35. Data Protection Activity Report

of the state representative for the

Data protection and freedom of information

Baden-Wuerttemberg

2019

Released

by the state representative for the

Data protection and freedom of information

dr Stefan Brink

Koenigstrasse 10a, 70173 Stuttgart

Telephone 0711/615541-0

https://www.baden-wuerttemberg.datenschutz.de

Email: poststelle@lfdi.bwl.de

Twitter: https://www.twitter.com/lfdi_bw

PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Published as State Parliament Printed Paper No. 16/7777

Table of Contents

foreword

1. Priorities

1.1 From Baden-Württemberg to Europe -

LfDI evaluates the GDPR

1.2 Survey on the implementation of the GDPR

in the communal area

1.3 Data protection as a cultural task

1.4 Bodycam - Control visits at

police stations

1.5 Data Breaches in Medical Offices

1.6 E-mail advertising according to UWG - an exception in

narrow legal limits

1.7 The right to information under Article 15 paragraph 1

Letter c GDPR

1.8 Art. 15 GDPR in the context of employees

1.9 Technical and organizational data protection

1.10 More data protection also means more Europe!

1.11 News from the fine office

1.12 Bye Bye Twitter

2.

internal security

2.1. cell query

2.2 Eurodac

2.3 Abusive songs in the football stadium

2.4 Checking the implementation of communications from

Public Prosecutor's Office on the outcome of the case

3. Video Surveillance

3.1 Everything ready for the inspection? –

Video surveillance in gyms

3.2 Our daily bread - video surveillance in

bakeries

3.3 Legitimate Interests

3.4 Guidance on Video Surveillance

4. Traffic

4.1 Traffic

4.2 Authorities rely on postcards

4.3 Development of Artificial

Intelligence (AI) in the field

Traffic

3

7

7

10

11

17

20

23

25

26

28

36

40

42

47

47

48

49

52

56

56

57

58

59

63

63

63

64

1

LfDI BW - 35th activity report 2019 5th

justice

67

5.1 How do notaries fulfill their data protection laws

Information and documentation requirements?

67

5.2 Implementation of Directive (EU) 2016/680 in the field of justice 69

6. Municipal

6.1 The “List of Conspicuous Ones”

6.2 Community Network

privacy

7. Health and Welfare

7.1 Be careful when sending e-mails

7.2 Data protection in outpatient and inpatient care

7.3 The obligation to provide information in the event of collection

personal data of the data subject

by social service providers

8. School and colleges

8.1 Usage Regulations for Information Technology

at a school

8.2 Revision of the brochure

“Privacy in day-care centers”

8.3 Revision of the administrative regulation on the

Privacy in Public Schools

9. Privacy Policy

9.1 Temporary employment - processing on behalf?

9.2 Parking surveillance by private companies

9.3 Data Protection Liability

9.4 Data protection in property management

9.5 Data protection in the banking industry

9.6 Consent texts and data protection information using the example

raffle tickets and sweepstakes

on websites

9.7 On the High Seas

9.8 News from the field of international data traffic

10. From the office

10.1 From the office

10.2 Press and Public Relations

Information about the service

73

73

74

77

77

77

81

87

87

89

90

95

95

96

97

99

101

106

108

109

113

113

115

121

Appendix

2

from 123

LfDI BW - 35th Activity Report 2019 Foreword

2019 – #GDPR works!

In terms of data protection, things are going uphill

Schlag: After the all-outshine

Deadline May 25, 2018 and the advisory

marathon of the first year of EU data

General Protection Regulation (GDPR).

we already have the 2nd activity report

according to the new European legal

gimme before.

Since 2018, the GDPR has been in force throughout

EU directly applicable data protection

right, and it bestowed on data protection

an unprecedented attention

resulting in a flood of inputs, requests

and complaints, in numerous inquiries

after consultation, after training and

tion reflected as well as in one

unusually large media interest.

Our experience in 2019: It lets

not after! The GDPR has arrived –

and she won't go away!

