailing opinion, processors are still

"recipients" (Ehmann/Selmayr/Knyrim Art.

13 para. 33; Gola/Franck Art. 13 para. 15; Kühling/Buchner/Bäcker Art.

13 para. 28; Paal/Pauly/Paal Art. 13 para. 18, Art. 4 para. 57; BeckOK

data protectionR/Schmidt-Wudy, 35.

Ed. February 1, 2021, GDPR Art. 14 para. 51), with the result that

they are also exempt from the information obligation under Art. 13 Para. 1

Letter e GDPR are included.

According to Paal/Pauly/Paal DS-GVO Art. 15 para. In principle, there is

a right to choose between "recipients" and "categories of recipients" in

favor of the person responsible.

Baker in Kühling/Buchner DS-GVO Art. 15 Rdnr. 16, on the other hand, states: “If he still or already knows the recipients of the data, he must name them on request. However, this can lead to a collision between the Data protection right of the person concerned to information and conflicting secrecy interests of the data recipients. If these confidentiality interests prevail, the person responsible may (and if necessary must) limit the information to a categorical description (unlike the previous edition). "The "or" in Art. 15 Para. 1 Letter c DSGVO can only be difficult to overcome. In case of doubt, I accept the indication of the category, although “contract processor” is actually very general and can be anything from document shredders to letter shops to contract data centers.

Recital 63 seems to support the view that in any case the

What should I do?

In order to create the necessary transparency, processors must also be specified by the person responsible for the proper fulfillment of the information obligations.

"recipients" are to be informed and that the categories of recipients are optionally informed can become.

However, the simple statement “contract processor” will not be sufficient as a category, so a more precise definition is

required.

3.2 Right to information

3.2.1 Information according to Article 15

GDPR by the bailiff

ÿ Art. 12, 15 GDPR

A petitioner approached my authority with the statement that

a bailiff he was asking for information on processing

processing of his data in accordance with Article 15 of the

General Data Protection Regulation (GDPR), had refused the

information on the grounds that this was to be provided by the

local court in whose judicial district he was active.

According to Art. 15 Para. 1 GDPR, the data subject has this

Right to request confirmation from the person responsible as

to whether personal data concerning you

are processed; if so, she has a right

for information about this personal data and on

Further information.

The local court, which was asked by my authority for an opinion, initially

stated that bailiffs had an independent obligation to provide information

on request under Art.

15 GDPR and corresponding requests for information are to be answered

by the management of the competent district court.

My - contrary - position is as follows: I have always seen

the bailiff, who is an independent enforcement body alongside the enforcement court (BVerwG, 29.04.1982, Az.: 2 C 33/80), as data processing or responsible body and since in force comply with the GDPR as responsible within the meaning of Art. 4 No. 7 GDPR (cf. 19th activity report for the public sector, 04/2017 to Activity report 2017/2018: ÿ sdb.de/ tb2109 12/2018, page 196). From my point of view, the following considerations are decisive for this classification.

The bailiff acts independently in the enforcement assigned to him (§ 1 Para. 1 Sentence 1 of the Bailiff Ordinance {GVO}). He keeps an official seal and business and cash books as well as his own responsibility for the files. He regulates his business operations at his own dutiful discretion (§ 29 GVO) and keeps an office at his office at his own expense (§ 30 Para. 1 GVO). The bailiff is obliged to employ office workers at his own expense, insofar as business operations require it; He is responsible for their activities (§ 33 Para. 1 GVO). He keeps the files according to §§ 38ff. GVO and is responsible for their correct storage and destruction (§ 43 GVO). According to § 29 GVO, the bailiff decides on the introduction of data processing procedures in his office on his own responsibility (point CI of the administrative regulation on the business instructions for bailiffs {GVGA} and the GVO); he has when using

data processing procedures to ensure compliance with

data protection regulations (point C.XV. of the VwV on
the GVGA and GVO).
The degree of autonomy and personal responsibility
expressed in these provisions when fulfilling his tasks also and especially with regard to aspects of data protection law - justifies considering the bailiff as the
person responsible, who has the Zwe
The scope and means of processing personal data (Art.
4 No. 7 GDPR) and data subject rights within the meaning
of Art. 13ff. GDPR has to be fulfilled on their own
responsibility. He is not to be regarded as an employee
of the District Court.
If one placed the obligation to fulfill information claims of
affected persons regarding their data processed by the
bailiff with the authority management of the district court,
this led to the absurd situation in terms of data protection
law that the bailiff initially
would have to provide the court with data about the
person concerned that is not available there, which the
court would have to take note of and forward to the
person concerned solely for the purpose of providing
information. This contradicts both the principle of data
minimization (Article 5 (1) (c) GDPR) and the legislator’s
will to initially and permanently assign the processing of
personal information from enforcement contexts
exclusively to the bailiff without court proceedings (see
also § 42a paragraph 3 Saxon Justice Act).

This finding is underlined by the regulations on the access

to files for parties involved in the proceedings, which the

bailiff has to grant and not the (enforcement) court, § 760

Code of Civil Procedure (ZPO), § 42 GVO.

In a decision dated May 20, 1998, Az.: 1 UE 1127/95,

the Hessian Administrative Court naturally assumed that

the bailiff

acts as an independent data processing agency and

corresponding data protection obligations - also

towards data subjects – has to be fulfilled. The legal situation on which

the decision is based has changed in

substantive-legal point of view by the entry into force of

DSGVO not changed.

In this regard it is worth noting that also

according to the Saxon State Ministry of Justice

and for Democracy, Europe and Equality, the courts

executor in the Free State of Saxony of my data protection law

are subject to public supervision because they are not courts when

carrying out enforcement actions.

The district court was requested by my authority to refrain from the

previous procedure and request information from the bailiffs of this own

What should I do?

Applications addressed to

to be processed responsibly. In the specific case, hit the

bailiffs by data subjects

persons upon request

Bailiffs are obliged to respond to requests for information addressed to

Art. 15 GDPR are through the

them in accordance with Art. 12 and 15 GDPR.

bailiffs themselves

The district court then announced that it had corrected the procedure and

answer that to that extent

Responsible in the sense of

had informed the bailiffs working for the responsible district court

Art. 4 No. 7 GDPR.

accordingly.

3.2.2 Admissibility of data

deletion when returning a defective

hard disk and right to information

ÿ Art. 4 No. 2 GDPR, Art. 6 Para. 1 Letter a GDPR, Art. 15 GDPR

After a complainant bought a laptop in April 2018, he discovered a hard

drive failure within the three-year warranty period. He then sent the hard

drive and the personal data stored on it to the dealer in April 2020,

although the dealer had previously pointed out to him that data backup

was his responsibility as the buyer.

A short time later, the dealer sent the buyer a hard drive that, as it turned

out immediately after the first test, was not his own.

First of all, the buyer tried to obtain information about the whereabouts of

his personal data on the hard drive by means of civil law, and

also assert a claim for damages by this means.

Although a civil court decision was imminent, the buyer felt compelled to (also) contact my authority at the same time with a data protection complaint. In it, he initially stated that the hard drive sent to him contained highly sensitive personal data belonging to a third party neither a confirmation of the proper deletion of all data nor a certificate documenting the destruction of the hard drive dealer received.

court decides

In its decision, the civil court followed the reasoning of the retailer, who claimed to no longer be in possession of the hard drive. The hard drive was replaced, the old hard drive destroyed and the personal data supposedly on it was therefore not passed on to any third party. The complaint under data protection law and the civil lawsuit were based solely on the assumption that the personal data allegedly present on the hard drive had been unlawfully disclosed. However, there was a lack of objective evidence of a data protection violation in this regard, since the buyer failed to provide proof of access to the hard drive and thus access to the data on it.

As a result, the complainant appealed against the firstinstance judgment of the civil court and at the same time

brought an action against my negative decision with the responsible administrative court. However, the Court of Appeal rejected the appeal in its entirety, citing the judgment of the first instance. As a result, the complainant apparently saw little chance of success even through administrative legal action, so he decided to withdraw the action against my authority.

In this case, the court of appeal saw no illegal data processing by the retailer in the destruction of the hard drive. The associated deletion of the data represents data processing in accordance with Art. 4 No. 2 General Data Protection Regulation (GDPR). This also applies if it was carried out solely by destroying the data carrier (cf. insofar as Kühling/Buchner/Herbst, 3rd ed 2020, GDPR Art. 17 para. 39). From a data protection point of view, consent or another legal basis from Art. 6 Para. 1 DSGVO was required for their admissibility.

In this respect, the destruction of the hard drive was neither necessary to fulfill the contract between the buyer and the dealer (Article 6 (1) (b) GDPR) nor due to a legal obligation (letter c), to perform a task in the public interest (Letter e) or to protect a vital interest of the data subject or another natural person (letter d). However, the court saw the data medium destruction as being legitimized by the buyer's consent (Art.

6 paragraph 1 letter a GDPR). The consenting act lay in the coherent conduct of the buyer in returning the hard drive as part of the contractual guarantee, since the retailer had pointed out that the buyer was solely responsible for data backup.

request for information

As far as the request for information on the basis of Art. 15 GDPR is concerned, this only includes the right to information as to whether personal data is being processed. An obligation to provide information relating to the past, which also includes data that has already been deleted, would otherwise contradict the principle of storage limitation in Art. 5 Para. 1 Letter e GDPR and the storage periods to be specified via Art. 15 Para. 1 Letter d GDPR (Kamlah in: Plath , GDPR/BDSG, 3rd edition 2018, Art. 15 GDPR, No. 5; BeckOK data protection R/Schmidt-Wudy, Art. 15 GDPR para. 52; Kühling/Buchner/Bäcker, Art. 15 GDPR para. 9).

With the information about the whereabouts of the hard drive, the court considered the right to information according to Section 362 of the German Civil Code (BGB) to be fulfilled.

In this regard, it referred to the decisions of the Federal Court of Justice, according to which a right to information is fulfilled if the information according to the declared will of the debtor represents the information in the total scope owed.

Any inaccuracy of the content of the information does not preclude the fulfillment of the obligation to provide information, because only the possibly implied declaration of the information debtor that the information is complete is essential. Only the suspicion that the information provided is incomplete or incorrect cannot justify a claim for information to a greater extent (cf. BGH, judgment of September 3, 2020 - III ZR 136/18, GRUR 2021, 110 para. 43 with other evidence). The acceptance of such a declaration content therefore presupposes that the information provided should clearly and completely cover the subject matter of the legitimate request for information (Federal Court of Justice, judgment of June 15, 2021 - VI ZR 576/19 -, para. 19 -20, juris).

This sums up the following:

• From the point of view of data protection law, it is undisputed that in the destruction of a data medium containing personal data is

What should I do?

As far as affected persons

processing of personal data in accordance with Art. 4 No. 2 GDPR. • The consent according to Art. 6 Para. 1 Letter a

It is recommended to use IT service

providers who entrusted to the service

providers

to back up personal data stored on

data carriers beforehand in order to

be able to access copies in the event

of a possible loss of data.

GDPR in

the data processing (here: destruction or deletion) can also take

place through conclusive behavior, such as returning a hard

disk to the seller under a contractual guarantee with prior

reference to the sole responsibility of the buyer for data backup.

• In order to fulfill the obligation to provide information according

The information of the person responsible

must be done in full.

It is not about the correctness of

to Art. 15 GDPR, it is sufficient if the information is provided

according to the will

the content. Subjective doubts as

to the completeness do not justify

of the person obliged to provide information includes the scope

any claim to a further scope of

information.

owed, even in the event of any incorrect content

of information.

Machine Translated by Google

The legal dispute was pending at the Dresden Higher Regional

Court, judgment of August 31, 2021 - 4 U 324/21 -.

3.2.3 Free copies of exam

papers

ÿ Section 28 (2) SächsJAPO, Article 15 (3) sentence 1 in conjunction with Article

12 (5) sentence 1 GDPR, Article 23 GDPR

During the reporting period, a petitioner turned in a data protection complaint to my authority. He shared that he was after after successfully completing the state compulsory subject examination, I applied for electronic copies of his written exams from the State Judicial Examination Office (LJPA). The LJPA also complied with this, but charged costs of 30 euros. The petitioner saw the obligation of the LJPA, according to Art. 15 para. 3 sentence 1 in connection with Art. 12 para. 5 sentence 1 of the General Data Protection Regulation (GDPR) to make the copies available free of charge violates.

When I asked, the LJPA informed my authority that the costs would be charged on the basis of Section 13 (5) of the Saxon Administrative Costs Act (SächsVwKG) as expenses for reproductions. Until the decision of the Federal Administrative Court in an (apparently) similar legal dispute from North RhineWestphalia (see Higher Administrative Court for the State of North Rhine-Westphalia, June 8, 2021, Az.: 16 A 1582/20), this approach will be followed hold onto.

GDPR applies

The LJPA's approach of charging expenses for the provision of copies of examination papers violates Art. 15 (3) sentence 3 in conjunction with Art. 12 (5) sentence 1 GDPR. The provision of information in accordance with Art. 15 Para. 3 GDPR takes place in the case of initial information in accordance with Art. 12 Para.

5 sentence 1 GDPR free of charge. This also applies to a copy.

The Saxon Administrative Costs Act does not apply to the

issuance of copies in accordance with Art. 15 Para. 3 Sentence 1

and Sentence 3 GDPR.

The GDPR applies to written examination papers.

The written exams prepared by the petitioner and the examiner's reports

are personal data within the meaning of Art. 4 No. 1 DSGVO, with regard

to which

he basically has a right to information in accordance with Art. 15 Para. 1

GDPR and the right to have copies made available in accordance with

Art. 15 Para. 3 Sentence 1 GDPR. This corresponds to the supreme case

law of the European Court of Justice (ECJ, December 20, 2017, case

no.: C-434/16). In addition, this personal data is also stored in a file

system in accordance with Art. 2 (1) GDPR. After

written exchange with the LJPA existed regarding

of the applicability of the GDPR to the present case, there was early

agreement between our houses.

In the Free State of Saxony there is no regulation that

right to information and the issuance of a free first copy with regard to

legal examination work in accordance with the provisions of Art. 23 GDPR.

The Saxon regulation on the inspection of examination papers cannot

restrict the right under European law to receive a free copy. The right to

inspect examination papers is only standardized in a legal ordinance,

namely in Section 28 (2) of the Saxon Lawyers Training and Examination Regulations (SächsJAPO).

This provision – which nowhere refers to the right to information that is determined by European law and includes written examination papers – is to be qualified as a legal-restricting standard that supersedes the right under Art. 15 GDPR, with the requirements of Art.

23 para. 2 GDPR to a legally restrictive regulation

just as difficult to reconcile as with the essentiality theory of the Federal Constitutional Court, according to which the decision on essential questions is reserved for the parliamentary legislature and cannot be transferred to the executive. The right to inspect examination papers is not mentioned in § 9 of the Saxon Lawyer Training Act (SächsJAG), the legal basis for issuing a statutory ordinance; in

§ 9 SächsJAG also has no reference to Art.

15 GDPR or to a possibility of restricting the right to information according to Art. 15 GDPR. Since the GDPR came into direct effect on May 25, 2018, both the Saxon Lawyer Training Act and the Saxon Lawyer Training and Examination Regulations have been amended.

In none of these changes was a restriction of the right to information under Art. 15 GDPR considered or even implemented.

The Saxon Administrative Costs Act and thus Section 13 (5) SächsVwKG, on which the LJPA is based, apply to the collection

of fees and expenses (administrative costs) for individually attributable public-law services by the authorities of the Free State of Saxony, but according to Section 1 Para. 2 SächsVwKG to the collection of administrative costs according to other legal provisions, including the directly applicable legal acts of the European Union, only supplementary application, insofar as nothing there
Deviating is determined. In Art. 12 Para. 5 Sentence 1 GDPR the free of charge is clearly standardized - in connection with Art. 15 para. 3 sentences 1 and 2 GDPR, it also refers to misleadingly on a first copy - so that the Saxon Administrative Costs Act does not apply in this respect, precisely because of a different regulation in a directly applicable EU regulation. The state legislature has seen the priority of application of European law here and has particularly emphasized this in the formulation of Section 1 (2) SächsVwKG – declaratively.
procedure changed
Unfortunately, the LJPA did not respond to these indications of the – clear – Saxon legal situation and announced that it would continue to charge costs for copies of examination papers in accordance with Section 13 Section 5
to raise SächsVwKG.
Only after my directly opposite the Saxon State Ministry of Justice and for Democracy, Europe and Equality

intention expressed by way of an order pursuant to Art.
58 Para. 2 Letter c GDPR to instruct the LJPA to test
are able to provide a first copy of their written examination
What should I do?
papers free of charge upon request, the LJPA has
The LJPA must provide examinees with
reviewed its legal position and previous practice again
a copy of their examination papers that
they have requested free of charge.
and decided to no longer adhere to this and to issue
copies free of charge.

4 Obligations of controllers and processors

4.1 Responsibility for processing, technical design

4.1.1 Simplified test scheme for the use of additional services on websites/apps according to GDPR, TTDSG and Schrems II

ÿ § 25 TTDSG; Art. 6, 8, 25, 28, 32, 49 DSGVO

Again and again I am asked by those responsible that it
is so terribly complicated with cookies and data protection.

Well, it's actually not that complicated, there are also

many working aids from the supervisory authorities, most

recently the Telemedia Orientation Guide, which was

OH telemedia:

ÿ sdb.de/tb2110

updated due to the changes in telemedia. Nevertheless, I

will try to present it briefly here

which requirements must be observed and which points

the supervisory authorities pay particular attention to

when examining websites and apps.

In principle, there are three groups of requirements

observe. On the one hand, of course, the Basic Data Protection Ordinance

ordinance (DSGVO) - in particular Art. 25 and 32 - for all

processing of a website or an app. It should be noted that

each resource, including an integrated font or an

embedded video from a third-party server, represents

separate processing. Furthermore, the Telecommunications

Telemedia Data Protection Act (TTDSG) has been in

force since December 1, 2021, which in principle requires

consent to the setting and reading of cookies and

similar technologies on end devices. Finally, the so-called Schrems II

judgment of the European Court of Justice must be observed, which

makes data transfers to non-European third countries significantly more

difficult.

How can these requirements be met and when is consent

required?