The number of complaints remains high

level that take advice requests

by no means off, and also the public

Interest continues unabated. For us

there is no doubt: the GDPR works.

It works through its clear, free

friendly regulations of information,

Correction and deletion claims

Citizens, through clear (and

often complex) announcements to the

Those responsible (i.e. companies and

Authorities that process personal data

ten) and last but not least by very massive

threats of fines.

Another finding from the past

genen year: We are now

one of the best equipped data

protection supervisory authorities in Germany

(and Europe) – but we can't all-

les: Advice and control work

really good on its own –

but not at the same time. We can - and

We proved that in 2018

provided - advised, we can also - that

we have with our wide-ranging

Control actions of the year 2019 shown –

also effective and controlled with a sense of proportion

ly. But both at the same time is (still) possible

Not. We have enough staff for that

despite the really high personal

don't put off my colleagues. What

about has meant that we will in 2019 willy-nilly

voluns our consulting services

back somewhat in favor of the control density

had to drive. And that the waiting times

in the case of submissions by citizens

are still too long.

Our core tasks (advising citizens

and citizens as so-called

met” or as for data processing

"Responsible" in companies, authorities

and associations/enlightenment and

raising public awareness on issues

of data protection/regulatory authorities

enforcement of data protection law

Test measures and sanctions)

the 2019 supplemented by the “European

dimension” of the new law: as part of a

ner European data protection administration

we coordinate with 48 other

supervisory authorities – the administrative culture

structure and assertiveness

but "tick" clearly differently than we do. Of the

Process towards a uniform acting

European data protection supervision

certainly still several years to go

take. But he is, as the saying goes,

without alternative. As an authority we are in Eu-

arrived and have a

taken a pleasant place: As

German representative in the influential

Social Media Group of the European Data

data protection committee, as rapporteur

and as a conversation partner for international

active companies and media.

The focus of our activities was and

the consulting work continues: In

thousands of one-on-one conversations,

current events and seminars,

by means of dozens of orientation aids in

our ever-expanding internet

net appearance ("hit" is still ours

Practical guide "Data protection in the association")

or via Twitter, where we have more than 5,000

Followers from the privacy community

millions of citizens

Privacy information reached. There-

but that's the end of it now: the through

the European Court of Justice and lastly

by the Federal Administrative Court

clearly confirmed legal situation does not allow it

more to, as a data protection supervisory authority

de active part of a social media platform

to be having quite significant doubts

with regard to their data protection compliance

are exposed. That's a shame, because the

lively communication also on this

this level was exciting and fruitful,

but we have to be consistent – and

make every effort that way

good and constructive communication

legally compliant and independent others

switch channels. It is also clear: The

new legislation will also have consequences for the

Presence of public and non-public

Have jobs on social media. Like it

running now, it can not stay. we will

to push the dialogue here further and

for good (at least acceptable) solutions

search for Ultimately, there is the GDPR

here, too, the direction is clear.

"If it's not reasonable, then it is

no data protection!” We have this motto

also taken to heart in 2019, for example with the

monies where we build our reputation as a regulatory

authority quickly, constructively, but also

to act consistently.

But we don't have eyes for it either

closed that the GDPR as a legal

not norm in all areas of wisdom

the final conclusion is - and have decisive

for the German Data Protection Conference

renz DSK, but also in the "Ländle" with everyone

affected actors from the trades

the middle class to science

and authorities in evaluating the DS

GMO worked. The GDPR itself

has to get better.

Looking at staff development

can be said: The occupation of our

vacancies were not a problem,

even in the highly competitive area of

not. The LfDI can obviously

an attractive task and a good one

Build reputation, we are also for colleagues

from the administration of the country, for inter-

Essents from other German

supervisory authorities and also for

lige from the private sector obviously

a job with attraction. There

strengthens us now in turn from Parliament

ment decided, in a federal comparison

uniquely good increase in staff

in an excellent way. We're off

2020 a training and further education center

trum of data protection and information

build freedom of operation and our benefit

for the citizens, but also

companies, companies and authorities

further expand the country.

Ultimately, however, data protection is not (only)

made by the supervisory authority, otherwise

by the citizens

perceived (or not) and

by the responsible bodies in

companies and administrations more or

lived less convincingly. What

We as those affected and measure interpretation

holder of fundamental rights

future ours

Right to informational self-

 Are we just willing con-

sumenten, which amenities and

“Being there” seems more important than that

Opportunity to enter the digital age in a self-determined

age to step? A basic right without

bearer of fundamental rights, its substance

also appreciate, has no future –

not even with a European DS

GMO.

The ongoing momentum of the GDPR

we continue to take op-

timistically - the basics for our

more confidence can be found in this

activity report. Thanks again

all my employees

bitern with my deputy mr

Broo at the top for her amazing work that

goes far beyond what can be expected - we

Data protectionists are just "conviction

perpetrator". I can thank this one

But also with the members of the

State Parliament of Baden-Württemberg, which

This task will also be decisive in 2019

designed, accompanied and promoted

and with the state government and administration

and the local authorities for always being fair

and largely consensual

work.

Your country representative

dr Stefan Brink

1.1 From Baden-Württemberg to Europe - LfDI evaluates the DS GMO

The year 2019 was also under for us

the sign of the evaluation of the GDPR.

According to Art. 97 DS-GVO, by May 25th

2020, i.e. two years after it came into force

of the GDPR, this of the European

be evaluated by the Commission. To this

Purposes can use it by Member States

and the regulatory authorities information

request.

1.1.1 Field report of the independent

data protection supervisory authorities

Federal and the states

The Conference of Independent Data

protection supervisory authorities of the countries and

of the Federal Government (Data Protection Conference - DSK)

has established itself as a body for all German

ten protection supervisory authorities

prepared by a working group

has used, the feedback of all

to coordinate supervisory authorities

into a unified report

grasp. The chair of this working group

ums was awarded by the LfDI Baden-Württemberg

accepted.

From the beginning of the year to the

decision of the report by the DSK in

November we have five in collaboration

other supervisory authorities in total

five days of meetings and constant coordination

planning work and taking into account

tion of the resolution of the DSK and their

working groups drafted a report

who first manufactures the principle work

working group and then the DSK itself

ted. On November 06, 2019, the

98. DSK the experience coordinated by us

ment report approved. The report

is on the homepage of the DSK and the

LfDI Baden-Württemberg in German and

available in English and was

by the DSK chair to the European

Data Protection Committee (EDPB).

In addition to those required by law in the event of a

Evaluation request by the Commission

specified topics of Art. 97 paragraph 2

GDPR, the focus was on any changes

change due to the application

experiences in the first year. This

both in relation to existing regulations

as well as to the possibly necessary

agile creation of further regulations.

Also the recitals of the GDPR

were included in the considerations

gen. The issue of dealing with any

Problems with the implementation of the GDPR

in federal and state law has not been incorporated into

included the DSK report. This

happened to the knowledge of the DSK by a

Query by the Commission with the national

interior ministries. According to the

LfDI can arise from problematic national

nal implementation standards, however

Need for changes to opening clauses

DS-GVO itself arise.

Significant results of the DSK were published in

dealt with the following main topics:

In the information and transparency

obligations according to Art. 13 and 14 DS-GVO ha-

there are implementation problems in practice

shown, e.g. B. in the case of telephone data collection

exercise. This is particularly about the

question whether first a more general in-

formation at a central location is sufficient and

specific information only upon request

can be submitted later. also

beginning and content of the information requirements

could possibly be more workable and

be defined in a more citizen-friendly way. In the

LfDI BW - 35th Activity Report 2019 - 1. Focuses In practice, the question sometimes arises

the suitability for everyday use of the regulations of

GDPR. ways to facilitate

Application of the information requirements

Obligation to report data protection

mandated to the regulators as well

the right to a copy under Article 15 paragraph 3

GDPR came into focus.

A widespread concern about the

Possibilities of sanctions of the DS-GVO

based on the experience of regulators

led to many data breaches being reported

which actually have no data at all

ten breakdowns are or their risks already

have long since been eliminated. Therefore were

exorbitant rates of increase in the

to record data breaches.