Understandably, many people in charge want to

do without the unloved consent banner that many users find annoying.

However, this is only possible under very strict conditions. The GDPR

regulates all processing and requires the existence of a valid legal basis.

The most likely legal basis for websites and apps, in addition to consent

(Art. 6 Para. 1 Letter a), is legitimate interest (Art. 6 Para. 1 Letter f).

However, this legitimate interest must be proven and requires a balance

between the interests of the person responsible and

the interests or fundamental rights and freedoms of the

affected person. This is anything but trivial, a mere

A justification of usefulness on the part of the person responsible is not

sufficient. In practice, this is one of the most common mistakes when the

supervisory authority asks the Ein

set of a third-party service purely with the interests of the Ver

responsible and existing risks are justified purely by the fact that the

users want it that way. On the one hand, this is not a risk assessment

and it is also wrong, as the consistently high number of complaints in the

telemedia sector shows (see 6.2.2).

Facts that speak for a weighing of interests in favor of the person

responsible are, for example, verifiable order processing with an integrated

service provider that meets the requirements of Art. 28 GDPR or

processing by the person responsible himself or technical and

organizational measures such as rapid anonymization of data personal

data (e.g. IP addresses, cookie identifiers). Processing which, due to its risk, tends not to be based on a legitimate

Another interest that can be supported is the formation of profiles and so-called user journeys, i.e. everything that is commonly understood as tracking. As a rule, the legitimate interest must also be questioned if a third party uses the data obtained for their own purposes or if this is not clearly excluded. To put it bluntly: the use of the services of large providers whose business model is the collection and aggregation of usage data for advertising purposes and who also have the corresponding market power is of

legitimate interest

se of the person responsible. Especially since in many cases If the person responsible does not even know exactly how the service provider deals with the data obtained. However, case law clearly assumes that the person responsible also shares responsibility for the services used. If the prerequisites for a legitimate interest are not met, there is usually only recourse to consent. All the requirements of the GDPR must be observed, which requires strict rules for transparency, certainty and voluntariness as well as the consent of the legal guardian in cases of use by minors. It is indeed difficult to meet all these requirements

in practice, so I always recommend a careful check of

which processing operations are actually absolutely

necessary.

If consent is obtained, it must also represent actual

consent. Tricks that are often found in practice (keywords:

dark pattern and nudging) are clearly illegal if they exceed

a certain limit.

Small scope for cookies without

consent requirement

If cookies or similar technologies are used in addition to

processing, their use must meet the requirements of the

TTDSG, which generally requires consent. Even if this

law, which has been in force since 2002, converts the

European ePrivacy Directive into German law

sets, has not changed much, it should be clear to everyone

responsible that the mass setting of cookies is now

must come to an end. Exceptions to a consent requirement

are narrowly limited to an absolute necessity, so that the

provider can expressly request a consent from the user

desired telemedia service can provide.

What does that mean in practice? Of course, I support the

reversal of the consent requirement called for by some voices

according to the motto "People want it that way!"

not, but I also see possibilities for setting and reading cookies without consent. Based on the terminology of the user request and necessity, each cookie must be checked: When, how, for how long and for whom is a cookie set? It is about an evaluation of the purpose and the means!

The "when?" refers to the time of the betting.

An individualized shopping cart cookie in a

Online shop can only be set when the shopping cart is used.

This is not required for mere browsing. The same applies to cookies for additional functions such as chats or map widgets.

Here, the "when" can be determined based on the user's request; the cookie is only required when the service in question is actually available

is being used.

The "how?" refers to the content of the cookie. Cookies that set and/or read individual pseudonyms in the form of randomly generated or otherwise obtained information (unique device features in the form of fingerprints or device-specific identification numbers) are particularly relevant in terms of the provision of Section 25 TTDSG (protection of privacy in end devices). . In many

cases there is no need for this. That's how it is

It is not necessary to consider that consent management, which is intended to save the decision on the selection of desired processing, sets an individualized cookie (and certainly not when a website is called up initially before a decision has

been made, see above Unit volume). For storing the

It is sufficient to save this non-individually (e.g. in the form of

"tracking=false; comfort=true ...).

Since cookies with an individual ID pose the greatest risk to the privacy

of users

these are of particular interest to the supervisory authorities.

The “how long?” refers to the lifetime of a cookie. Again, it is crucial

whether it is a

individualized cookie acts because of this in combination

with a long running time enables the recognition of returning visitors to a

website. To be clear: cases of individualized cookies with

a runtime beyond a session are in practice

hard to imagine without consent. Also in the above

The shopping cart cookie mentioned above is permanent

Labeling of visitors is certainly in the interest of a shop operator, but this

is not possible without explicit consent.

The "For whom?" refers to the betting domain of one

Cookies or generally on the recipient of the data. Cookies and other

features that are set and read beyond the boundaries of the website

actually called up represent a high risk for privacy due to the associated

possibility of cross-website tracking. Here too, in practice, only very few

cases are conceivable which the exceptions to a consent requirement will

apply.

Better to avoid cookies

It must be clear to everyone responsible that the law requires that every

cookie has to be put to the test. If necessary, this opportunity should also

be used to check

which services also work without the setting of cookies

kidneys It is also clear that the supervisory authorities are not only

check the purpose, but also the specific means, and a general statement

that a cookie is required for load balancing, for example, is technically

checked in detail.

The consent requirement also includes "harmless" cookies, for

example a cookie that saves language settings in the form of

content such as "language=de". In this specific case, it is quite

possible that the supervisory authority will ignore the fact that

this cookie is already set when the website is called up.

Use of US service providers mostly

not possible

Finally, as a third aspect of a telemedia service, possible

references to third countries outside the EU must also be taken

into account. True, many service providers, especially

from the USA, European branches and offer order processing

contracts (their conformity with Art.

28 GDPR is left undecided here) and assure data processing

in Europe. However, data processing abroad “in exceptional

cases” is often not excluded in the contracts. In many cases,

the use of such service providers is simply not possible.

The conclusion of a contract with the European branch of a US

service provider also does not protect against access by foreign

authorities within the framework of the

Cloud-Acts.

Furthermore, there are no additional measures for the area of

usage data processing that can ensure protection of the data,

at least the IP address

and usage data of the end device are always affected and

cannot be secured. Even if those responsible occasionally put

forward it as an "additional protective measure", transport

encryption is clearly not such a measure, but standard and also

unsuitable for protecting exported data. In its guidelines 2/2018

on the exceptions under Article 49 of Regulation 2016/679, the

European Data Protection Board also stated that personal data

that is processed in connection with the regular tracking of user

behavior on websites or in apps is generally not based on

consent

What should I do?

Website and app operators

should avoid using

Cookies and other techno

check logies urgently.

In particular, the precise

design of the technologies and

their necessity must be

revised. kind and

Duration of storage and

subsequent processing must

meet the requirements of

Art. 49 Para. 1 Letter a GDPR transmitted to a third country

can become.

This article cannot cover all aspects, in particular those of

consent, in their entirety, but it is intended to show those

responsible how to operate a website or app securely

without requiring consent.

Because it is still possible to offer legally compliant services

without the unloved consent banner. However, it requires

a precise inventory and precise justifications.

TTDSG and DSGVO.

4.1.2 Electronic class register

ÿ VwV school forms

In the 18th activity report (2017), my predecessor in office

18. Activity report:

ÿ sdb.de/tb2111

described under 7.5 on page 96 that several inquiries about

the admissibility of a purely electronic grade book

unfortunately had to be answered negatively, since the

relevant VwV prescribed school forms for this as well as for the class diary, they in the format DIN A4.

With the new version of the administrative regulation of August 25, 2021, a different picture emerges. According to this, the student transfer directory, student file, grade book, class register and course book can now be in electronic form provided that specific technical requirements are met. For example, these documents must be backed up completely in unchangeable electronic form or in printed form as a stapled document. An electronic signature must also be used instead of the signum and signature. It remains to be seen how the latter in particular will be implemented in practice. Unfortunately, my suggestion to provide appropriate software as part of the Saxon school administration software (SaxSVS) has not been taken up for a long time.

4.1.3 Notices from bailiffs in sealed envelopes only

ÿ Art. 5 Para. 1 Letter f GDPR, Art. 32 GDPR

Citizens keep complaining to me about bailiffs who throw official letters or notifications relating to enforcement proceedings into mailboxes that other people have access to without an envelope, or who openly hand them over directly to

third parties (roommates or employees). It is thus possible for these persons (third parties) to gain knowledge of the existence of enforcement proceedings against the person concerned and of the content of the letter itself.

Regarding service by bailiffs, the 13th activity report for the public sector (2007), page 138, referred to the obligation to use envelopes. At that time it was about the formal (substitute) service of a court order.

On the occasion of the petitions that are still reaching me this topic I want to emphasize that not only formally documents to be delivered, but in principle also "simple" messages, for example the notification that contact is requested in a specific procedure, to be placed in a sealed envelope in the addressee's mailbox or - alternatively - handed over to a third party. Theoretically, an exception can only be made if the bailiff knows for sure that only the recipient has access to the mailbox. However, this will generally not be the case.

The reason for the obligation to use a sealed envelope – this also applies if it is put into a family mailbox on which only the family name is given – is that the bailiff is bound by official secrecy and to protect personal rights of the debtor concerned as the addressee of the letters ver is obligated. The fact that the addressee is involved in a foreclosure process is already a fact that requires secrecy and is not unauthorized

may be transmitted to third parties. Information about the debtor or the

subject of the proceedings that is subject to official secrecy must not be

passed to third parties (this also includes family members) without a

legal basis. There is no such legal basis for the disclosure of personal

data from the enforcement proceedings to third parties, which can also

What should I do?

lie in enabling the acknowledgment of an open letter. Therefore, the bailiff

For unauthorized knowledge

to avoid third parties

Bailiff notices and documents to

be served

always in a locked

always necessary for the protection of the debtor's right

Putting an envelope in the

mailbox or giving it to third parties

tary organizational measures - here the use of a sealed envelope - to be

hand over.

taken.

4.1.4 Forwarding of an email to a city

council by the Lord Mayor

ÿ Section 52 (5) SächsGemO, Art. 6 GDPR

A city councilor informed my agency that the Oberbür

germeister of a Saxon city addressed to him

Email from a citizen in response to a public

City Council meeting took place and the salutation addressed the City Council alone, read and instructed the “Ratsschreiber stube” to send this e-mail to everyone else forward to city councils.

The mayor, who was asked to comment, was initially unable to identify any data protection violations, since the message was addressed to the general city e-mail box. The original letter from the city council, to which the citizen had reacted, was also addressed “to the community of city councilors and the public”. Finally, it was objected that the citizen wanted to address the entire city council with the message.

The latter is not convincing because the city council was addressed personally in the e-mail. Also, addressing the City Council's letter "to the City Council community and the public" cannot be effect for the sender of the letter in question. Likewise, the forwarding of the e-mail was not

necessary. Although a mayor is officially obliged under Section 52 (5) of the Saxon Municipal Code (SächsGemO) to inform the city council about all matters relating to the municipality and administration, this does not include the forwarding of an e-mail addressed solely to a city councillor . The opposite does not result from a broad understanding of the concept of the matter in § 52 SächsGemO, in which a mayor decides on the

scope of his information obligation at his best discretion. The powers end where the personal rights of the recipient prevail, as is the case here.

The mayor finally recognized this and assured that in future the data protection regulations presented would be observed for explicitly addressed e-mails.

4.1.5 Cooperation on a successor solution for the video conferencing service

ÿ Art. 25 and 32 GDPR

The State Chancellery is responsible for providing and Operation of the Saxon administration network (SVN), with the all state and local authorities within one secure network can communicate. So-called basic services, such as a video conferencing service, are also part of the SVN. This was purchased as an on-premise service when planning the current SVN solution and made available to all authorities. On-premise means that the hardware and software for this solution are operated in a data center that is under the control of the State Chancellery stands. Now this video conferencing service was intended for special cases, because at the time of planning, situations such as a pandemic had not yet been considered. Unfortunately, when the public administration had to switch to home office on a large scale in the course of the corona pandemic, the solution was completely undersized. To remedy the situation, the State Chancellery has further licenses for the

Video conferencing service acquired and for sale to the authorities

made available.

Machine Translated by Google

Video conferencing service in the cloud not data protection compliant

After the additional solution, which was physically located in the cloud, my predecessor requested the underlying contracts and found that they did not meet the data protection requirements. For example, it could not be ruled out that the manufacturer used data for its own purposes, for example to improve the products, which is not compatible with order processing and for which a public body simply has no legal basis. Furthermore, it was not effectively ruled out that data transfers take place outside the European Union and data are processed in so-called unsafe third countries.

My authority pointed out these deficiencies to the State Chancellery, but in view of the urgent need for a video conference solution during the pandemic, a temporary toleration was agreed.

At the same time, it was agreed that a sub-working group of the SVN working group would be set up to find a legally safe successor solution that also met all the technical requirements. This sub-working group was headed by the SID on behalf of the State Chancellery and was made up of representatives from the technical departments of individual ministries and representatives of accessibility, the Information security and data protection.

As an explicit aim of the work, the state

law firm also strengthens the digital sovereignty of the

named Free State of Saxony, a goal that I also think

corresponds to ideas.

decision for free software

The sub-working group started its work quickly. A list of criteria with

legal, technical and professional requirements was created and numerous

possible products were examined in the context of tests.

As a result, the sub-working group made a recommendation for a product

based on free software

and operated by the Free State of Saxony under its own responsibility. It

became clear that too

Professional and technical requirements cannot only be met by wellknown manufacturers, as is often claimed.

My predecessor was also in favor of this product, both for reasons of

legal controllability and for economic reasons. For the cloud services also

included in the rating gro

My authority had asked for more international manufacturers

What should I do?

emphatically not said. Such data processing has high risks for legally

The Free State Authorities

compliant operation, since

Saxony are obliged to use video

Extensive contractual documents, complex data flows and frequently

conferencing services

to bring, which Art. 25 and 32

changing conditions are difficult to reconcile with the requirements for

DSGVO satisfy. The same applies

transparency, being informed and the rights of those affected. The result

to the use of cloud services.

has now been presented to the State Chancellery, I hope for a

corresponding response, but I will point out the deficiencies mentioned

Preference should be given to

systems operated autonomously and

above

under one's own responsibility.

no longer tolerate the future.

4.2 Order processing

4.2.1 Processing of personal

data when investigating

processes by "independent" expert comm

ÿ § 3 Saxon GDPR; §§ 4, 17 SächsVwOrgG; Article 28 GDPR

In the course of dealing with misconduct within the administration that

has become public knowledge and has the potential to cause a scandal,

an external expert or a commission made up of experts who are not

members of the Free State administration has been commissioned to

carry out the independent investigation in recent years

of incidents increasing in popularity. Mostly granted

Ministry of State, in whose area of responsibility the processes to be

examined took place, commissioned the expert by way of a civil law

contract to investigate and to submit a

final report. Particularly emphasized at the information

information to the public about the appointment of an expert

regularly the independence of the experts and the fact that they are not

given any instructions in the fulfillment of their mandate. Under a civil

contract, the experts are guaranteed access to official documents and

support from employees of the Free State.

I have long criticized this practice. On the one hand is the use of persons

under private law, for example in organizational investigations, in the

course of which no personal

Data are processed and not in fundamental rights of Per

sonen is intervened, unproblematic and given be

special expertise of externals for the desired purpose

On the other hand, the commissioning of private individuals to investigate

specific incidents that cannot be conducted without the processing of

personal data and for which the legislature has defined responsible state

agencies and procedural regulations, on the other hand, encounters the

greatest constitutional concerns.

No order processing when commissioning an

independent body

The indisputable power of a (supervisory) authority to obtain

comprehensive information about processes in its area of responsibility

to inform and this within the scope of their self-regulation

For constitutional and state organizational reasons, the investigation cannot include the commissioning of “independent” third parties or bodies outside the state administration to carry out activities that involve encroachments on fundamental rights. The assignment of a task alone does not authorize the competent state agency to transfer the execution of this task, which involves encroachments on fundamental rights, to a body outside the state administration that is independent and independent of instructions. A civil-contractual "appointment" cannot replace the necessary statutory transfer of a task performance that adversely affects fundamental rights. In terms of data protection law, it is also not commissioned processing (Art. 28 GDPR), the central element of which is that the commissioned processor is bound by instructions.

External, independent experts lack constitutional legitimacy

There is simply no such thing as state-initiated processing of personal data – an encroachment on fundamental rights – by an independent commission of experts, not bound by instructions, which is commissioned “freely” under civil contracts and whose members are not legally involved in the administrative structure of the supervisory authority responsible for the relevant investigations legal basis. However, such would be absolutely necessary and is to be found, for example, with regard to the involvement of other private individuals formal state procedures – namely the experts

who, in the event of their appointment, meet a public-law obligation to provide expert opinions and are remunerated in accordance with statutory provisions – in detail in the procedural laws.

So understandable the idea of a non-governmental, independent Commissioning independent private individuals who are not subject to directives to process personal data on their own authority, which public Saxon authorities have sovereignly collected and are storing within their statutory competence, is also just as unlikely to allow a pending body to examine official processes and incidents “particularly objectively”. essential principles of the rule of law. This

This applies all the more to cases in which there are misconduct relevant to disciplinary and/or criminal law, the prosecution of which is a core activity of the sovereign state and which is regulated in detail by law.

It is obvious that investigations by external experts in parallel with pending disciplinary and/or criminal investigations threaten to undermine statutory responsibilities and, above all, protective regulations. Strict legal rules bind the competent state bodies as norm addressees, but not the zi

contractually appointed external experts. The latter not only lacks constitutional legitimacy for its activities, it is also not subject to parliamentary control, unlike the state administration.

As a rule, the final report of the expert or the expert commission finds its way into the public domain, especially

if the results of the investigation show little or no evidence of incorrect action by the state ministry that commissioned the investigation. And of course such a final report is hardly conceivable without personal data from employees of the Free State or third parties.

Possibilities of involving external third parties

During the reporting period announced the appointment of an independent Commission of inquiry to clarify the so-called Ammunition scandals in the State Criminal Police Office to deal with these questions with the Saxon State Ministry of the Interior (SMI).