The DSK has already come up with possible solutions

dealt with.

In the area of earmarking,

in practice mainly questions regarding

on the legal basis and the

stipulations of the further use of the per-

personal data when changing the purpose

result.

Data protection by design can be found in the

Hardly any resonance in practice, since the user

scope of the DS-GVO manufacturers

just not recorded. The GDPR provides

but data protection by design by default

Principles on that are in the matter though

addressed to manufacturers, but accepts them

not as responsible in the duty. There-

here the question is raised whether also

Manufacturers, suppliers, importers and

sellers are held accountable

should, as in product liability law

is already the case.

In the main topic “Powers of

Supervisory authorities and sanctions practice"

have questions about that in particular

concept of "processing".

Art. 58 paragraph 2 lit. b GDPR and the

cooperation and the right to information

of the supervisory authorities in the fine proceedings

ren proved to be particularly urgent. in a

nem further in Art. 97 paragraph 2 lit. b DS-

GMO listed priority

the experiences of the supervisory authorities

with the topics "determination of

ments, cooperation and coherence”

shown.

In the case of direct advertising,

different constellations the question of

Admissibility, which through the creation

a specific legal basis

could become.

One of the central data protection policy

That is the challenge of our time

profiling. Despite the existing definition of

nition becomes the process of profiling

as such by most norms of the

DS-GVO - for example for automated development

divorce finding - not recorded, so

an assessment usually only according to the general

my facts of Art. 6 DS-GVO

he follows. The DSK calls for a tightening

of the applicable legal framework

the use of personal data

Effective and profiling purposes

to set actually enforceable limits.

With the focus on accreditation

te through a clarification in the GDPR

a significant national responsibility

question clarified and oversight by the

German data protection supervisory authorities

be ensured.

On the current dominant topic in

the scientific debate

tion, the issue of data protection in

field of artificial intelligence and

automated

decision-making

ren, the DSK also sent theirs

"Hambach Declaration on Artificial In-

8th

Requirements" from April 3, 2019 to the

EDSA. Although the requirements contained

are primarily based on future cases

and refer to norm constellations

the German data protection supervisory authorities

the observance of these principles in

the future evaluation processes

considered essential.

1.1.2 Contribution to the evaluation of the LfDI

Baden-Wuerttemberg

Since May 25, 2018, the state

commissioned for data protection and the

Freedom of information Baden-Württemberg

legally obliged to comply

implementation of the GDPR in Baden-Württemberg

to supervise and be responsible

chen in the country to advise. For evaluation

the DS-GVO I would therefore also like to say

Assessments based on the previous

practical experience of my independent

result from the supreme state authority,

the European Commission for information

bring nothing.

Not only from the knowledge which

almost a year as chairman of the

working group for the German evaluation

give, but above all from the innumerable

timely feedback, which the LfDI

from the country - be it for

events, training courses or directly

We have exchanges with those responsible

own contribution to the evaluation

is working.

Because the circle of those responsible in

Baden-Württemberg is with the federal

average only partially comparable.

According to the Ministry of Economy and Finance

zen Baden-Württemberg

small and medium-sized businesses each

second euro turnover in the country and

two-thirds of social security

compulsory employees. The middle class

is thus the backbone of the economy in

Baden-Wuerttemberg. Also dedicated
to a report by the Ministry of
cial and integration Baden-Württemberg
According to almost every second Baden-Württemberg
berger in his spare time on a voluntary basis (over
48 percent). That makes us the front runner.
Baden-Württemberg is both a state of
voluntary work as well as entrepreneurial
intellectual and thus has its own, specific
Challenges and concerns of one
practical data protection.
In order to share the experiences of those responsible
chen and users of the DS-GVO in
Baden-Württemberg to take into account
we have one on June 28, 2019
Hearing under the banner "#DS-GVO
works (?) - 1 year DS-GVO - practical experience
ments and evaluation" in collabora-
work with and on the premises of
Chamber of Industry and Commerce Region
organized in Stuttgart. For impulse lectures
Representatives were invited
Supervision, authorities, business, science
society, legal profession, associations and
processors. In a dedicated to this
configured e-mail inbox were also

In addition, letters throughout the year

collected from all parts of the country

and evaluated. These country-specific

In addition to experience, knowledge

ment report of the DSK a contribution to

Evaluation of the GDPR by the European

ic legislature.