As a result of the exchange, there was agreement that the processing of personal data as part of the exercise of technical and administrative supervision by the highest Supervisory authority - the State Ministry - on § 3 Säch The Saxon Data Protection Implementation Act (SächsDSDG) in connection with §§ 4, 17 Saxon Administrative Organization Act (SächsVwOrgG) can be supported.

The supervisory authority also has the option of entrusting processors with certain processing of personal data, whereby the requirements of Art. 28 GDPR must be observed. A transfer of functions in such a way that the tasks incumbent on the State Ministry and the powers to which it is entitled are transferred to third parties for treatment without instructions at their own discretion is excluded.

A comprehensive (first) collection of data by external parties

would be inadmissible in the currently applicable legal

framework; This would apply a fortiori to the assignment of

tasks to third parties that the legislature has assigned to

certain state agencies (e.g. the public prosecutor's office or

the State Office for the Protection of the Constitution).

It also follows from this that external persons have no authority to issue

instructions to employees of public bodies in the Free State. Accordingly,

employees of public bodies are not subject to any obligation to provide

information to these persons. Any conflicting civil agreements are

ineffective.

What should I do?

On this point there was between my authority and the

Public authorities are allowed

own tasks and powers of intervention

State Department Unity; the same applies to the existence of confidentiality

are not transferred to third parties under

obligations on the part of the processor and his obligation to hand over all

a civil contract to be carried out

data at the latest after the end of the activity.

independently.

The involvement of third parties in the

official fulfillment of tasks is at best by

If external persons are commissioned in future cases - if personal data

way of and under the narrow conditions of

are (are to be) processed as part of the commission - the procedure of

- bound by instructions - order processing

the commissioned third party should be responsible

according to Art.

28 GDPR permitted.

based on these principles.

4.2.2 Use of Chatbots by Public

Authorities

ÿ Art. 6 and 28 GDPR

In the year under review there were inquiries from local authorities

for the first time, which are so-called for simple inquiries from citizens

te chatbots wanted to use or at least with the

have dealt with the question of deployment in more detail. First of all, a

chatbot is a neutral technology that analyzes simple questions asked in

writing or orally with the help of speech recognition software and from a

fun

dus of standardized answers a quick help for

should enable the questioner. In order to be able to operate such a chatbot

sensibly, it is usually necessary to

To collect and evaluate input from users during operation so that the

knowledge gained from this can be incorporated into the supplement,

expansion and improvement of the service offered. This processing can

be done automatically with a form of artificial intelligence, usually so-called

“machine learning”, or manually by human processors. In most of them

Machine Translated by Google

In some cases, however, a mechanical component will also be used. It is clear that both operation and data for the improvement of the system results in the processing of personal data and thus requires one or more legal bases. First of all, informed and transparent consent in clear language is required for the use of the chat bot. Further consent is required if user data is to be used for other purposes, for example to improve the service or measure usage behavior. This consent must be designed in such a way that the chatbot can also be used without processing for these purposes. Special cases of consent, such as that of children, for which the consent of the legal guardian is required, must be taken into account. Duration of storage and processing must be specified for all purposes and the rights of those affected must be guaranteed.

If particularly sensitive data (e.g Automated information from health authorities on Qua banee provisions) are processed, technical and organizational measures must be taken to effectively reduce the risks, for example by erasing or anonymizing data as quickly as possible, restricting access rights, encrypting databases or other suitable measures.

If such a service is used as part of order processing, the

commissioned service provider must be checked carefully.

In particular, it must be ensured that the service provider

only uses the processed data in

Processed as part of the order and not for our own purposes.

For public bodies, such a transfer of data for use due to the

legitimate interest of third parties is expressly prohibited.

Data processing "to improve the product" in favor of the

manufacturer must be clearly excluded. Likewise, the

processing must take place within the European Union. This

applies in particular to the sub-processors used

processor. It is not uncommon in practice that the processor is

What should I

do? Public bodies or by

these obligated contractors

must when deployed

by chatbots or similar

based in Europe, but uses a global content delivery network for

the delivery of individual components and thus the transmission

of usage data to a cloud with non-European data processing is

not effectively ruled out .

Techniques ensure that the

requirements of the GDPR are met.

4.2.3 Use of the Corona-Warn-App

(CWA) by public authorities

ÿ SächsCoronaNotVO

A university asked whether a contract for order processing was required for the use of the Corona-Warn-App (CWA) if this was used for access control of teaching and other events at the university within the framework of the applicable corona protection measures is used.

The answer to the question is in the negative to the extent that such a contract cannot be concluded at all, since the university does not process any data at all. The public body only creates the QR codes with the data of the respective event on the homepage of the Corona-Warn App, with the help of which users of the app can check in and thus meet contact recording according to the Saxon Corona Emergency Ordinance.

The Free State of Saxony was the first federal state to has standardized this data-saving system, which is based on the personal responsibility of the users, in the state's Corona Emergency Ordinance as a substitute for its own contact tracing.

If the manual contact recording is still offered in parallel or if you use your own systems in which contact details of visitors to events are recorded, you are responsible for ensuring that you meet the data protection requirements.

4.2.4 Video Interpretation

ÿ Article 28 GDPR

During the reporting period, my predecessor received a request from a local authority's data protection officer about the use of video interpreters. Video interpreters are used if interpreters are needed at short notice or if interpreters are not available, for example in a certain language.

He asked for an opinion as to whether the use of video interpreters was order processing within the meaning of Article 28 of the General Data Protection Regulation (GDPR). A department of the municipality, which repeatedly uses interpreters at short notice, takes the view that there is no order processing because this is a freelance activity.

In the field of the judiciary, video interpreting is used as Auf contract processing and is used in correctional facilities in coordination with my authority.

In my opinion, the use of video interpreters in the context of order processing is possible. Order processing occurs because the interpreter translates what is said into another language. It is different with an appraiser who makes his own assessment. However, the latter is not the case here.

The objection that interpreting is

is a freelance activity.

The requirements of Art. 28 GDPR must be observed.

If the company employs freelancers, there is a

subcontracting relationship that must also meet the

requirements of Art. 28 GDPR.

4.3 Security of processing

4.3.1 Use of LernSax

ÿ Art. 32 GDPR

In the 2020 activity report, my predecessor had commented on the

Activity report 2020: ÿ

consent-free use of the LernSax under "2.3.2 LernSax - the Saxon school

sdb.de/tb2020

cloud" (page 90f.). In a petition I was now informed that a

teacher would have sent a message to a student via LernSax saying that

she was rated 4.5 and cheated. This message was sent to the entire

class. The school, asked for a statement, admitted the

data breach. This results from a verse

the teacher. This had a message in LernSax

answered the student and did not notice that this message was sent by

her personally, but from the class group. The teacher's answer was then

automatically visible to the whole group and not just to the student.

Noticing this, she turned

Contact LernSax support immediately to have the message deleted.

Finally, she apologized in a conversation with the student and her

parents. Against this background, my authority has refrained from further

measures.

4.4 Data Breach Reporting

4.4.1 Increase in reported data breaches

ÿ Art. 28, 32, 34, 83 GDPR

According to Article 33 of the General Data Protection Regulation

(GDPR), those responsible are obliged, in the event of a breach of the

protection of personal data, to

as soon as possible within 72 hours of the injury becoming known

to report this to the supervisory authority, unless the violation of the

protection of personal data has occurred

Machine Translated by Google

not likely to pose a risk to rights and free

units of natural persons.

923 such reports were received in the reporting period. Compared to the

reporting period of the previous year (635 reports), this corresponds to an

increase of around

45 percent. This is again a significant increase in the

record data breach reports.

The following groups of cases were reported particularly frequently in the

reporting period:

wrong shipment

As in the reporting period of the previous year, incorrect dispatch is one

of the most common case groups of reported data protection violations

and accounts for around 35 percent of all reports. The causes of these

incidents are incorrect allocation of documents, faulty enveloping or simply

careless mistakes. As a rule, the incorrect shipment is reported to the

sender by the wrong recipient and the documents are destroyed or

returned, so that in

Illustration 1:

reports from

these cases mostly not of a high risk for the

data breaches

concerned is to be assumed.

1.000

900

800

923

700

600

500

635

400

450

300

200

100

227

0

202020192018

2021

Activity Report 2021

Open mailing list

A very important aspect of data protection is due diligence. This is often neglected, especially when sending e-mails to large groups of recipients. As a result, sending emails (e.g. newsletters) from recognizable email addresses in copy (Cc) mode rather than blind copy (Bcc) mode is still a reported data breach, typically based on plain un due to the sender's care. Even if Since the risk for those affected can often be assessed as low, such a data protection violation must be reported under Art. 33 GDPR.

lost in the mail

In addition to incorrect shipments due to the fault of the sender, numerous reports of the loss of postal items were again received. This also constitutes a reportable data protection breach pursuant to Art. 33 GDPR if the sender has been informed of the loss of the postal item, which is usually initiated by the specified recipient by finding out about the whereabouts of the expected postal item.

Loss of media

Thefts also occurred again during the reporting period or the loss of data carriers, some of which contain sensitive data. It is particularly annoying – because avoidable – that the data carriers were usually

unencrypted, so that attackers or finders had direct

access to the data. In order to keep the consequences as

low as possible, one of the mandatory technical and

organizational measures relating to data carriers is

encryption. Corresponding functions are already available

in common operating systems or freely accessible

Notes from the BSI on

Generating secure passwords:

ÿ sdb.de/tb2112

software. When encrypting, it is important to use a secure

password. In addition to encrypting the data carriers, they

must always be properly stored and transported,

and regular backups should always be performed to ensure data

availability.

Data backups are often kept on storage media or photo documentation

is created. This is particularly sensitive data in day-care centers or

medical practices, for example, so that it is usually lost if it is lost

a high risk and associated considerable damage

that may arise for those affected. The consequence of such a

data protection violation with a high risk for those affected is

then always that the person responsible, in addition to the report

according to Art. 33 GDPR also the data subjects according to Art. 34

GDPR has to notify.

Data Breaches by Processors

This year there were also frequent incidents in which contract processors were affected by a data protection incident, which had access to personal data as part of the contractual relationship. This is often the case when external companies maintain software, take on the billing of services from external companies or the printing and shipping is outsourced. The processor has no decision-making authority over the data and does not pursue his own business purpose with the data.

In the event of data protection incidents involving a processor, the processor is obliged under Art. 33 Para. 2 GDPR to report this immediately to the person responsible so that the person responsible can fulfill his obligation to report to the supervisory authority pursuant to Art. 33 Para. 1 GDPR or possibly even his obligation to notify under Art 34 (1) GDPR can be complied with at all.

My authority received a reportable incident from a service provider, at which Saxon company

were affected and named. Due to a misunderstanding by some of the affected companies, these companies, as the responsible persons, did not submit their own notification to my authority, so that the reporting requirement was only met in fol

ge our request was met.

cybercrime

Around a third of the reports of data protection breaches received in

2021 can be traced back to cybercrime. This unspecific term encompasses all actions/offences that are committed through the use of communication and information technology.

One of the most notable cybercrime incidents was the vulnerabilities in Microsoft Exchange servers. Numerous reports were received by my authority at the beginning of 2021. At the beginning of March 2021, Microsoft released security updates for these vulnerabilities. At the same time, the company announced that the vulnerability had existed for some time and was also being actively exploited. Thus, users had no guarantee that alone

any danger was averted by the immediate installation of security updates. In addition, it was necessary to check whether the exchange server had already been compromised.

preventive measures

Prevention and precaution are the right means to counteract a data protection violation and the associated risks for data subjects and the reporting obligation in accordance with Art. 33 GDPR. I recommend the following precautions:

• Secure data! The data of companies and organizations must be secured at all costs. These backups should not themselves be vulnerable to cyberattacks.

• Configure the firewall correctly! The firewall should only allow necessary data connections. An early warning system about unusually high data traffic can also help those responsible for the system to

avert damage.

• Observe the emergency plan! In the event of cyber

extortion or hacker attacks, an emergency plan should

be in place, which should be processed in an emergency.

This also includes a regulation as to when the IT administrator, internal

Machine Translated by Google

Data protection officers, the data protection supervisory

authority or the employees, company management

management and customers are to be informed.

• Reserve technology! An urgent recommendation is also to keep reserve

technology available. Investigators can do that

examine the attacked IT system forensically for as long as

necessary, while the company despite

cyber attack is quickly able to work again. •

Communicate early! Those responsible should inform the people or

departments affected quickly about the incident even if it is not

yet certain

whether and which personal data is affected.

• Continuing education! IT managers and all those who work in

Companies and organizations responsible for information security

require regular training.

In connection with the obligation to report data protection violations

according to Art. 33 GDPR, I would like to point out that all data protection

violations must be reported to me. This is only excluded if the data breach

is not likely to result in a risk

for the rights and freedoms of natural persons.

In addition, I would like to point out that in addition to the basic accountability according to Art. 5 Para. 2 DSGVO in particular to the existing for reporting cases Documentation obligation according to Art. 33 Para. 5 DSGVO as well as the possible obligation to inform the data subject a person according to Art. 34 GDPR.

As part of the obligation under Art. 32 GDPR, the person responsible must ensure that the necessary technical and organizational measures are implemented and checked regularly so that data protection violations are avoided as far as possible. Violations of Art. 32 GDPR would be, for example, security updates not installed, missing backups, missing encryption, but also missing measures to raise awareness among those involved.

Violations of protective measures according to Art. 32 GDPR as well as against formal requirements of reporting or notification according to Art. 33, 34 GDPR can be the subject of a fine according to Art. 83 para. 4 letter a GDPR. Therefore I recommend like this probably to protect the interests of those affected as well as the own economic interests of those responsible to check the precautions mentioned and keep them up to date to stand firm.

4.5 Data Protection Officer

4.5.1 Data Protection Officer as Information Security Officer

ÿ Art. 37 GDPR, SächsISichG

The Saxon Information Security Act (SächsISichG) of 2019 obliges government agencies to appoint an information security officer; sometimes even full-time. However, non-governmental public bodies, such as municipalities, should also make such an appointment. A smaller Saxon municipality approached my authority with the question of whether the data protection officer appointed under Art. 37 of the General Data Protection Regulation (GDPR) could also be considered for a corresponding appointment.

The appointment of various other officers in the same person as the data protection officer is fundamentally problematic. However, the information security officer should be viewed less critically, since information security and data protection usually run in parallel. This also applies to the fact that extensive collections of personal data are processed for information security in order to detect misuse.

Art. 32 GDPR also addresses the security of the processing tion and also in paragraph 1 letter c) expressly the availability. However, this is different if the information security officer also has implementation tasks, even with budget responsibility.

5 International Data Traffic

5.1 New Standard Contractual Clauses

ÿ Article 28 GDPR

As a consequence of the judgment of the European Court of
Justice of July 16, 2020 - C-311/18 - ("Schrems II"), the
European Commission has issued new standard contractual clauses.
Old standard contractual clauses may no longer be used for
new contracts. By December 27, 2022, old contracts based
on the previous standard contract clauses must be changed.
In addition, old contracts must be checked with regard to the
legal situation and legal practice in the third country and the
guaranteed level of protection.
The European Commission has issued an implementing
decision for the new standard contractual clauses,
Implementing decision (EU) 2021/914 of the EU Commission
EUR-Lex:
of July 4, 2021, file number C (2021) 3972, Official Journal EU
ÿ sdb.de/tb2113
No. L 199/31 of June 7, 2021.
The new standard contractual clauses take into account the
usual data transfers to controllers in third countries and the
use of processors and sub-processors. However, it is still
necessary to examine the legal situation and legal practice in
the third country and, if necessary, to take additional protective
measures. If the level of protection cannot be guaranteed, the
What should I do?
data should not be transferred to the third country.
The new standard contract clauses

are to be used unchanged, if

necessary as part of a contract.

If order processing contracts are used, the new standard

Only then does freedom of approval

contractual clauses take into account the requirements of

apply.

Article 28 of the General Data Protection Regulation (GDPR).

6 Saxon Data Protection Officer

6.1 Jurisdiction

and Requirements for Complaints

6.1.1 Model projects according

to the Saxon Corona Protection Ordinance

ÿ §§ 8g, 36 SächsCoronaSchVO; Art. 51 Para. 1 GDPR, Art. 57 GDPR

After the Free State of Saxony since December 2020 in the

lockdown and social public life was only possible to a

limited extent, the Saxon Corona Protection Ordinance

(SächsCoronaSchVO) of March 5, 2021 was intended to

allow relaxation.

Idea of model projects

Among other things, so-called model projects should

contribute to this. According to § 8g of the

SächsCoronaSchVO of March 5, 2021, the responsible

district or the responsible independent city for the area

or a part of a municipality could allow deviations from

the restrictive regulations of the SächsCoronaSchVO in

the context of model projects. According to the ordinance,

these model projects should serve to investigate and

develop the course of infection, non-discriminatory

testing of corona test concepts and digital systems for

data protection-compliant processing of personal data

and their transmission to the health department for shortterm and complete contact tracing.

142 |

Chapter 6

Machine Translated by Google

Initially, the approval of the model projects by the responsible districts

and urban districts required the approval of my authority. In later

versions of the

SächsCoronaSchVO should initially be agreed

and later only the behavior with my office to be established. In addition

to the participation of my authority, the competent approval authority,

i.e. the district or the urban district, also had to involve the supreme

state health authority in this multi-stage administrative procedure. These

participants were also changed in the course of the adjustments to the

SächsCoronaSchVO.

For example, according to the SächsCoronaSchVO of March 29, 2021

(in the consolidated version of April 16, 2021), the Saxon State Ministry

for Social Affairs and

Social cohesion and the at the Staatsmi

nister for culture and tourism in the state ministry for

Science, culture and tourism committee to be involved.

Difficulties in procedures and projects

This regulation posed major challenges for my authority, particularly in terms of personnel, but also in relation to the non-coordinated procedure between the different parties involved in the procedure, because of the unclear application requirements, but also in relation to the diversity of the projects, which required a comprehensive and careful individual assessment required. My office had to deal with a flood of applications and large numbers of cases.

The restrictions on commercial operations due to the Corona measures, such as the closure of the hotel and

Hospitality establishments and restaurants and also the ban on

According to my observation, events led to the pilot projects being used as an instrument for circumventing the protective measures or opening them up and only secondarily for testing digital systems for data protection-compliant processing of personal data

should be.