Overall, it has been shown that the

responsible in Baden-Württemberg itself

solutions that are more suitable for everyday use in many areas

ments and some regulations

hard on data processing

activities of small companies or

official work. in the

Questions about

to a possible relief for the domestic

information, transparency and information

to obligations to create processing

directories and naming

by data protection officers, as well

the introduction and supervision of a

liability as well as ambiguities in the

joint responsibility, in particular

others in the "social media" area.

Despite numerous samples and practical advice

About my and other regulators

still appears to be a significant legal

uncertainty among those responsible

to be at hand. have contrary to expectations

worried about sanctions – at least

below our practice – not as a priority

exposed. This may not least

to lie that we are in Baden-Württemberg

have repeatedly made it clear that it is

we care that those responsible

on the way to a data protection

have made compliant processing.

About 75% of the companies gave way

DIHK survey indicates that the GDPR (to

at least partially) implemented

to have. My experiences with it are in

Overall congruent.

The data protection supervisory authority in Baden-Württemberg is based on the motto “If it's not useful, it's not data-protection". Under this objective should also our report that we sent to the EDPB the, to be understood.

1.2 Survey on the implementation of the DS GMOs in the municipal sector

The municipalities in Baden-Württemberg
are as responsible public bodies
to a large extent with the implementation
tion of the new requirements from the
General Data Protection Regulation
takes. In order to continue to provide adequate
services in the municipal sector
provide, requires my office in
reliable and
comprehensive information as well the
Cities and municipalities in the country their work
already adapted to the new requirements
fit and where they still need to improve
have to.
Against this background, the summer
2019 a comprehensive questionnaire
all 1101 Baden-Württemberg com-
munen sent, the implementation
status of the new data protection law
asked. The municipal administrations
an online catalog with 50 questions
lays out the most important areas of the new
en data protection law had as its content.
The communities received an email
individual participation link and had in
the questionnaire also the possibility

to give individual answers. in the

968 municipalities (around 87%) have the result

took part in the survey.

12% of communities have defied

multiple requests not involved,

among them, 6% never have the survey link

called.

The evaluation of the survey clearly shows

that the communities as a whole get through

the requirements of the General Data Protection

regulation feel heavily burdened. to it

to clarify with an example: Dem

Processing directory of the responsible

there is one in data protection

central importance to. But almost one

Third of the communities have not yet

started setting one up. The-

So far, these communities have not

Overview of the processing activity

in their area of responsibility.

More than half of the congregations gave

indicate that there are problems creating a

there is a processing directory.

Simultaneously with the evaluation of the survey

ge my office has a brochure

for the Baden-Württemberg municipalities

expressed need for advice

picks up and a further orientation in

to provide municipal data protection.

The evaluation, the press release and

like the brochure "Data protection at

think" can be accessed here.

is working,

Key Results of the Survey:

LfDI and Ge

The communication

mean

the cooperation

is pleasingly high.

operational readiness

The municipalities are ready and willing

lig, the

"Challenge DS

GVO", but there is a lack of know-how

How, staff and support –

especially in small communities.

The status achieved so far in terms of

Data protection and data security is in many

areas insufficient.

1.3 Data protection as a cultural task

What associations do citizens and

Citizens if they are attached to any

authority think?

And, to go one step further

hen:

What associations arise when

they think of an authority whose

Main task is to become familiar with the topic

to deal with data protection?

Whether the citizen or the citizen to do so

probably an evening with sinologists to

menfeld China, an evening with the

Federal Ministry of Justice and Consumer Protection

nister dr. Katarina Barley or even the

Production of a music video that

dancing state representatives present

animals?