This is evidenced by a large number of model project applications

Associations, companies and organizers, in particular

for example from the event area, which is severely affected by restrictions, as well as the planned use of digital systems, which are often far removed from data protection standards, should be developed and put into operation at short notice. Necessary procedural descriptions

that describe the data processing processes were a regular feature –
in particular who exactly collects which data for what purpose and time,
who forwards data for what purpose, when the data will be deleted, how
the persons concerned are informed, which
technical and organizational measures have been taken to protect the
data - non-existent or insufficient, sometimes rudimentary.

Structural flaws in legislation

Due to the lack of participation of my authority in the
Introduction of this regulation and the short notice with which this
regulation came into force, neither the application requirements nor the
procedure between the participating approval authorities were
coordinated and procedural
structured.

My authority takes the view that the
Question of the implementation of the model projects primarily in
protection law and not data protection law
were physical matters that would have to be decided by the relevant
health or licensing authority. Even if the model projects regularly had
data protection problems, the General Data Protection Regulation
(GDPR) does not allow my authority to be involved in this form. To what
extent such a task assignment to my authority by the Saxon legislator
conforms to European law, cf. Art. 51 Para. 1, Art. 57 GDPR, should
have been examined in depth by the Saxon legislator.

The tasks of my authority are conclusively regulated by the General Data Protection Regulation or formal law. Nevertheless, my authority checked the model project applications.

The regulations of the SächsCoronaSchVO for the model

Projects regarding the participation of my authority were not compatible with the system or not coordinated with the European regulation, since my authority is locally only authorized to supervise the responsible persons and processors located in Saxony. There is also no factual responsibility of my authority towards model project applicants who are not themselves data-processing bodies. These are not obligated to my authority and cannot be imposed or controlled. In addition, there is a possible collision of supervisory responsibilities with specific supervisory authorities, for example in the case of church authorities, for which my authority is also not responsible. In any case, the implications were not taken into account by the legislator, but had become apparent very quickly in the processing of the model project applications and had a significant impact on the procedure, particularly with regard to the involvement of other data protection supervisory authorities and the processing time. It also remained to be noted that, in addition to the tasks assigned under European law for participation in formal, tiered administrative procedures

perso

What should I do?

As far as the Saxon Ge

nally and factually the resources in my authority were missing.

If the legislator or legislator intends

to test automated processes in

summary

projects, the Saxon data protection

officer can be notified of this. In this

way one can also

At the end of April 2021, the Infection Protection Act was amended. Due

to the restrictions specified therein (so-called "federal emergency brake"),

the realization of the model projects was anyway due to the high incidence

participation take place. A data

protection and

information security law

quality more automated

figures

no longer feasible. After the federal government expires

emergency brake could only be carried out in isolated model projects

due to the problems described above.

Procedures, on the other hand, are

primarily to be safeguarded by those

responsible for the project.

In my opinion, due to the circumstances described above, this was done

with the model projects

linked target missed. This affected both the development of

digital systems for the data protection-compliant processing of

personal data and their transmission to the health department

for short-term and complete contact tracing.

6.1.2 Data processing by a youth

welfare office as part of family court

proceedings

ÿ GDPR, SGB VIII

The procedure for the temporary admission and accommodation

of a child or young person in an emergency situation by the

youth welfare office is regulated in Section 42 of the Eighth

Book of the Social Code (SGB VIII). If the caregivers or legal

guardians object to such taking into care or if they cannot be

reached, the youth welfare office has a decision from the family

court on the necessary measures for the well-being of the child

or young person

bring about.

§ 42 SGB VIII also regulates the possibility of temporarily

accommodating a child/adolescent with a suitable person.

Participation in proceedings before the family court according

to § 50 SGB VIII is one of the tasks of child and youth welfare

according to § 2 paragraph 3 and 6 SGB VIII. In this respect,

the Youth Welfare Office is entitled to participate in proceedings

of the family court to decide whether a child is to be taken into

care, i.e. also to the question of who can be regarded as a

suitable person for an intended taking into care in an individual case.

The youth welfare office is therefore entitled to issue a specific,

personal opinion on the person in question to the family court

with regard to the question of suitability. A consent requirement

of

data subject is not required for this.

What specific technical requirements are required for taking a

suitable person into care and whether these are specific and

factual in relation to their person

have been correctly assessed is a technical legal issue,

but not a data protection issue, so that this is not subject

to review by my authority.

6.1.3 Violation of the imprint obligation

ÿ Section 1, paragraph 2, sentences 2 and 3 of the Saxon Law on the

Implementation of the State Media Treaty and the State Broadcasting Contribution

Treaty, Section 106 MStV

Complaints I receive again and again contain (also) a

reference to a missing, incomplete or incorrect imprint on

a website. In one case, a homeowner approached me

and explained that it was wrong on the Facebook fan

page of a business

used the address of his apartment building as a business address

be specified. The homeowner saw the danger that

potential tenants could become aware of this and be put

off by it. As it turned out, the owner of the company had

his private apartment in the apartment building until a few

years ago.

First of all, the homeowner requested my authority to intervene on the basis of data protection law, which my predecessor had to refuse, citing the non-applicability of the data protection regulations. As a result, the homeowner asserted a breach of the imprint obligation because of the incorrect address given and wanted to know where to turn in this regard.

Responsibility reorganized

My predecessor had already dealt with the imprint obligation and the question of the competent authority in his activity report for the reporting period from April 1, 2017 to December 31, 2018 (6.1.2, page 230f.). At that time, he referred possible violations of the provider identification obligation to the Saxony State Directorate.

In the meantime, however, the Saxon legislature has newly regulated the question of jurisdiction for all matters relating to The one on which the statements at that time were based

The Interstate Broadcasting Treaty was replaced by the Interstate Media Treaty in November 2020. According to this, the responsibility for nationwide offers lies with the state media authority of the respective federal state (§ 106 Media State Treaty). In the Free State of Saxony, the Saxon State Authority for Private Broadcasting and New Media, FerdinandLassalle-Strasse 21, 04109 Leipzig, as the state media authority, is the

competent supervisory and administrative authority for administrative

What should I do?

For compliance with the imprint

offenses (Section 1 (2) sentences 2 and 3 of the Saxon Law for the

implementation of the media state treaty and the broadcasting contribution

obligation for telemedia, in

Saxony the Saxon country

state treaty).

agency for private broadcasting and

new media

and responsible as a fine

authority. The Saxon Data Protection

Whether or not there is a fine in the case described cannot be assessed

due to the lack of competence of my authority. However, the homeowner

Officer, on the other hand, does not

concerned is probably primarily concerned with the fact that his rental

check the provider identification

property is not associated with a commercial operation, which could have

obligation, but is responsible for

reduced the attractiveness of his housing offer.

fulfilling the information obligation in

accordance with Articles 13 and 14

GDPR.

6.1.4 Private enforcement and

damages for data breaches

ÿ §§ 3, 3a, 8 UWG; Art. 12ff., 15, 20, 57, 82 GDPR

Behavior in accordance with data protection (data protection
compliance) is a central obligation of every data protection company
responsible. This knows the circumstances of the concrete
Data processing at its best and has a direct influence on it. This is the
most important level of enforcement.
The legal community is dependent on compliance by those responsible
in the area, breadth and depth.
Accordingly, the legal system provides a wide range of enforcement
mechanisms. The incentives generated in this way for those responsible
to comply with the data protection rules are decisive. It is of practical
importance that the sanctions for data protection
breaches must outweigh the additional gains that the controller derives
from ignoring
of its data protection obligations.

Machine Translated by Google
Violations of data protection law are therefore subject to severe sanctions
– fines of up to 20 million
n euros or 4 percent of the worldwide annual turnover and
up to three years imprisonment.
Parallel to such sovereign sanction options, those affected by the illegal
data processing have claims for compensation for their material and
immaterial damage, Art. 82 General Data Protection Regulation (GDPR).
Irrespective of damage and sanctions, there are also direct claims by
the person concerned and – with regard to data protection standards,

which at the same time represent a market conduct regulation within the meaning of Section 3a of the German Act Against Unfair Competition (UWG) – also by competitors and others authorized to enforce rights.

In some cases, the person concerned's own first steps are a prerequisite for official proceedings.

In addition, private lawmaking has various advantages, not least in terms of speed, range of enforcement of claims and broad effect on compliance across the board. In this respect, private enforcement complements official enforcement.

In related areas of law, private enforcement of rights is of substantial and often increasing importance. In data protection law, it is already becoming apparent today that

the GDPR will become the basis for a similar development should. In this way the means to the through multiply regulation of data protection law, which in turn benefits the protection purposes of data protection law.

(Provable) assertion of the rights of those affected as a procedural precondition

Those affected often ask me to assert their rights against the actual person responsible or to request their corresponding claims directly to fill.

However, the GDPR provides rights for the majority of those affected under Art. 12ff. first assert the claims directly against

the person responsible; this applies in particular to the right to information and a copy, Art. 15, 20 GDPR. Accordingly, I can usually only take action if the person responsible does not (or at least plausibly prove) respond to corresponding requests from the data subject (or does not do so in a timely manner).

In a large number of such complaints, the object of the complaint is resolved when the person concerned is informed of the need to (provably) assert their rights against the person responsible and this caught up.

False denial by a person responsible, ent

Having received speaking inquiries, on the other hand, constitutes an independent serious data protection violation punishable by a fine or penalty, in addition to that regularly also existing failure to meet deadlines.

The false assertion of facts to the supervisory authority attacks the supervision at its roots.

Accordingly, such (suspected) cases would be mine special attention and would give special prosecution enjoy priority.

Insofar as the complaint raises the suspicion in relation to a person responsible that he or she leaves inquiries received unanswered or withholds them, I am authorized to carry out appropriate searches.

In the case of (deliberate) false allegations to the authorities by

(allegedly) affected persons or whistleblowers, there is regularly

false suspicion, which is punishable under Section 164 of the

Criminal Code. Incorrect information provided by the person

responsible is a violation of the cooperation requirement and the

obligation to provide information, which is subject to a fine, and

can be punishable under Section 42 of the Federal Data

Protection Act (BDSG), among other things. If the suspicion is

substantiated, the importance of truthful information to the

supervisory authority for the supervisory authority requires appropriate criminal p

cause.

Advantages of private law enforcement

All individual rights under data protection law

are directly entitled to the person concerned, i.e. can directly

be asserted before the civil courts. Besides

are directly subordinate to competitors, among others

claims against those responsible who compete against the market

behavior regulations of the

violate data protection law.

Such private legal enforcement has a number of advantages.

This is particularly evident in areas in which the authority of the authorities

and the scope of data protection law do not or only partially address the

problematic facts

wisely covered.

This is supported in particular by the sometimes significantly faster enforcement of rights through civil legal remedies such as temporary orders and warnings for private enforcement of rights.

Also, my authority is usually further away from the place suspected data protection violations removed as the data subject and the locally competent civil courts, which determine the facts and possible solutions

can lighten.

A data subject affected by data protection violations is able to sue the controller before the court responsible for his or her own place of residence without a decision from the possibly reticent supervisory authority at the controller's headquarters

to wait and see.

Finally, the reliable judicial finding,

that for certain data breaches a damage

replacement is owed, appropriate practices promptly and

effective also in width. Although an ent

speaking judgment only between the parties. However, the scope of a well-reasoned damages judgment is not limited to the parties or the jurisdiction of the

sentencing court. Rather, such a

Radiation effects unfold, with official

decisions can only be made to a limited extent. Because the limited

resources of the supervisory authorities are well known and sometimes influence location decisions from data processing companies.

In addition, judgments on damages have the advantage that the injured party receives direct compensation for the damage suffered, while official decisions for the person concerned with regard to past violations can at best be immaterial satisfaction and the basis for a claim for damages.

Example: video surveillance by neighbors

Complaints about video surveillance from neighbors often fail because a data protection violation cannot be determined. Because the application of data protection laws requires specific unjustified processing of personal data. The limits of permissible video surveillance beyond one's own property under data protection law are narrow; monitoring of the neighbor is not permitted in this respect (cf. also 2.2.52.2.5).

However, my agency's investigative powers are limited in relation to residential premises. Especially in the case of remote-controlled video cameras and so-called dome cameras, videography that has been checked by me and is permissible under data protection law can also be changed without any special effort in such a way that data protection violations take place after the recording field has been changed. After all, I'm not responsible for dummy cameras due to a lack of data processing.

On the other hand, a claim for injunctive relief under neighborhood law can also exist if third parties only objectively have a serious

reason to fear surveillance by surveillance cameras (“surveillance pressure”). This also includes dummies in particular.

It is true that the precise individual case must be taken into account. In administrative and administrative offense proceedings, however, in Kern the authority the evidence of a data protection violation to lead. In contrast, in the neighborhood lawsuit, the

the one who uses the camera or dummy camera is heavily burdened with the burden of proof and presentation.

The established neighborhood law requirements of the civil courts are stringent in this respect:

“The fear of being monitored by existing surveillance devices is justified if it appears comprehensible and understandable on the basis of specific circumstances, for example with regard to a escalating dispute between neighbors or due to circumstances that objectively arouse suspicion. If such circumstances exist, the personal rights of the (supposedly) monitored person may be impaired simply because of the suspicious situation. However, the mere hypothetical possibility of surveillance by video cameras and similar surveillance devices does not affect the general personal rights of those who could be affected. Therefore, the installation of a surveillance system on

private property is not unlawful if it is objectively certain
that public and third-party private areas are not covered,
if such a detection is only possible through an externally
perceptible technical change to the system and if other
rights are also granted third parties will not be adversely
affected.”

Federal Court of Justice (BGH), judgment of March 16, 2010 - VI ZR 176/09;
cf. also District Court of Frankenthal (Palatinate), judgment of December 16,
2020 - 2 S 195/19

“When installing video surveillance systems on private
property, it must be ensured that neither adjacent public
areas nor neighboring private properties are captured by
the cameras. Something else only applies in individual
cases if, when weighing up personal rights, it can be
assumed that the operator of the system has an overriding
interest.”

Koblenz District Court, decision of September 5th, 2019 - 13 S 17/19

The person concerned (possibly not under data protection law)
can follow these established lines of jurisdiction
Neighbor obtain an immediately enforceable title from the
locally competent court within a few days in the preliminary
injunction proceedings and, if necessary, have it enforced
promptly with the support of the bailiff, without

it would depend on data protection violations and their proof.

On the other hand, if those affected choose to complain to my authority, the – more extensively required – factual determination is often significantly more time-consuming. If no data protection violation can be determined, private enforcement of the law after official proceedings have been carried out remains the only option for neighbors who object to cameras or cameras want to ward off dummies and the monitoring pressure they emanate.

Ultimately, in view of the far-reaching legal requirements for videography in the neighborhood, a legal dispute will often be unnecessary. Addressing the videotaping neighbor directly can help prevent the (further) deterioration in the relationship between the neighbors, which can result from the complaint to the supervisory authority

authorities or a court case. Besides

is for Saxon facts in particular on the Ver

drive before the magistrate to point out that for such neighborhood disputes offers a low-threshold and consensual conflict resolution option.

Example: data protection in the press area

and media law

My powers of supervision and intervention in the field of journalistic activities are defined by Section 11a Clause 4 of the Saxon Press Act (SächsPresseG) in conjunction with Art. 85 GDPR significantly restricted.

Accordingly, I am not authorized to monitor companies and
auxiliary companies of the press in terms of data protection,
insofar as they process personal data for journalistic or literary
purposes. Because of the importance of media privilege for
public discourse and

the functioning of democracy, this exception is to be interpreted broadly
and is fundamentally independent of journalistic quality or independence.
That standard also severely restricts the rights of data subjects under
the GDPR. However, there are a number of rights under press and
media law that give those affected some related rights, albeit to a limited
extent in view of the importance of freedom of the press, information and
opinion.
Claims under press and media law for injunctive relief, counterstatement,
revocation and correction of a specific report, as well as for damages,
have similar effects to the corresponding claims under data protection
law.
However, they are completely independent of data protection law and
can only be enforced privately. Although this is not an enforcement of
data protection law, these claims serve closely related protective
purposes and fill a gap in protection created by the exception rule.
Example: Unfair competition by
data breaches
Violations of data protection law can constitute unfair acts in competition.

Competitors, relevant associations with legal capacity, qualified
institutions within the meaning of the Injunctive Relief Act and the
Chambers of Industry/Commerce/Chambers of Crafts can, in principle,
take action independently and in their own right against the person
responsible for such legal violations, §§ 3, 3a,
8 UWG. A data protection self-affected is
not mandatory.
In this respect, it is disputed whether and which data protection
legal rules represent a so-called market conduct regulation and justify
corresponding claims for injunctive relief and claims for damages under
fair competition law. However, the courts have established a fairly farreaching line of jurisprudence here, which is largely
based on the old

Legal situation developed judicature builds. For example, a number of
higher courts have confirmed corresponding claims (cf. OLG Hamburg,
judgment of October 25th, 2018 - 3 U 66/17; OLG Munich, judgment of
March 21st, 2019 - 6 U 3377/18; OLG Naumburg, judgments of November
7th, .2019 - 9 U 6/19 and 9 U 39/18; OLG Stuttgart, judgment of February
27th, 2020 - 2 U 257/19).
Under the old legal situation, the European Court of Justice (ECJ) had
answered the previous question of the so-called blocking effect of legal
remedies under data protection law in the negative (ECJ, judgment of
July 29, 2019, case no. C-40/17). In the reporting period, the Federal
Court of Justice again submitted this question to the ECJ under the new

legal situation (BGH, decision of May 28, 2020 - I ZR 186/17; registered
at the ECJ under C-319/20, Facebook Ireland Limited vs. Bundesverband
der
Consumer centers and consumer associations - Consumption
Central Federal Association eV). Accordingly, a binding supreme court
decision is pending, which could eliminate the existing uncertainty.
The fair enforcement of data protection regulations without self-affecting
has a number of significant advantages over official action. However,
measures and sanctions by the data protection supervisory authorities
can certainly be based on corresponding findings.
In this way, competitors and other claimants make additional resources
available to monitor market-related compliance with data protection rules
without being affected by data protection law themselves, and
such as data protection.
In addition, market participants are sometimes more familiar with the
specific data protection problems in their industry than they may not have
been before
involved supervisory authorities.
After all, the usual form of enforcement in this area is the warning, which
can usually lead to the termination of data protection-violating practices
within a few days, which is only rarely successful in official proceedings.
Even if the complete development of private law enforcement in this area
still depends on a – foreseeable –

final clarification of some legal questions, it can already be stated today that it is worthwhile full complement of data protection law enforcement instruments.