All this is just a small excerpt of-

see what I've done this year.

At the beginning of the year I

together with the Viennese singer Daniela

Flickentanz (yes, that's her real name), the

Stuttgart Media University, and some

of my employees

ter a music video on the subject of data protection

produced. From the first contact

me up to the day of shooting were pretty accurate

four weeks - and these four weeks has

quite a bit.

But we made it, mid-February

ar 2019 was the jointly developed

screenplay, the song lyrics were adjusted,

the stage directions ready, all

Props organized and last but not least

Daniela Flickentanz from Vienna to Stuttgart

arrived.

So it could start...

 The result was data protection of the whole

other kind...

to catch. You can also open this evening

track youtube.

Our music video not only

sang and danced, no this video there

- I think - in a humorous and a-

common way recommendations for action

on the subject of data protection - so to speak

swinging how-to.

Which authority can

main, their legal advisory

commissioned in the form of a music video

to become…!?

You can find our music video on our

website or on YouTube.

My special thanks go to Daniela

Flickentanz and the highly professional

Team of the Media University, Stuttgart

and of course my experimental

happy employees. I'm still

excited about what we create together

to have!

With that we are right at the beginning of the

res boarded with an attraction – and

that wasn't the only attraction of the

year 2019!

In March I was able to

Minister of Justice and Consumer Protection

dr Bring Katarina Barley to Stuttgart.

Together with our proven co-

operations partner, University of Media,

Stuttgart, we met as part of a

Panel discussion on the topic:

#Doxxing #data theft #digital ethics

Our digital life – no alternative?!

dealt with. the event

was fully booked, even the additional

chen standing room could the rush and

the enthusiasm of the audience

In May we set out for that

Made the Middle Kingdom - of course only

virtual and acoustic.

CHINA -

Empire, Terracotta Warriors, Chinese

Wall, Ming Dynasty, Chinese Script

sign, the forbidden city, buddhism,

Chinese tea, silk, Beijing opera, …

Who does not start with all these terms

dream of...

However, the modern popular

public China not only about this historical

cal and cultural goods. The current

developments in the Middle Kingdom

no more reason to dream - completely

on the contrary... they exhibit dystopian

trains up. The country has a social credit

or social scoring system introduced,

based on a reward or punishment

system based. The population

holds bonus points for behavior that

positive from a state perspective

is. This includes, for example, caring for

the parents. Conversely, if

desired behavior Malus points in de-

brought train. Even the disregard

a red traffic light gives rise

to reduce the individual points contingent

adorn. Provided a certain minimum amount

is undercut at points, reacts

the state with reprisals such as

Access to study or training places

zen, use of flights and trains, ...

And not just for the polluter –

the reprisals can affect all families

lien members extend.

All this goes hand in hand with extensive technical

nical surveillance paired with social

and “friends”… There is no question that

dealing with someone who is in debt

has and whose points account rather in the

is located in the lower regions, also

negative effects on one's own

cial status and thus also on the

can have an existence. The consequence of this

means for those affected and their families

s, possibly in addition to the already mentioned

ten reprisals, social isolation.

These developments offer for me as

Freedom guards cause for great concern.

It was therefore important to me to

to inform developments competently and

with interested parties and experts

facts and related issues

to critically examine the effects and

to discuss. In May 2019 I have to

entered the Church of St. Maria in Stuttgart

load.

Under the motto “China – the country behind

the smile” first granted us Ms

dr Ricarda Daberkow from the Linden Museum

in the historical development of a

thousand-year-old culture insight. After a

After a short break, Dr. Ma

reike Ohlberg from the Mercator Institute for

China Studies (MERICS) in the People's

Republic of China already practiced Social

Scoring and its implications for the

individuals in everyday life.

The extent to which state surveillance

already now in the Middle Kingdom

includes, could not reach any of the listeners

pass by without a trace. All the more since that

still dormant potential immeasurable

other monitoring options

offers that of a complete synchronization

and thus the abolition of any

home sphere.

China

The land behind the smile

Introduction: China - Country, People & Culture

Sinologist Mrs. Dr. Ricarda Daberkow

The Digital Big Brother? Citizen Rating in China's Social Credit System.

Sinologist Mrs. Dr. Mareike Ohlberg

Small Chinese specialties are offered during the break.

Admission free.

May 16, 2019 at 7:30 p.m

Church of St. Mary

Tübinger Strasse 36, 70178 Stuttgart

The lectures of the two sinologists and

also the subsequent discussion at the

fet with small Chinese delicacies

have made it clear that freedom in

every form is a good that is not at all high

can be appreciated enough. However

also became clear that all these

is not a matter of course, but

that each of us contributes every day

gen to maintain this freedom and to

receive.

I remembered a little one evening in the

felt reminded last fall. At this

evening I have together with the Stutt-

garter inner-city cinemas, the Hollywood mo-

presented as "THE CIRCLE". This ba-

based on the idea that

only the person who is constantly observing

attention is aware, behaves correctly. What

in a person who is unobserved

tet believes is not always guaranteed.

The price for this is called PRIVACY!

 Shocked everyone who thinks critically

Man this approach far from himself. That

The Middle Kingdom does not seem to take this approach

only taken over, but consistently

to have developed.

In September 2019 I managed one

Panel discussion with representatives

of the Enquete Commission "Artificial In-

intelligence" of the German Bundestag

present. I have this in common

with the state representative of Rhein-

state-Palatinate, Prof. Dieter Kugelmann,

to the Ernst Bloch Center in Ludwigs-

port, invited.

One of the big buzzwords of the year

2019 was "Artificial Intelligence". in the

April 2019 my colleagues and

I at the 97th Conference of Independent

gigantic data protection supervisory authorities

federal and state (DSK) the "Hamba

cher declaration on artificial intelligence”

developed and approved.

He's been dreaming for centuries

man from the artificially created, in

higher intelligence human-like machines

nature. For that there is in the literature

and history many prominent

ker, researcher and inventor. The Greek

Forge god Hephaestus, Leonardo da

Vinci and Mary Shelley's Frankenstein

en only mentioned here as an example.

With the complex of topics Artificial Intel

intelligence (AI) are not just hope

connected - but also many

fears and existential concerns.

In the medium term there will be almost no life

Give more to the practice area, not to the AI

will have an impact. Is the use of

artificial intelligence already today

te spread more widely than many of us

let dream ...

The evening in Ludwigshafen was

thought the invited speakers

to leave the podium to their expertise.

Three members of the Commission of Inquiry

on "Artificial Intelligence - Society-

social responsibility and economic,

social and ecological potentials".

German Bundestag, Dr. Petra custom

(The Left), Dr. Anna Christmann (Federal

nis 90/The Greens), the experts

Lena-Sophie Müller from the D21 initiative

and Professor Doris Aschenbrenner

from Delft University of Technology (NL)

offered insight into their work and the associated

related social issues.

Following the panel discussion-

the questions and statements of the

likums made it clear again how

already a matter of course in many areas

is used and which con-

result.

the numerous contained in the lecture

transported in short video clips.

Ultimately, a significant

point again and again. the zen

The central question is no longer: “What

is technically possible?" but "What

we as a society - in which direc-

do we want to develop?”.

There is no question that this all-encompassing

don't send questions in one evening

can be answered. But the evening

was a good start most diverse

social groups together

bring and talk to each other

come.

It's never too early to appreciate the value of private

sphere to draw attention and that

applies in particular to children and adolescents

che. Together with cooperation partners

I take this topic with great

joy every year. with a

gene of the cooperation partners is one

annually recurring and ongoing

cooperation emerged.

I support the initiative "Data

protection goes to school” of the professional association

of the data protection officer German

lands (BvD) e. V. not only, I build these

together with my co-workers and

employees actively. For that I have

my colleagues of the

their data protection supervisory authorities

a joint action across the

invited across borders. The countries-

overarching agreement and coordination

tion was in Baden-Württemberg.