Broad effect and damages for data breaches

The damage resulting from data protection violations is usually of an immaterial nature. German courts are generally very reluctant to award damages for immaterial damage. However, the GDPR has introduced a completely new legal basis with Art. 82, whose effectiveness must of course first develop.

Under Union law, the damage suffered must be fully and effectively compensated (Recital 146 GDPR). In this respect, an extensively developed Union law judicature on the law on damages, in particular after antitrust law violations.

Because the member states - including the courts dealing with claims for damages - are obliged, according to the idea of Art. 4 Para. 2020 – 13 Ca 1046/20).

After initial hesitation, German courts have increasingly developed a judicature whose awarded damages sometimes expressly state “dissuasive we kung” should have. On the other hand, compensation in money is sometimes rejected if intentional data breaches of protection have caused not inconsiderable damage.

This contradiction of EU law requirements and German judicial tradition is illustrated by a data protection-related decision of the Federal Constitutional Court: A district court had rejected the claim for damages of a person affected by an illegal advertising e-mail: Here there was only a minor impairment that could not justify a claim for damages . The Federal Constitutional Court overturned this decision because

District Court should not simply assume that there is a threshold of significance that has not been specified anywhere. Before the claim for damages is rejected, the underlying question of interpretation must therefore be submitted to the European Court of Justice (Federal Constitutional Court, decision of January 14, 2021 - 1 BvR 28531/19).

Sometimes it is said that those responsible would through the obligation to replace the immaterial damage caused excessively and beyond concrete reproaches. This represents an abstract danger that repeatedly brought up by interested parties. However, such a disproportionality is not apparent from specific judgments and would also be in contrast to the basic characteristics and other damage compensation weightings of German courts. Rather, the controller who has complied with his duty

of care and documentation should be able to exculpate himself without further ado, Art. 82 (3) GDPR.

Finally, when looking at the incentives to act, fines, claims for damages and damage to reputation multiplied by the probability of detection, sanctions and conviction represent the “costs” of a breach. As long as these costs are lower than the costs of data protection compliance, it’s business as usual economically rational to undertake suboptimal compliance efforts. This is especially true if these "costs" only threaten after the tenure of those responsible within the company, while the corresponding bonuses are there to be realised.

Due to their capacity, the data protection authorities can only impose fines on a fraction of the violations that require sanctions. Against this background, imposing full and effective compensation for the (immaterial) damage caused in this way on those responsible for data protection violations appears urgently necessary in order to provide sufficient incentives for appropriate care when processing personal data.

The obligation to pay damages also has a direct effect of attracting attention: because the person responsible must be aware of having to specifically compensate for damage that arises from the realization of the

risk caused by data processing. Only through an effective and complete
obligation to compensate is the risk assessment under data protection
law not only abstract, but is in reasonable proportion to the resulting ge
put those affected at risk.

A large number of judgments have already been passed across the
country in which the data subject has been awarded not inconsiderable
amounts of compensation for data protection violations. The subject of
the legal infringement that triggered liability was, for example, the
unauthorized disclosure of (sometimes incorrect) personal data to third
parties or their publication, the refusal or late provision of information
required under data protection law.

On the other hand, courts have rejected corresponding claims because
no damage was incurred or demonstrated, it was based on a substantiated
explanation or proof of a data protection violation, its purchase
sality or fault of the person responsible was missing.

The requirement of substantial damage, on which not a few dismissive
judgments are based, is currently subject to an assessment by the ECJ
(see above).

It is true that the person concerned sometimes finds it difficult to access the data
breach of protection, the resulting damage and the
to prove causality between violation and damage. Al
However, Art. 82 (3) GDPR establishes a presumption of fault on the part
of the person responsible, de
ren range is disputed. In addition, it is currently subject to clarification by
the highest court as to the effects of the general accountability of Art. 5
Para. 2, 24 Para ; Appeals are pending at the Federal Court of Justice).

I hope for those affected that clarification will soon be brought about in their favor.

Companies often have a considerable interest in fending off claims for damages in order to prevent those affected from asserting their rights. Accordingly, highly qualified lawyers act on the side of those responsible in court, whose cost-intensive work can be explained solely by the interest in avoiding precedent decisions. On the side of those affected, litigation financiers and specialized consumer lawyers are hesitant to observe, which is certainly also the case in the based on the reluctance of the German courts to award compensation for non-pecuniary damage.

Overall, a new area of law is developing with damages for data protection violations, which has considerable potential to offer decentralized incentives for compliance with data protection law. This is to be welcomed unreservedly, as it supports the supervisory authorities in their goals of strengthening data protection.

Effective clarification of open fundamental questions by the European Court of Justice

However, in order to make the protection of data subjects effective through claims for damages, some basic questions still need to be clarified. A comparison with the similar

developments in antitrust law suggests that the effectiveness of

the claims for damages under Art.

82 GDPR will only meet the requirements of the GDPR and

Union law after decades of judicial clarification. A fundamental

lesson from this and related areas is that in areas determined

by Union law

Questions only the European Court of Justice can bring legal

clarity. A corresponding submission offers the first instance

court the possibility, in accordance with Art. 267 of the Treaty

on the Functioning of the European Union (TFEU), to deal with

questions of data protection and damage compensation law in

a binding, relatively inexpensive and timely manner

to clarify. A variety of both German dishes

as well as courts of other member states of the EU have

benefited from this obligation or possibility of submission in the area of

Data protection compensation law already use ge

might. Based on these procedures is already the binding

clarification of many open legal questions in the near future

expect.

Right of referral and duty of referral of German courts

Preliminary rulings by the European Court of Justice lead directly to legal

clarity for all legal practitioners within the scope of the GDPR. In Germany,

open legal issues have so far been clarified primarily in lengthy processes

by the courts. In fact, this often leads to the long-term effect of parallel,
often contradictory, lower and higher court decision-making lines with
corresponding legal uncertainties,
process risks and other problems. The Federal Constitution
On the other hand, the Supreme Court has expressly pointed out, also for
the area of the GDPR, that in particular the claim for monetary compensation
for data protection violations has not been fully clarified in the case law of
the Court of Justice of the European Union and that the relevant specialist
courts have a corresponding obligation to refer, specifically the Goslar
District Court (Federal Constitutional Court, decision of January 14, 2021 1 BvR 2853/19).
Many courts have already used this option in data protection law, so that
a large number of preliminary rulings, some of which overlap in terms of
content, are pending in Luxembourg. For example, the Saarbrücken
Regional Court and the Austrian Supreme Court clarify the question of
whether claims for compensation for imma
material damage from data protection violations is a minimum
threshold or demonstrable damage
(Saarbrücken Regional Court decision of November 22, 2021 - 5 O 151/19
= ECJ C-741/21 and Supreme Court of the Republic of Austria, decision of
April 15, 2021 - 6 Ob 35/21x = ECJ C-154/21). In contrast, many other
German (upper) courts have ruled without regard to the special
nationalities and the autonomy of Union law German law
Common principles applied, and thus de facto legal protection

made difficult or even impossible. Against this background, the Federal Constitutional Court is a reminder of the duty of courts of last instance to make a submission, and the possibility of making a submission for all courts, including the local and regional courts, is emphasized.

The Saxon Data Protection Commissioner urges the responsible courts to use the opportunity to refer matters to the European Court of Justice in cases of doubt and thus contribute to increasing legal clarity. As a result, and by suspending proceedings until the ECJ has made a decision in referral proceedings with the same problem, unnecessary stages of appeal and many other processes can be avoided.

Last but not least, the legal clarity that can be achieved in this way can also Make data protection compliance much easier for all legal users, including controllers.

Advisory mandate of the Saxon data protection officer and broad impact

My authority is neither responsible for the assessment of data protection claims for damages nor claims for injunctive relief under neighbour, press or fair competition law.

However, as part of my advisory and clarification mandate under Article 57 Paragraph 1 Letter b, e, i, v GDPR, I am obliged to inform those affected, those responsible and the public about data protection and to monitor the corresponding developments.

What should I do?

Direct enforcement of

However, through specific or general information on the

Data protection law can

possibilities of private legal enforcement, external resources,

Have a number of advantages,

such as those affected and those responsible, can

especially for those affected.

For some rights sees that

Data protection law already one

primary obligation of the person

concerned to assert this directly

Appropriate consultants and competent civil courts can also be

used to enforce data protection law

be made.

It is not just in the areas listed as examples that individuals can

against the person responsible.

enforce their rights, if necessary with the support of relevant

In the neighboring law are civil

interest groups such as consumer advice centres, but also in the

procedural means sometimes much

sharper and more effective than

regulatory investigative and remedial

Participate in clarifying open questions and eliminate data protection

powers.

violations effectively and sustainably.

Especially in case constellations in which there is a broad effect

me practices are not privacy compliant while the

competent supervisory authority remains inactive, private enforcement is

recommended as a more effective means of helping data protection law

to apply in practice. This data protection compliance, in turn, is a central

goal of my work.

6.2 Figures and data

on the activities in 2021

6.2.1 Overview of the main areas of work

As in the previous reporting period, my department again recorded the

largest number of complaints and requests for advice – around 45 percent

altogether.

Furthermore, formed the cooperation with the German

regulators a priority. The lively exchange on data protection topics

continues, as does the increase in reports of data protection violations in

Figure 2:

Main areas of work

accordance with Article 33 of the General Data Protection Regulation.

according to the number of processes

Press

inquiries 1%

administrative

offenses 3%

EU/International

5%

other 7%

Complaints

24%

General administration

7%

Cooperation

with German

regulatory authorities

15%

reports from

Data breaches 17%

Consultations 21%

6.2.2 Complaints and Notices

The number of complaints in the reporting period was at the high level

of the previous year. Since the General Data Protection Regulation

came into effect in 2018, the number of complaints and reports received

each year has more than doubled.

While submissions in the public sector fell in 2021, they increased in

the non-public sector compared to 2020.

1.400

1.279

1.254

1.247

1.176

1.200

1.000

910

819

770

800

744

597

600

503

376

400

484

387

357

221

200

0

20202019201820172021

Number of complaints to telemedia

Figure 3:

complaints and notices

public area

non-public area

In this reporting period, too, there was a consistently high volume of

complaints in the field of telemedia. A total of over 80 complaints were received, most of which were justified. Most of the complaints were total complaints directed against Saxon website operators who had integrated cookies and tracking elements into their websites without consent or who transmit visitor data to third countries such as the USA. Far fewer complaints were filed in 2021 due to a lack of encryption on websites; here it can be assumed that the majority of website operators meanwhile uses reliable transport encryption. The

Despite the efforts to automate it that started last year (see TB 2020; 4.1.1 Testing tools for websites and requirements for website operators, page 115f.), the processing of complaints is still laborious in terms of

preparation and the procedure with the respective companies responsible. In advance, all data processing taking place on a website (inclusion of third-party resources, cookies and other technologies) as well as the website's data protection declaration must be analyzed and evaluated, which is often very time-consuming due to the sheer number of technologies used. It is not uncommon for more than 20 cookies to be set when the home page of an individual website is called up and for connections to up to 40 third-party servers to take place. which receive all visitor data. In the process of

Those responsible are then often provided with extensive documents such as contract data processing contracts and other agreements, which in turn have to be evaluated. Those affected are regularly informed about the status of the process and can contact my authority at any time if they have any questions.

6.2.3 Consultations

The digitization of almost all areas of life continues. Consequently, more and more personal
data processed. What is allowed here and how the data
citizens are to be protected was a frequent topic in talks with those responsible in 2021. Overall, the number of consultations rose by more than 9 percent to 1,112 compared to the previous reporting period. That was almost as many as in 2018, when the Da
General Data Protection Regulation came into effect. The increase is due to information provided to both the public and the non-public sector. Many inquiries were related to the coronavirus pandemic and are also listed as examples in this activity report (see 1.1, 2.2.10, 2.4.1).

1.200

1.133

1.112

1.019

1.000

884

834

800

687

608

600

446

446

368

368

400

240

228

185

200

62

0

2020201920182017 2021

Figure 4:

consultations

public area

6.2.4 Data Breaches

ÿ Art. 33 GDPR

non-public area

The number of reports of data breaches pursuant to Art. 33

consultations total

of the General Data Protection Regulation has increased

steadily since the General Data Protection Regulation

came into force on May 25, 2018. In addition to the

registration, the reports must be evaluated and, if necessary,

categorized for supervisory follow-up work. Article 4.4.1

provides an overview of the content-related processes.

6.2.5 Cooperation with European

supervisory authorities - Internal

Market Information System

ÿ Art. 56, 60, 61, 64 GDPR; Regulation (EU) 1024/2012

The data protection supervisory authorities in the European

Union coordinate their Zu in cross-border cases

cooperation according to Articles 60 to 67 of data protection

Basic Regulation through the so-called Internal Market

Information System (IMI).

It is a web-based network for

exchange of information and for cooperation

public bodies, which is provided by the Commission of the European

Activity report 2020: ÿ

sdb.de/tb2020

Union (see also Activity Report 2020, Item 6.2.5, page 144). Details of

this administrative cooperation are set out in Regulation (EU) No.

1024/2012 (IMI Regulation).

In the IMI, information about the procedures set up there, the so-called

IMI notifications, is also sent to me every day. I get between 10 and 20 such messages every day. I check whether I am the leading supervisory authority or just (co-)affected, and - if I am the supervisory authority affected - whether
I am involved in proceedings of other supervisory authorities on the subject stand or would like to comment on decisions. I will also be informed about how other supervisory authorities are involved
handle certain cases.
A total of 2,367 procedures were discontinued in the IMI system in 2021 with the participation of German (lead or only affected) supervisory authorities. Of these, 128 were reinstated (statistical information from November 4th, 2021).
I, too, was involved in a variety of procedures as well
ne supervisory authority involved. As lead supervisor
authority I have two procedures in the reporting period
taken because the respective companies have their main office in Saxony. Saxony is in six
procedure in charge. I have a case to the pen
leading supervisory authority of another member state in a procedure pursuant to Art. 56 GDPR.
Since July 2021, the German supervisory authorities have also been using it the IMI module "Internal Written Procedure" (IWP) for their internal coordination in written procedures of the European Data Protection Board (EDPB). In this way, they create common positions in accordance with Section 18 of the Federal Data Protection Act (BDSG). In this context, among other things, I gave my vote for statements by the EDPB

on binding internal regulations of companies

("Binding Corporate Rules"), on requirements for the accreditation of

certification bodies (Art. 64 Para. 1 Sentence 2 Letter c of the General

Data Protection Regulation) or for Ant

Written letters to various institutions of the European Union. I assume

that in future the number of complaints from data subjects in the European

Union and also in Saxony and thus also the number of

cross-border procedures in IMI will continue to increase.

6.2.6 Register of Designated

Data Protection Officers

ÿ Art. 37 para. 1 and 7 GDPR

In the reporting period, 1,015 reports on appointed data protection

officers were received in my department. These notifications included

notifications on the appointment of official and company data protection

officers (DPO), on changes or on the termination of this function.

The General Data Protection Regulation (GDPR) provides

Art. 37 (1) obliges the controller (public bodies in general; non-public

bodies under certain conditions) to appoint a data protection officer

to name. According to Art. 37 Para. 7 of the GDPR, a Ver

responsible or a processor not only to publish the contact details of the

data protection officer,

but also to notify the supervisory authority. The documentary

mentation of the designation and the fulfillment of the reporting obligation is the

responsibility of the person responsible.

The messages sent are used by the specialist departments of my authority, among other things, to check compliance with the reporting obligation pursuant to Art. 37 (7) GDPR or the possible existence of conflicts of interest pursuant to Art. 38 (6) GDPR.

6.2.7 Formal monitoring of legislative projects

ÿ Art. 36 Para. 4 GDPR

According to Art. 36 Para. 4 of the General Data Protection Regulation (GDPR), the Free State of Saxony has me in the preparation of a draft law or a statutory ordinance

to consult the draft relating to the processing of personal data. During the reporting period, my Authority introduced during the process of legislative projects. In Saxony, for example, these included statements on the law on the further development of municipal law, the Transparency Act, the amendment to the Higher Education Freedom Act and the ordinance based on the Information Security Act and the Infection Protection Act. My predecessor also dealt with legislative projects for Germany and Europe. This related, among other things, to the Register Modernization Act, the evaluation of the Federal Data Protection Act and the Telecommunications and Telemedia Data Protection Act (TTDSG).

6.2.8 Resources

Activity report 2020: ÿ sdb.de/

tb2020

Since the General Data Protection Regulation came into force, I have

seen a continuous increase in the workload

in my office. On the grounds is my presiding officer

already received several times (cf. activity report 2020, 6.3, page 145f.).

Figure 5:

Since the Covid 19 pandemic, the workload has increased again

volume of documents

clearly increased. In the reporting period, 16,453 Post

total written material

inboxes

incoming and 22,111 outgoing mail registered. The amount of written

Mail outputs

material was almost at the record level of 2020.

25.000 25000

22.559

22.111

18.897

20.000

20000

17.152

16.453

17.775

15.000

15000

12.839

13.984

13.179

10.000

10000

9.360

5.407

4.913

5.658

5.000

5000

4.596

3.479

00

2020201920182017 2021 2017 2018 2019 2020 2021

Activity Report 2021

| 169

Machine Translated by Google

As in previous years, my authority was not able to fully fulfill the statutory tasks. The staffing situation in my authority has eased as a result of the eight new posts assigned to me in the reporting period. I would like to thank the members of the Saxon state parliament for this.

However, due to the passing of the 2021/22 budget in June 2021, I was only able to do so in the second

Half of the reporting period actually filled

begin the procedure. The development of personnel over the past few

years, as of December 31, is as follows:

• 2017: 22 posts

• 2018: 24 posts

• 2019: 28 posts

• 2020: 31 posts

• 2021: 39 posts

Figure 6:

increases in important

From 2017 to the end of 2021, the annual number of new cases in key

areas of activity

areas of activity more than tripled (Figure 6). I hope that I can adequately

reports from

cope with the consistently high number of complaints and advice given

data breaches

with a fully staffed department.

consultations

complaints

3.500

3.288

2.901

3.000

2.555

2.359

2.500

2.000

1.500

1.043

1.000

500

0

2020201920182017 2021

170 |

Chapter 6

Machine Translated by Google

In important areas of activity such as the processing of
Complaints, reports of data breaches and consultations
have resulted in the understaffing of the
Department revealed last year. Specifically: before
It was often only possible to complete work with a delay
of several months, unprovoked data protection controls
were unfortunately only carried out to a limited extent and
speaker activities at various specialist and further training
events could only be carried out to a limited extent. (see
6.5.2). Furthermore, old cases from previous years still
have to be processed. This is a situation that is difficult to
understand, especially for the persons concerned, whose
data may therefore be processed unlawfully over a longer
period of time, especially since I
I am entitled to advise citizens, business and administration
earlier and more comprehensively. Prevention is known
much better than intervention.
Successful employee training

In my office, four employees are now qualified as expert assessors from the German Accreditation Body GmbH (DAkkS), the national accreditation body of the Federal Republic of Germany based in Berlin. They are thus qualified to participate in the accreditation of certification bodies and meet the requirements for issuing certificates in the area of data protection in accordance with the General Data Protection Regulation.

Saxon

official

Data Protection Officer

Data Protection Officer

Deputy

Data Protection Officer

• Household Officer

Unit 1

Unit 2

Unit 3

• Information

technology

• Media •

• Non-public

• Municipal •

• Justice

Area •

Public

Healthcare • E-

• Police •

Government • Social •

Protection of the Constitution

Judiciary/

Unit 4

Administration

• Principle

• Legal

Services •

Administration • Public Accreditation/

work

certification

Service law

Statistics • Science

• Employee

data protection

Administration

• Personal

• Budget •

Organization

• Register •

Secretariat

Figure 7:

Simplified organization chart

of the authority

6.3 Data protection

supervisory powers,

administrative decisions

6.3.1 Utilization of the

right to refuse information

ÿ Section 40 (4) sentence 2 BDSG, Section 383 (1) No. 1 to 3 ZPO, Article

58 (1) (a) and (4) GDPR, Article 31 GDPR

According to Art. 58 Para. 1 Letter a General Data Protection Regulation

Regulation (DSGVO), the supervisory authority can instruct the

person responsible to provide all information that is necessary for

required to perform their duties. The term

“Information” includes the provision of documents or files.

Art. 31 GDPR corresponds to this provision and obliges

the person responsible to comply with the

to cooperate with the supervisory authority and to assist them in fulfilling

to support them in their tasks. However, due to the rule

of law clause in Art. 58 Para

information itself would incriminate. This information

The right to refuse can be found - in this respect initially

limited to cases of pure provision of information - in

Section 40 Para. 4 Sentence 2 of the Federal Data Protection Act (BDSG), according to which the person obliged to provide information can refuse to provide information on questions to which he himself or one of the persons listed in Section 383 Para 1 no criminal procedural principles. The prerequisite for exercising the right to refuse information is that the request for information or the provision of information relates to behavior that could constitute a criminal offense or an administrative offence. If the supervisory authority asks about various facts, it must be differentiated accordingly.

From practice: cooperation better than refusal to provide information

That's the theory. Apparently, the possibility of this right to refuse information in practice occasionally tempts one to evade the provision of information to the supervisory authority – which appears to be rather time-consuming – or one associates the Hope that the supervisory authority will be satisfied with this and that in this way one can avoid being punished for a potential violation.

The following example shows that this hope can be deceptive and that it

can ultimately lead to even greater trouble and effort:

A petitioner had given the supervisor two dome cameras

shown on private property used for residential purposes. A camera was

placed on the front next to the entrance to the house and aimed at it and

possibly also at the street a few meters in front of it; the second camera

was on the rear balcony in an exposed location on a probably extra

reason there

erected mast. Directly behind the marked by a fence

A hiking trail led along the tenth property line.

The – legally represented – person responsible had to Auf

demand of the supervisory authority merely claims that

neither third-party property nor public traffic areas

would be under video surveillance. He had not provided any additional

information required, nor had he provided any evidence/documents

requested in this regard,

in particular, no screenshots of the camera images

laid. Instead, after being asked to do so again, he made use of his right

to refuse information. An on-site review of the facts was not possible

because there was no access due to the lack of commercial use

right for the supervisory authority existed.

To the extent that it was assumed that the responsible person's assertion

that he was not monitoring any areas outside his own property was true,

invoking the right to refuse information would have been unlawful.

Because if the video surveillance was actually limited to his own property,

by answering the questions of the supervisory authority he would not

have been subject to dangerous criminal or administrative offense

prosecution

exposed.

In view of this, the further – then formal – claim against the person

responsible for the provision of information/information came into

consideration. However, it was foreseeable that - because of the expected

judicial clarification - no reliable ones would be forthcoming in the near

future

and result corresponding to the actual conditions

se could be achieved. The person responsible would also be

always been able to subsequently legally compliant

create conditions and only then to the supervisory authority

answer.

Administrative offense proceedings and

search warrants The transition to

administrative offense proceedings appeared to be more effective in

the present case. In view of the use of the right to refuse information,

there were indications that areas outside one's own

property were under video surveillance. Within an order

criminal proceedings, this could then be checked at short notice with a

corresponding search warrant and, if necessary, proven and also

punished.

In fact, the investigating magistrate at the competent local court issued

a search and confiscation order, which the supervisory authority and the

local police finally executed a few weeks later in the early hours of the morning.

The visibly surprised homeowner was cooperative – probably also to avoid extensive (but still permissible) intrusions and insights into his private sphere. Even if the cameras were no longer active at the time of the search, the homeowner agreed to the storage media previously used for video recordings being secured, so that confiscation was not necessary. The outcome of the proceedings was still open at the time this report went to press because the data carriers had not yet been evaluated.

Nevertheless, the conclusion should be drawn from the description of this supervisory case that making use of the right to refuse information needs to be carefully considered. Although not every situation will be able to justify such drastic investigative measures, it cannot actually be assumed that a supervisory procedure will simply deal with the

What should I do?

A claim of

Right to refuse information

assertion of the right to refuse information. Anyone who instead

– especially as a private individual – cooperates with the

in the supervisory process

supervisory authority from the outset and also sees a supervisory

must be carefully considered

procedure as an opportunity to use video surveillance

by the beneficiaries. Note: In

to make the investigation legally secure will hardly run the risk

the case of particularly farreaching violations, however,

of being fined for it.

cooperation with the supervisory

authority, a fine cannot be ruled

out.

6.3.2 Penalty payment for refusal to provide information

ÿ § 19 para. 2 sentence 1 SächsVwVG, Art. 58 para. 1 letter a GDPR

A Saxon commune published in their community

despiegel a letter from the Saxony State Directorate (LDS),

without blacking out the name and contact details of the contact

person in the LDS. After I was informed of the publication, my

authority asked the municipality to name a legal basis or

otherwise, for example, to black out a publication on the Internet

and to sensitize their employees accordingly to future

publications. My predecessor

had to remind him of his letter several times.

Finally, the municipality initially denied the necessity of having

to name my authority a legal basis for the processing of

personal data and later had a lawyer commissioned to inform

me that on the one hand this was in the Saxon Data Protection

Act

(SächsDSG) can be found, on the other hand there is a basis

for authorization for interventions in individual rights

Official officials anyway not needed, since there is such a one due to a lack of individual rights. My authority replied that the SächsDSG was not applicable at the time of publication (rather, due to the General Data Protection Regulation (GDPR), it was replaced by the SächsDSDG with significantly different regulations), and the rest of the presentation corresponds to current case law. Rather, fundamental rights apply to civil servants in the context of the employment relationship in the same way and not just to a lesser extent.

My authority then announced that the municipality would use Official decision to use for information and the ent to enforce the relevant administrative act using coercive measures in the form of a fine of EUR 500 in accordance with Section 19 (2) sentence 1 of the Administrative Enforcement Act for the Free State of Saxony (SächsVwVG). This announcement finally resulted in the commune acknowledging that names had not been redacted in the published letter of the LDS he accidentally followed and this is carried out in the event of a publication on the Internet (which has not yet taken place).

6.4 Fines and Sanctions, Criminal Proceedings

6.4.1 Administrative offense

proceedings in the public sector

In the reporting period, the Saxon data protection officer was

responsible for prosecuting and punishing administrative

offenses in the public sector

• § 38 Para. 1 Saxon Data Protection Act old version (§ 38

Para. 3 Sentence 1 SächsDSG old version),

• Section 22 (1) of the Saxon Data Protection Implementation

Act (Section 22 (3) of the Saxon GDPR),

• Section 48 Paragraph 1 of the Saxon Data Protection Implementation Act

(Art. 48 Para. 3 Sentence 1

SächsDSUG), • Art. 83 General Data Protection Regulation

(Art. 58 Para. 2 Letter i GDPR, Section 14 Para – in

connection with § 41 Federal Data Protection Act, Art. 83

Para. 5 General Data Protection Regulation (Art. 58 Para.

2 Letter i GDPR, § 14 Para. 1 SächsDSDG).

In the reporting period, a total of 93 fine proceedings were

pending in the public sector. Of these, 15 were completed with

a fine. 3 procedures are after lodged

An objection to the fine has been submitted to the competent district

court. A decision is still pending. In 22 proceedings, a discontinuation

took place or the prosecution was refrained from. 56 procedures were

still being processed at the end of the reporting period.

reporting period

01.01.–31.12.2021

pending total

93

of that

Procedure from previous reporting period

55

new procedures

38

37

completed

of that

with fine

15

with warning money

0

discontinued/absent from prosecution

22

still in progress

56

Total fines and warnings imposed in euros

8.250

Table 1:

Administrative offenses

proceedings in public

Area

The sum of the fines and warnings imposed amounted to 8,250 euros,

that of the final fines to 6,920 euros.

Compared to the previous reporting period, the number of new administrative offense procedures has almost doubled. Despite this, twice as many procedures were completed compared to the 2020 reporting period, mainly due to an increase in personnel, which in turn resulted in a higher sum

of the imposed fines.

The corona pandemic, which lasted during the reporting period, and However, the associated temporary limited functionality of the authority and the constantly increasing processing effort in the area of administrative offenses continued to have a negative effect in the long term

of the procedure.

Machine Translated by Google

Proceedings mainly against police officers

Once again, in a large proportion (approx. 75 percent) of the administrative offense proceedings, officers of the Saxon police were/are suspected of having accessed unauthorized personal data in electronic information systems that are only available for official purposes and not generally accessible, or personal data in them to have processed the connection without permission.

Furthermore, employees of various (social) authorities in Saxony were suspected of having processed non-public

personal data without authorisation.

The proceedings concluded with a legally binding fine in the reporting period all related to unauthorized retrieval of non-obvious personal data from the police databases (Section 38 (1) No. 1a SächsDSG old version) and/or unauthorized processing of non-obvious personal data (§ 38 Para. 1 No. 1a SächsDSG old version) by police officers.

Mostly privately motivated data retrieval

The persistently large number of administrative offense proceedings against Saxon police officers results, on the one hand, from the above-average reporting behavior of the police departments, which violate data protection regulations rigorously pursue violations – also under employment law – but also indicates that there are still ambiguities in the related to the use of police databases. It is regularly a matter of privately motivated data retrieval from the police information systems on friends, colleagues, neighbors or other acquaintances, but also research on one's own person. As already explained in detail in previous activity reports, the entire police service may only process the personal data that is required to fulfill its tasks (section 53 of the Saxon Police Service Act (SächsPVDG) in conjunction with section 3 of the SächsDSUG).

Thus, the individual police officer is only entitled

to process the data required to fulfill his specific official task. An official authority and necessity are mandatory requirements for every processing and for every retrieval of personal data from the police databases. Moreover, it would be unrealistic and absurd to assume that police officers could seriously assume that it is permissible to find out, for example, whether friends or acquaintances are friends or acquaintances by querying police files without an official reason or they themselves are recorded in police proceedings simply because such research is technically possible in the police databases. Personal curiosity or private motivation therefore does not replace the authorization required to process and/or retrieve non-obvious personal data.

The public's trust in the reliability of the authorities can already be severely damaged by mere incorrect handling of personal data by public authorities. The Punishment of administrative offenses in the public sector is essential.

6.4.2 Administrative offense proceedings in the non-public area

During the reporting period, my agency recorded 81 new ones Reports of administrative offenses – the number was thus essentially at the level of the previous year. Almost

two thirds of the advertisements (52) related to the production of video recordings: stationary cameras (34), dashcams (12), mobile phone and photo recordings (6). This means that the main focus (64 percent) of the administrative offense reports I receive is still clearly on video surveillance (previous year: 56 percent).

Machine Translated by Google

A total of 207 administrative offense proceedings were pending in the reporting period. Of these, my predecessor was able to close 73 cases and 23 fines fix.

reporting period	01.01.–31.12.2021
pending total	207
of that	
Procedure from previous reporting period	126
new procedures	81
73	
completed	
of that	
with fine	

23

discontinued/absent from prosecution

50

still in progress

134

Total imposed fines in euros

7.550

Table 2:

Administrative offenses

do not proceed in the

public area

Dashcams

19 fines related to the illegal use of dash cams by private

individuals; their amount ranged between 100 and 1,000

euros (totalling 6,250 euros). Insofar as dashcams were

only minor violations or prosecution of the impermissible

dashcam use was waived for other reasons, I have

discontinued the fine proceedings and instead issued

a warning in accordance with Article 58 (2) (b) of the

General Data Protection Regulation (GDPR) or issued

a corresponding notice (Article 58 (1) (d) GDPR).

Videography by private

individuals The remaining four fines (a total of 1,300

euros) also affected private individuals. In three cases, my

authority punished inadmissible video recordings. In one of those ca

the person concerned had a wildlife camera on their property

installed to allow a third party to submit their statements

after stalked, to convict. However, the camera was aligned in such a way that it also captured the public traffic area in front of the property and at the same time recorded the conversations on the neighboring property right next to it. The affected neighbors or their guests were not captured by image, but by audio

been identified and could be identified without a doubt

become. Since they had not filed a criminal complaint, this matter was prosecuted as an administrative offence. The two

other video cases involved video recordings of a tenant

with a camera in the inner courtyard of a large residential property, as well as secret video recordings with a mobile phone during a court hearing. Finally, the fourth proceeding was directed against the former owner of a fitness studio, who had publicly apologized via Facebook for the delay in opening his studio at the time, but at the same time shifted the blame by disclosing further personal data to a named employee and thus to him had exposed and denounced to the club members.

Search and confiscation orders In the activity reports for

2019 (page 126ff.) and 2020 (page 154ff.), my predecessor reported a house search in connection with a very extensive

Reported use of dash cams. Also in the reporting period

my authority obtained a through in a dashcam case

search and confiscation decision, but the situation here was completely

different: the starting point was verbal insults by the person concerned, which in principle is a criminal offence, against the crew of a radio patrol car who was on another assignment. As part of the check that was then carried out, the person concerned stated that he had recorded everything with his dashcam – which was permanently in operation. It is his right to film traffic with the dashcam and he can do so at any time. After it was foreseeable as a result of the appearance of the person concerned,

that a seizure or confiscation of the dashcam
only under considerable resistance and presumably under
The camera was initially refrained from confiscating because it could be used under direct coercion and at the same time the urgent processing of the original mission order was pending, but a complaint was made to this effect.

It was therefore a case of an administrative offense report, which was not already attached to the evidence (memory card of the dashcam) as is usually the case. Instead, however, there were other strong indications of illegal dashcam use. A hearing of the person concerned would very likely have resulted in the person concerned denying the allegation to the administrative authority without being able to verify it, or in deleting the memory card before it was handed over to the administrative authority, or in handing over another data medium straight away. An alternative investigative measure was not evident; the accusation but at least so

serious that even a hiring was out of the question. The result of the search, which was limited to his vehicle and the dashcam located there due to the presence and willingness of the person concerned to cooperate, was surprising in that it did actually no relevant video recordings were contained on the memory card. The person concerned stated that he was only bluffing the police officer and that he had only bought the dashcam for use abroad. The example shows, on the one hand, that searches are not exclusively with the aim of finding incriminating evidence be led, but of course can also lead to to relieve those affected. On the other hand, this It's clear that hasty statements made against police forces with the aim of intimidating them are not very promising and can quickly turn into the opposite.

The second case in which I applied for and executed a search and seizure warrant concerned stationary video surveillance in which the person concerned

was of the opinion that he could evade access by the information authorities by invoking his right to refuse information, and in which I had no other choice than to switch from the supervisory to the administrative offense proceedings due to the lack of further opportunities for clarification and the lack of access rights, cf Statements under 6.3.1 on exercising

the right to refuse information.

6.4.3 Sanctioning of so-called

employee excesses

ÿ Art. 25, 83 GDPR; § 48 Saxon GDPR

My predecessor in office had commented on the procedures

for prosecuting employees in the event of violations of Article

83 (5) of the General Data Protection Regulation (GDPR),

Activity report 2017/2018: ÿ sdb.de/

see activity report from April 1, 2017 to December 31, 2018, page

tb2109

252ff.

No penalty without a clear legal basis

According to Art. 83 GDPR, only those responsible, Art. 4 No.

7 GDPR, or persons in the

Cases in which this is determined by area-specific regulations

– for example state fines – and for which the regulations of

the Administrative Offenses Act (OWiG) then apply mutatis

mutandis.

Sanctioning requires a clear legal basis that satisfies the

principle of certainty.

Prerequisites for the applicability of Art. 83

General Data Protection Regulation

The inappropriate viewing or retrieval of information in the

infrastructure of the employer or the employer is not sufficient

for the assumption of responsibility under the GDPR.

Cumulatively, that must be added

retrieving person also via the means of data processing

tion. The employee is not already responsible if he or she has

a certain degree of personal responsibility

has been transferred, which allows him to independently view or retrieve

personal data from automated processes, at least not if the individual

authority of an individual who is assigned to the person responsible is not

expressly sanctioned by law, cf. below on the application practice . Much

more is therefore required the authority to dispose of the means, that is

Employee excesses that reach

a certain extent are regularly

reported, also with regard to

those of the person responsible – the authority or the company

men – to organize compliance with data protection regulations, data

Art. 25 GDPR and

protection organizational measures, consideration of the rights of those

insufficient technical and

affected, etc.

organizational measures by the

person responsible for enabling

the employee to access the data.

In addition, in practice, the traceability of pure "curiosity requests" that

occur particularly frequently should regularly fail due to Art. 2 (2) (c)

GDPR.

However, the excess of employees can in turn then declined

be tionable if the information retrieving Be

processed them further with his data processing devices, which means

that further data processing phases outside the employer's sphere were

added.

Example: An employee of a controller calls up name and address data,

saves it on his own data carrier and processes it for the purposes of his

part-time job – the sale of financial products

home on his home computer.

Previous court decisions

With the Administrative Court of Dresden and in its decision of February

5, 2020 (VG Dresden, judgment of 05.

February 2020 – 10 K 372/16.D –, para. 83 - 85, juris) referred to by the

established case law of the Federal Administrative Court, my authority

assumes that the use of official information systems - even for nonemployee, private purposes - is an internal act. This, in

particular the

integration of such a breach of duty Ver

keep in the office and in the associated official

Activity (Federal Administrative Court, judgment of August 19, 2010 -

–,

2 C 5.10 juris para. 9), precludes the assumption that the employee as a

private individual and his own responsible person

would be treated within the meaning of Art. 4 No. 7 GDPR. This

applies a fortiori to actions that are exclusively official

serve purposes.

So far, two other court decisions were after

effective date of the General Data Protection Regulation, which at least

marginally tend to have its own

ne responsibility of employees who act excessively

take, LG Freiburg and VG Mainz. court decisions,

According to Art. 83 data protection for employee excesses

Basic Regulation does not apply are not known.

In a decision of November 30, 2021 - 4 U 1158/21 - the OLG Dresden

also took the view that a business

leader of a person in charge next to the person in charge

itself is to be regarded as its own responsibility.

application practice

My authority applies with regard to an administrative offence

only landed at public Saxon offices

of the legal fine regulations, according to the provision of § 48 Saxon Data

Protection Implementation Act in dir

line area.

An application of Art. 83 GDPR to employees who have processed nonpublic data without authorization in the course of their

professional activity

is generally not carried out by my authority for the reasons set out above,

provided that there are no further processing steps. It would be the sole

responsibility of the legislator or legislator to regulate further.

6.5 Public Relations

6.5.1 Press work

and online communication

Press and media work remains an important communication tool for my authority. In the reporting period, this not only included answering media inquiries, but also publishing press releases, for example on the register modernization

law, Safer Internet Day, data protection in schools, examining media companies and the dangers of cyber attacks.

Since June 2021, media information from my authority

Press releases of the SDB:

ÿ medienservice.sachsen.de

via the media service of the Free State of Saxony free of charge

be subscribed to.

Journalists also approached my authority with a wide variety of questions. A lot was related to the pandemic and digitization. Among other things, it was about data leaks at test centers, digital health applications, bonus programs for vaccinated people, model projects, the school app Scoolio, the data protection compliance of fax machines, video surveillance in Chemnitz and much more.

Another important communication tool is my website. Preparations for the redesign began in the reporting period. At the same time, the employees in my department regularly posted information on current topics on the previous platform. A focal point

repeated the data protection in the corona pandemic.

But also information on the use of consent layers

and the Telecommunication Telemedia Data Protection Act

setz (TTDSG) and many other data protection issues have been published.

Interested parties received further support and advice from the Virtual

Data Protection Office, which I also contact

involved. This is an information portal for citizens that is operated by

Virtual Data Protection Office:

German-speaking state, church and broadcasting data protection officers.

ÿ www.datenschutz.de

6.5.2 Training and Lectures

During the reporting period, employees

held 21 training seminars from my office, including at the Saxon

Administrative and Economic Academy in Dresden, at the training center

of the

Free State of Saxony, at the State Office for Schools and Education

and at a school in Dresden. There were also shorter occurrences

sluggish, for example at an event with the Säch

sian youth foundation in November. 35 FSJler (voluntary

social year) took part.

Compared to the previous year, there was a slight increase

in the number of lecturers, favored by increasing digitization

and a broader range of online seminars.

In the overall view of the longer past years, however, a

decline in the number of lecturers can be seen

place. The causes also include protection against infection

measures in connection with the coronavirus pandemic,

which is why a number of events have been cancelled.

Furthermore, the decline is due to the high workload in the

office.

In the presentations during the reporting period, the basics

and current issues relating to the General Data Protection

Regulation were dealt with in particular. Data protection in

schools and local government was also an issue. In

addition, the basics in the area of employee data protection

were increasingly taught in the reporting period.

Chapter 6

Machine Translated by Google

7 cooperation of

data protection supervisory authorities,

Data Protection Conference

A look at the following resolutions, resolutions, orientation aids,

statements and application notes makes clear the variety of topics with

which I am dealing

authority in the context of the data protection conference.

7.1 Data Protection Conference

Materials – Resolutions

Resolutions are public statements by the DSK on data protection policy

issues, such as the introduction

of a new law.

• Use the opportunities of the Corona-Warn-App 2.0 (04/29/2021) •

Proof of vaccination, proof of negative test results

and proof of recovery in the private sector and in employment are

regulated by law! (03/29/2021)

7.2 Data Protection Conference

Materials – Resolutions

Resolutions are positions that relate to the interpretation of data

protection regulations or corresponding recommendations.

• On the possibility of non-application of technical and organizational

measures according to Art. 32 GDPR

at the express request of data subjects

(24.11.2021)

• Processing of the "vaccination status" date of employees by

the employer (October 19, 2021)

• Processing of positive data from private individuals from

contracts for mobile phone services and long-term trading

accounts by credit bureaus (09/22/2021) • Pool of energy

suppliers must not lead to transparent consumers* (03/15/2021)

7.3 Data Protection

Conference Materials - Guidance

Orientation aids and standardization are technical application aids

for those responsible, contract processors, manufacturers and the

public.

• Frequently asked questions and answers for processing

processing of employee data in connection with the corona

pandemic (December 20, 2021) • Guidance from the

supervisory authorities for providers

Telemedia users from December 1, 2021

(20.12.2021)

• Measures to protect personal data when transmitting by email

(06/16/2021) • Use of digital services for contact tracing

Follow-up on visits to events, facilities, restaurants and

shops to prevent the spread of Covid-19 (04/29/2021)

7.4 Data Protection

Conference Materials – Statements

Opinions are positions that are given in judicial or legislative

proceedings, among other things.

• Responsibility in Using Contact

tracking systems such as the Luca App (05/21/2021)

• Technical data protection requirements for messenger

services in the hospital sector (04/29/2021)

• Contact tracing systems – in particular to “Luca” from

culture4life GmbH (04/29/2021) • Contact tracing in

times of the corona pandemic – combining practical solutions

with a high level of protection of personal data (03/26/2021)

• Evaluation of the BDSG (03/02/2021)

7.5 Data Protection

Conference Materials – Application

• Requirements for data protection certification programs - data

protection test criteria,

Test systematics and test methods for adjustment and

Application of the technical standard DIN EN ISO/IEC 17067

(program type 6)

7.6 European Data Protection

Board documents: guidelines,

recommendations, best

practices

The European Data Protection Board approved the documents

listed below.

• Guidelines 05/2021 on the Interplay between the application

of Article 3 and the provisions on international transfers

as per Chapter V of the GDPR (18.11.2021) • Guidelines

10/2020 on restrictions under Article 23 GDPR (13.10.2021)

• Guidelines on the terms “controller” and “processor” in

the GDPR (07/07/2021) • Guidelines 04/2021 on codes of

conduct as tools for transfers (07/07/2021)

• Guidelines 02/2021 on virtual language assistants –

Version 2.0 (07/07/2021) • Recommendations

01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (06/18/2021) • Recommendations 02/2021 on Legal basis for the Storage of credit card data solely for the purpose of facilitating further online transactions (05/19/2021)

• Guidelines 8/2020 on the targeted addressing of users of social media (04/13/2021)

• Guidelines 03/2021 on the application of Article 65(1)(a) GDPR (13.04.2021)

• Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) (06.04.2021)

• Guidelines 09/2020 on the relevant and justify th objection within the meaning of Regulation (EU) 2016/679 (09.03.2021)

• Guidelines 02/2021 on Virtual Voice Assistants – Version 1.0 (03/09/2021) • Guidelines 01/2020 on the processing of personal data in connection with connected vehicles and mobility-related applications (03/09/2021) • Recommendations 01/2021 on the reference basis for the term “Adequacy” in the Policy on Data Breach in Law Enforcement (02/02/2021) • Guidelines 01/2021 on Examples regarding Data Breach Notification (19/01/2021)

Chapter 7

Machine Translated by Google

7.7 Joint Review

by media companies

data protection supervisory authorities

ÿ Art. 6, 28 GDPR

Activity report 2020: ÿ

sdb.de/tb2020

In the 2020 activity report (section 7.8, page 164), my predecessor reported on a joint audit of media companies, in which a total of eleven of the German data protection supervisory authorities are taking part. In 2020, questionnaires were developed for this purpose and sent to the online media with the greatest reach in the respective state shipped.

In the first half of 2021, the questionnaires in the various federal states were evaluated by the supervisory authorities and individual services were subjected to a more in-depth review. Information on individual services was exchanged between the supervisory authorities, but information on the audited companies was kept strictly within their respective areas of responsibility. In view of the well over 100 different services used, in some cases with different configurations, the examination of the sometimes very complex data processing and the available contractual documents proved to be very time-consuming. It would be just as time-consuming to bring about coordinated views on individual services or the permissible design of consent solutions.

From the summer to late autumn, talks were held with all the media

companies affected by the audit in my area of responsibility. In doing

so, questions of

Deployment of services discussed: data transfers to the outside

European countries, individual solutions for bringing about a consent

decision as well as third-party services and their necessity. My

predecessor in office made it clear where he felt changes were

necessary and that he also took note of the media companies' arguments

regarding the financing of online journalism

What should I do?

media companies are

kept the existing ones

Business models and there

in particular the transfer of user

men has. Overall, the talks were very constructive, and

there have already been a number of adjustments in the

meantime, so that a significantly better level of data

protection can be seen compared to the year before the

joint review. The talks are not yet over. Even if extensions

of deadlines have been granted to date for the

Techniques.

implementation of the changes, which are quite complex

from a technical and business procedural point of view, I

cannot rule out that individual aspects of data processing

will have to be cleaned up by means of supervisory law

and that courts may have to deal with the questions of

the admissibility of individual processing operations.

data

to set the test. This

requires a precise examination of

all services used and their use of

data by cookies and similar

8 Directive area - Directive (EU) 2016/680 - and other areas

8.1 Tasks of the GKDZ according to § 4 GKDZ-StV

For several years now, I have been supporting the process of setting up a joint competence and service center for the police forces of the states of Berlin, Brandenburg, Saxony, Saxony-Anhalt and Thuringia in the field of police telecommunications surveillance as a public-law institution with legal capacity (GKDZ).

In the future, the GKDZ is to act as the central service provider for the responsible states in the area of police telecommunications surveillance, data from telecommunications surveillance measures in accordance with the respective state police laws and Sections 100a et seq process countries.

On September 8, 2017, the sponsoring countries signed the state treaty

on the establishment of the GKDZ (GKDZ-StV), which was subsequently confirmed by the parliaments of the sponsoring countries.

The Saxon state parliament approved the state treaty by Ge added on December 13, 2017.

Position of the state data protection officers of the sponsoring countries

In the course of the participation of the state data protection officers of the responsible states in the planning of the GKDZ already in 2019 a dissent between the GKDZ and the State data protection officer with regard to the tasks assigned to the GKDZ by state treaty, which also

reporting period could not be dissolved and think Predecessors and my counterparts caused the Interior departments of the sponsoring countries as holders of the legal to inform you about our position via the GKDZ:

§ 4 GKDZ-StV is decisive for the determination of the tasks, the fulfillment of which is assigned to the GKDZ as a sovereign institution under public law. According to this, the sponsoring countries use the institution by way of order processing for data from police telecommunications surveillance according to the respective state police laws and §§ 100a ff. StPO (core task), § 4 paragraph 1 sentence 2 GKDZ StV. The term telecommunications surveillance is defined below in Section 4 (1) sentence 3 GKDZ-StV:

“Telecom monitoring is the processing of usage, content, traffic,

inventory and

location data for the purposes of prevention, detection,

Detection or prosecution of criminal offenses and

Protection against and averting of dangers for the

public safety."

According to this, it is excluded that the tasks of the GKDZ could extend

to order processing of data from police or criminal procedural measures

that are not related to telecommunications processes and/or

telecommunications surveillance.

Data that is collected from information technology systems, for example

by way of online searches (§ 100b StPO or corresponding regulation

under state police law),

are not telecommunications data within the meaning of § 4 para.

1 sentence 3 GKDZ-StV. It is just as little concerned with data obtained

from acoustic monitoring of living space, Section 100c StPO, acoustic

monitoring outside of living space, Section 100f StPO, and other measures

outside of

Housing according to § 100h StPO will be charged to Telekom

communication data. The same applies to data that was collected by way

of seizure or confiscation in accordance with §§ 94, 98 and 99 StPO

(postal confiscation). According to these regulations or the corresponding

state police law

The data collected by the authorities does not originate from

telecommunications processes and can therefore not have been obtained by means of police surveillance of telecommunications; their (order) processing by the GKDZ is not covered by the assignment of tasks in § 4 GKDZ-StV. The same applies to data from the state police's electronic reconnaissance. Even taking into account the system- and development-open design of Section 4 (1) GKDZ-StV from the point of view of the GKDZ and the case law of the Federal Constitutional Court on telecommunications secrecy that is open to development, a qualification of processes and activities that go beyond Sections 100c, 100f and 100h StPO in a criminal investigation, as "telecommunication" under no legal, factual or technical point of view possible. If data carriers are secured or confiscated, there is a data collection measure in the form of "security" or "seizure" with regard to the data contained in them, which is also referred to as summoning up ter fantasy not as a measure of telecommunications monitoring can be qualified.

Interpretation of the concept of telecommunications

From the point of view of the Federal Constitutional Court (BVerfG), the concept of telecommunications secrecy is open to development and technology, but at the same time the court emphasizes that only "with the help of the available telecommunications technologies subsequent transmissions of information" are covered (BVerfG, 9.10. 2002, Ref.: 1 BvR 1611/96, 1 BvR 805/98). Such information transmissions take place in circumstances in which §§ 100b, 100c, 100f, 100h and 94, 98, 99 St

Application come, simply does not take place.

An interpretation of the terms “telecommunications” and

“telecommunications monitoring” completely detached from the

general understanding, from legal definitions and from the case

law of the constitutional court is prohibited for an institution under

public law bound by law and justice as a processor as well as for

Criminal prosecution and hazard prevention authorities as those

responsible for data protection who use the GKDZ for order processing.

The Saxon State Ministry of Justice and for Demo

kratie, Europe and Equality shares this view.

Thus, § 4 para. 1 GKDZ-StV sets the framework in which the

GKDZ may become active and process personal data of persons affected

by police intervention measures. At the same time, Section 4 (1) GKDZStV stipulates that the core task is to be fulfilled by

means of order

processing. The fulfillment of other tasks associated with encroachments

on fundamental rights - the provision of support and advisory services in

accordance with Section 4 (2).

GKDZ-StV is not covered by this

–,

is the GKDZ as öf

public body denied due to lack of statutory assignment of tasks. This

also applies to activities outside the area specified in § 4 Para. 1 GKDZStV if they are also

how the core task is to be carried out by way of order processing, as the

statutory provision stipulates that (only) the assigned task is to be fulfilled

by way of order processing. For the GKDZ, this means that order

processing of data that does not originate from police telecommunications

surveillance is not provided for by law and is therefore inadmissible.

No unauthorized extension of the legal

range of tasks

A public body that has been assigned specific tasks by the legislature is

not entitled to

this – finally formulated here in § 4 GKDZ

to expand the gift catalog on their own. The clear will of the legislator or

legislators would therefore oppose order processing outside of the

statutory framework; even an agreement between two executive branches

cannot circumvent such a (and restricted) assignment of tasks by the

legislature.

Should the sponsoring states wish to transfer further tasks

associated with fundamental rights encroachments to the

GKDZ, they and first and foremost their parliaments would of

What should I do?

The GKDZ has registered with Ver

course be free to expand the range of tasks of the GKDZ by

amending the state treaty.

to limit the processing of personal

I will use the powers available to me to enforce compliance

data by way of order processing to

in accordance with my legal role

the tasks assigned to it by law in

data protection regulations by the GKDZ - here

accordance with § 4 GKDZ-StV.

to enforce the processing of sovereign data only to the extent

specified by the legislature.

8.2 Use of a facial

recognition program for

criminal prosecution by

the Dresden police department

ÿ § 48 BDSG, § 163 StPO

My authority became aware of this through media reports

It is notable that the Dresden Police Headquarters used a

program with a facial recognition function to investigate a

large number of crimes, some of which were serious, in

connection with the riots surrounding a Dynamo Dresden

sports association football match on May 16, 2021

uses.

The police directorate answered the related data protection

questions in the context of a discussion and the presentation

of the program. In addition, a data protection impact

assessment was submitted in accordance with Section 67 of

the Federal Data Protection Act (BDSG).

The procedure followed by the police is as follows

measures.

Due to the events on the afternoon of May 16, 2021, in the course of which massive attacks on police officers and considerable damage to property were carried out from a large crowd, the Police Directorate tion Dresden a special commission for criminal law reconnaissance used.

Images from various sources

Police officers had video recordings during the riots based on the Saxon Police Enforcement Service Act (SächsPVDG) and the Code of Criminal Procedure (StPO). Subsequently, the police secured the time of the crime me video recordings from the scene of the crime adjoining video surveillance systems (e.g. that of the Rudolf Harbig Stadium). The investigators also saved recordings of the riots on publicly accessible video and social media platforms YouTube and Facebook. In addition, an information portal was activated on which witnesses or other third parties were given the opportunity to download multimedia data on the incidents to deposit.

The collected and stored image data are then stored together and brought into a place-time reference, which enables the search for a specific (crime) place or a (crime)

time.

Software generates biometric data

The software used automatically detects facial and body

images from the image data collected, which are used in

the context of subsequent comparisons that are triggered

manually. In the course of storage, the images are

automatically indexed, in

in which the image material is screened and significant

points of patterns relevant to face detection are determined,

which in a next step allow identification or comparison.

As part of data processing, software-based algorithms are

used for automated processing of personal data for the

purpose of face detection and face identification based on

biometric data (facial images).

Automated face detection describes the technical

Process in which automated and not individualized

a search is made for existing facial patterns in an image,

a sequence of images or a video. Through this tech

nical methods, suitable facial images are calculated for comparison.

Of particular importance are features of the face that are subject to

few changes due to facial expressions (e.g. hollow edges of the eyes,

sides of the mouth, ...). The result of the calculation is referred to as a

"template".

Face detection is followed by face identification

Face detection is a required technical pre-requisite

stage for the subsequent automated face identification. This processing

step captures all people or faces or faces recognized by the program

in the image material.

face pattern; It is irrelevant whether the person concerned

son is shown in criminally relevant acts.

The faces or the “templates” calculated from them are stored in a

reference database within the program, with which the reference data/

identities presented by the investigators are then compared by way of

automated face identification.

Automated facial identification describes the tech

nical process in which face

detection-indexed face images with face images

Reference data are automatically compared. As a result of the auto

mated method of face identification becomes a

Correlation of the matched facial images is calculated. Depending on

the calculated match, a hit case is displayed.

Pictures or videos of people known to the investigators,

who were identified on the day of the assignment through the

identification service or similar can be stored and analyzed in the

program as reference data (identity). You can then search for them in

a targeted manner in order to find incriminating and exculpatory video

material.

If hitherto unknown persons are found in the secured data, for whom,

based on the recordings, there are sufficient actual indications for a

traceable

a criminal offense or an administrative offence, the detected

Machine Translated by Google

The animal face/object (body) can be created as a reference

file (identity) and thus further video material with the person

can be searched for.

After comparing the reference images with the entire image

material (reference database), the system displays faces

with a high mathematically calculated similarity (hits) in

relation to the identity sought. The maximal

The number of hits can be set by the user. The

Sorting is based on the calculated probability, sorted from

highest to lowest. The system does not automatically decide

that there is a match. It is just a pre-sorting to enable the

subsequent manual verification check

lighten.

An employee checks the factual accuracy of the hit case by

comparing the created identity with the calculated comparison

images (manual verification check).

"Hit images" where the manual verification check did not

confirm the hit case are automatically reposted

Termination of search in the separate hit file deleted;

however, the deletion does not affect the data

reference database.

Technical and organizational protection of data

The server technology, on which the application analyzes

the saved data in order to compare it with the reference data,

is operated separately from other data systems in a closed

area. insight into

Only the investigators entrusted with the facts have data

ler and video evaluator. In addition to access at file level,

which is accessible to the investigators of the procedure,

additional access (user name, password) is required to

process the case with the software.

The police directorate sees the legal basis for the collection,

storage, comparison and deletion of the image data in the

Code of Criminal Procedure (StPO), which also forms the

legal framework within which the image data in the

May be further processed in case of a hit. The basis specifically for the

creation and use of the reference database, which contains the data or

images with which the stored image material of the criminally relevant

processes is compared, lies in Section 163 (1) StPO in conjunction with

Section 48 (1). , 46 no. 14 letter c BDSG.

legal framework

Although I consider the processing of biometric data, in particular in the

form of automated facial recognition and in the context of the fulfillment

of police tasks, to be critical and risky from a data protection point of view,

I have opposed the use of software in narrowly limited applications that collects biometric characteristics of data subjects within generated and compared from lawfully obtained evidence, no serious concerns. The use of the software in the concrete,
the manner described by the police department
not to complain about.
The footage used in the proceedings of the riots on May 16, 2021 is likely to have been lawfully collected on the basis of §§ 161 Paragraph 1, 163 Paragraph 1 StPO, insofar as the police themselves made the recordings to preserve evidence. Photographs taken by the local police to the dangers defense on the basis of Section 57 (2) SächsPVDG may use it to prosecute crimes committed there in accordance with Section 79 (2) SächsPVDG. Third-party image material was lawful on the basis of Section 94 (1) StPO
to ensure.
The processing of this data in the form of storage as well as reading, using and comparing (§ 46 No. 2 BDSG) can be based on § 163 Paragraph 1 StPO. However, this provision does not automatically allow the processing of biometric data (Section 46 No. 12 BDSG) as used by the police
Direction Dresden using the software described above
makes. If biometric data is used to uniquely identify a natural person (§ 46 No. 14 Letter c BDSG), their processing according to § 48 Para. 1 BDSG is only

negligent if it is "absolutely necessary" to fulfill the task (§ 48 Para. 2 BDSG).

Processing is "absolutely necessary" if it appears almost indispensable for the fulfillment of the task.

I regard this condition as fulfilled in the present case. The state has an obligation to ensure effective criminal prosecution, but at the same time its actions must always be proportionate. If the criminal prosecution authorities have footage of suspected serious crimes, including those directed against individuals, they are obliged to investigate these crimes. If, due to the number of legal violations depicted and the extent of the image material, a purely "human" viewing of the material would take a disproportionately long time and effective criminal prosecution would thus be practically thwarted, the use of available technical aids for viewing and evaluating the Image material and therefore for the timely investigation of criminal offenses for the task of criminal prosecution incumbent on the police and the public prosecutor's office "absolutely necessary" within the meaning of Section 48 (1) BDSG.

However, Section 48 (2) BDSG – in parallel with or in the form of the principle of proportionality, which must always be observed – requires suitable guarantees for the legal interests of the data subjects when processing special categories of personal data.

The approach taken by the Dresden Police Headquarters and the precautions it has taken to minimize risks for the people depicted on the photos used, who are biometrically recorded and therefore included in the system-based comparison, do not raise any serious concerns in this respect. However, I have considerable doubts as to the suitability of the provision of Section 48 BDSG as a general authorization standard for the use of facial recognition software in the area of criminal prosecution. The provision essentially only reproduces the wording of Art. 10 of Directive (EU) 2016/680 and only lists possible measures to protect those affected as examples. With regard to other processing situations

With regard to other categories of data that are particularly worthy of protection, this may be sufficient; as a basis for generating biometric data from under circumstances the hundreds or even thousands of those affected, most of whom were not involved in criminal offenses, and their intensive use in the form of repeated comparisons, § 48 BDSG is unlikely to meet the requirements for a sufficiently specific, clear and proportionate overriding standard. My assessment can therefore only apply to the specific use of the program with face recognition function in the specific investigation into the riots on May 16, 2021 at the Rudolf Harbig Stadium in Dresden.

However, the use of the software cannot be attested to be generally unobjectionable under data protection law. On the contrary, the description of the procedure shows that programs with an automated facial recognition function may only be used if proportionality is strictly observed. The reason for this lies in the large number of people affected by the processing, who neither appear as disruptors under criminal law nor as suspects under criminal law, but only appear by chance and as bystanders in the image material that depicts the behavior of individuals relevant to the police. These uninvolved third parties are also subjected to police processing of their data – just like all of the people captured in the photos without exception

category of personal data that is particularly worthy of protection

data concerns.

The system-immanent creation and indexing of comparison data, which already takes place in the course of storing the investigation-relevant image material and without exception affects all persons depicted and is only the basis for results in comparisons to be carried out later, creates a - temporary - database with biometric data of everyone in the recordings depicted persons.

The associated depth of intervention with regard to the

The fundamental right of those affected to an informational self

determination is significant – not only are images relating

to you stored, but biometric data relating to you are also

–,

obtained from them and processed – the risks are obvious. With unrestricted use of biometric comparison data generated from image recordings from (numerous) different procedures and different sources, the technology enabled rapid comparability and person-related research, which would be all the more extensive in terms of time and place, the longer the image and comparison data were stored and made available across procedures would. The creation of detailed individual behavior and movement profiles would be possible without much effort.

Such processing of personal data – with regard to uninvolved persons or persons not identified in verified hits, this was done “in advance” and therefore illegal – would be clearly unconstitutional (cf. here on the case law of the Federal Constitutional Court on automated license plate recognition and the obligation to immediate, traceless Deletion of "non-matches", BVerfG, 18.12.2018, Az.: 1 BvR 142/15, No. 97, 98).

The use of comparison data based on biometric features must therefore be strictly limited to the specific investigative procedures remain limited. This data, most of which can usually be attributed to uninvolved persons, must be deleted at the latest when the evaluation of the images stored as evidence has been completed.

Minimum requirements for the use of

facial recognition software

Against this background, I consider the following

requirements to be indispensable for the use of face

recognition software for the purpose of criminal prosecution,

limited to a single investigation:

• The use of programs with automated face recognition is to be

restricted to processes of criminal law that are significant due

to the

Individual circumstances not cleared up in any other way or

only cleared up with a disproportionate amount of time

could become.

• To interfere with the right to informational self

In order to keep the identification of data subjects as low as

possible, when deciding which image material is to be included in

the evaluation, strict attention must be paid to necessity and

proportionality (§ 47 No. 3 BDSG).

• When pre-selecting the visuals to be included

therefore a narrow local and temporal restriction is to be

implemented; Footage taken outside the crime scene

or in its immediate vicinity and outside the time of the crime, must

be disregarded

remain.

• A comparison with images that do not have such narrow location and
Time reference to the crime must be avoided (this applies in
particular to image data that is not crime-related
from social media channels and not directly tatbe
recorded recordings from official and private video surveillance
systems, for example in public places, train stations or in local
public transport).
• The reference database must not be mixed with other files
or sources of knowledge are networked (§ 48 Para. 2 No. 5
BDSG).
• The templates stored in the reference database may not be used
for purposes other than image matching in the specific procedure;
a procedure
Cross-border use of the comparison data from the reference
database is not permitted. • An internet-based application
("cloud application") is not permitted, the technology must be operated
separately from other data systems.

• A transfer/disclosure of personal
Data to the manufacturer of the program or other
third parties, also in the context of support or
maintenance work, is not permitted. • Access to
the application and the reference database is to be
restricted to a small, clearly defined group of

people.

• The reference database must be deleted at the latest upon completion of the evaluation of the image material. • Image data that was created on the basis of a supposed but actually unverified match (false positive hits) must be deleted immediately. • Measures that have an impact on individuals affected may not be taken on the basis of "system-side" signals, ie solely on the basis of a computing process and without human control and decision (§ 54 BDSG).

Under these conditions, I consider the use of software with a facial recognition function for criminal prosecution purposes in a specific investigation acceptable under data protection law.

In view of the extent of the measure’s encroachment – even if the above-mentioned high requirements are met – and its potentially wide spread, as well as the vagueness of the provision of Section 48 BDSG, a standard-clear

What should I do?

The use of programs with legal regulation on the use of facial recognition software would ensure legal security for the law enforcement automated facial authorities and could at the same time reduce the risk recognition in criminal

minimize disproportionate harm to data subjects. I think

prosecution is only under narrow

Boundaries and not procedural

it is necessary to create a corresponding legal basis.

universally permitted.

208 |

Chapter 8

Machine Translated by Google

9 case law on data protection

9.1 Compensation for pain and

suffering for each breach of the GDPR?

ÿ Art. 9 GDPR, Art. 82 Para. 1 GDPR

The European Court of Justice is currently dealing, among

other things, with the questions of whether Article 82 (1) of the

General Data Protection Regulation (GDPR) has a special or

general preventive character, following a preliminary ruling by

the Federal Labor Court (ruling of August 26, 2021 – 8 AZR 253/20).

It is also checked whether this is the case when measuring the height

a non-material damage to be compensated according to Art. 82

GDPR at the expense of the person responsible or

Processor must be taken into account and whether it is when

assessing the amount of an immate to be replaced

tial damage to the degree of culpability of the responsible

literal or order processor arrives.

The Federal Labor Court is of the opinion that the person

concerned does not have to have suffered consequences of

at least some weight, but that a breach of the General Data Protection Regulation itself constitutes non-material damage to be compensated. The Austrian Supreme Court (ruling of April 15, 2021 – 6 Ob 35/21x –; ZD 2021, 631) and the Supreme Administrative Court of Bulgaria (European Court of Justice, case C-340/21) have made similar submission decisions.

These questions are based on a case from Ar right of employment. A medical service worker a health insurance company was seven months after starting a Illness on behalf of his health insurance because of doubts

medically examined by his employer due to his incapacity to work. A doctor at his employer diagnosed a “severe depression without psychotic symptoms”.

The plaintiff learned from the doctor treating him that he had been contacted by the expert. A colleague from the IT department confirmed to the plaintiff that a report about him was stored in his employer's digital archive and photographed it for him. The plaintiff and his colleague were fired during the course of the lawsuit.

The plaintiff sued his employer for material and immaterial damages due to violations of data protection regulations in the employment relationship.

The answer to the questions referred will also be of considerable

importance for Saxony. Because if a mere violation of the

What should I do?

General Data Protection Regulation without the existence or

The decision of the ECJ remains

proof of damage being sufficient as a reason for compensation,

to be seen. Only

this would be very badly affected

the consequences for local

practice can be drawn.

friendly and could lead to a wave of lawsuits as in the so-called

th diesel scandal.

9.2 BAG on the right to information

- right to a copy of data in

accordance with Art. 15 (3) GDPR

ÿ Section 253 (2) ZPO, Art. 15 (3) GDPR

In a judgment of April 27, 2021 - 2 AZR 342/20 - the Federal

Labor Court (BAG) ruled on the right to information under

Article 15 of the General Data Protection Regulation (GDPR).

It was about the right to be granted a copy of the data.

In the process to be decided, the employee claimed to receive

a data copy of all business emails against his employer, Art. 15

(3) GDPR.

In the dispute, the court ruled that the claim was not enforceable

as it was not clear to which

e-mails based on the request for surrender. A content-related

data protection assessment was not carried out.

The court referred to the civil procedural rule

Machine Translated by Google

What should I do?

When asserting a right to

information, Recital 63 of the

General Data Protection

of Section 253 (2) of the Code of Civil Procedure (ZPO) and an

impossibility of determining in a specific case in the enforcement

proceedings which e-mails are to be disclosed as copies. The limitation

Regulation must be observed,

and consideration of the court is in line with recital 63 sentence 7 of the

according to which the data subject

General Data Protection Regulation.

must specify which information he

or she is referring to.

9.3 BGH: content and

scope of the right to information

ÿ Article 15 GDPR

In a decision of June 15, 2021 - VI ZR 576/19 - the Federal Court of

Justice (BGH) ruled on the content and scope of the right to information

under Article 15 of the General Data Protection Regulation (GDPR).

The legal dispute to be decided was about the fact that the

owner of a life insurance policy had received information

from the insurance company - the person responsible - and this

but considered incomplete. The person concerned took the position that

all the data available about him at the company, including

Correspondence and internal records and notes to be informed. The

lower court had such a far-reaching right to information

already denied.

The Federal Court of Justice, however, judged the process

differently and considered the right to information under Article 15 of

the General Data Protection Regulation to be fundamentally comprehensive.

In principle, all stored or

processed data relating to the data subject

reportable. This means that internal documents and correspondence in

which the person concerned was not involved also belong to the

information provided.

However, the court restricted that to the not to

information provided data on internal appraisals

The insurance company's claims and legal assessments made counted,

as these did not

Information about the person concerned and thus no personal

represented data. The same applies to commission payments to third

parties. Corresponding documents may also be blacked out in this

respect.

What should I do?

A central point of the decision was also that the right to information

The right to information according to

according to the Federal Court of Justice was fulfilled if the information

Art. 15 GDPR is generally comprehensive.

Is information

debtor declared when providing information that the information was

on the part of the person responsible

complete or if this resulted from his information. In this respect, a mere

has been granted - at least in the

suspicion opens up that the information provided is not

absence of further evidence

points - it can be assumed that the

obligation under Art. 15

is correct or incomplete, no entitlement to information to a greater

DSGVO has also been fulfilled.

extent.

9.4 Statutory retention

requirements and the right

to erasure

ÿ § 147 AO, Art. 17 DSGVO

On December 14, 2021, the Dresden Higher Regional Court ruled - 4

U 1278/21 - on the question of whether unauthorized data should be

deleted if the corresponding documents are subject to statutory

retention requirements.

In the initial case, a company asked a supposed debtor to settle an

outstanding claim. Due to the same name, however, it was the person

concerned who was addressed in this way

not the actual debtor. The person concerned

then requested the person responsible to delete it. The person

responsible – the company – argued against this that there are storage

obligations under the tax code, Section 147 of the tax code (AO).

The court, on the other hand, recognized an obligation to delete the

name, address and date of birth of the person concerned while at the

same time observing the receipt of the business correspondence to be

stored,

hence the information that would allow the person concerned to be

identified in the documents. In this respect, the person responsible

would have to check the legal basis for storing individual data contained

in documents

What should I do?

Even if there is a legal obligation

to retain data, the rights of those affected

bodies obliged to store the data are obliged to organize

their database in such a way that access to unlawfully

collected data of data subjects is not possible, for

must be taken into account as far as

possible with regard to (possible)

example by corresponding blacking out.

unlawful data collection.

Publisher

Saxon data protection officer Dr. Juliane

Hundred

Devrientstraße 5

01067 Dresden

Contact

PO Box 11 01 32, 01330 Dresden Phone

0351/85471-100 Fax 0351/85471-109

saechsdsb@slt.sachsen.de

www.datenschutz.sachsen.de

cover photo

© Tomasz Zajda/stock.adobe.com

Print

New Süddeutsche Verlagsdruckerei GmbH

Edition

1,500 copies

publication

May 2022

reference

free of charge

Central brochure dispatch of the Saxon state government

Hammerweg 30

01127 Dresden

Phone: +49 351 210-3671 / -3672

publikationen@sachsen.de

www.publikationen.sachsen.de

Distribution Note

This activity report is issued based on the obligation under Article 59 of the General Data Protection Regulation. It may not be used by political parties, their candidates or supporters for the purpose of election advertising. This applies to all elections. The distribution at election events, at information stands of the parties as well as the insertion, printing or sticking of party-political information or advertising material is particularly improper. It is also forbidden to pass it on to third parties for use in election advertising.