The initiative "Data protection goes to

le" sensitizes students

to a conscious handling of the

ternet and social media. Especially

entertaining and above all clear

through the abstract topic of "data protection".

On the occasion of Safer Internet Day on 5.

February 2019 we have various campaigns

days in different cities and schools

len Baden-Württemberg offered and

carried out. The events offered

for young people the opportunity, for example

Limits of Big Data, Smart Home and

also the use and data transfer

when using messenger services

the price of disclosing private information

information and data to be viewed critically

ten. Convenience versus privacy

became a big issue. Clearly

was also that free offers

should be vigorously questioned.

Is the messenger offered free of charge

service really free? From which

reason many companies offer customers

thinking cards and associated discounts

and loyalty bonuses? Fast became for

the students realized that in

the present time no company something

has to give away.

I was particularly impressed by the

tered feedback from young people,

of the teachers, the school

management and the lecturers

centers of the respective supervisory authorities

as well as the press echo in the regional

newspapers happy. do all this

yet clearly how important and meaningful it is

is, children and young people in dealing with

their personal data on the Internet

net and what challenges

Demand it also represents this topic

with a word appropriate to the target group

to explain sweetheart.

net services for data protection sensitive

and support with tools? Included

the teams developed some demanding

le software solutions to raise awareness

the user, for training purposes

subject of self-data protection and

support of companies in the implementation

compliance with data protection regulations

at the end of the semester by a jury,

in which also one of my employees

is represented.

https://www.dhbw-stuttgart.de/themen/

university/registration/2019/02/study-

de-develop-solutions-for-the-data-

protection/

A continuation of the cooperation between

the Baden-Württemberg Cooperative State University

berg and my authority is already with

again in the winter semester 2019/2020

started.

At the end of a year with many

highlights and attractions

I te again in October 2019

the data protection autumn conference

as

present patron. organizer

this symposium is the professional association
the data protection officer German
lands (BvD) e.V.. The patronage
I got mine this time with my two
Bavarian colleague Thomas Kranig, President
sident of the Bavarian State Office for
Data Protection Supervision, and Prof. Dr. tho
mas Petri, Bavarian state representative
for privacy, shared. As already in the
last two years stood the first
two days under the motto “Economy
meets supervision".
The third day of the event offered like-
the one special. under the mot
to (supervisory) authority helps authority –
Source: published in the Rhein-Neckar-
Newspaper of February 6, 2019, Photograph:
Helmut Pfeiffer
Specifically, in Baden-Württemberg alone
temberg a total of around 600 students and
Schoolgirls in Stuttgart, Esslingen, Dit-
zingen, Walldorf, Bad Friedrichshall, Lud-
wigsburg, Ettlingen, Lorch and Pforzheim
with the joint and transnational
pending action of the supervisory authorities in
Cooperation with the BvD achieved.

However, it also became clear that the

allowed in schools is much, much higher than

we could satisfy with our action-

ten.

Summary of our international activi-

on:

We will continue!

More information about the initiative

Privacy goes to school, see

the website of the BvD.

We have also been able to do this since 2017

existing cooperation with Dualen

University of Baden-Württemberg successful

continue rich.

Under the guidance of Professor Dr.

Tobias Straub, Michael Schlegel and Ivan

na Marevic developed a total of eight

student teams applications too

we have specifically focused on the circle of authorities

specialist lectures tailored to the

ge and discussions offered.

For the year 2019 I had the motto:

Go on!

Looking back I can say -

Source: BvD e.V. / Uli Schneider

The autumn data protection conference offers
Lectures, discussions, expert
talks, guidelines for action, examples
from practice for everyone who is familiar with the
ma data protection are concerned. The formats
“Economy meets supervision” and also “(super-
supervisory authority helps authority" are federal
therefore unique and offer the possibility
bility topics, questions and problems directly
with experts and representatives of
to be able to discuss with supervisory authorities.
The response to our event is
enormous. With around 300 participants
nationwide it is the current am
most frequented event
topic of data protection. In this
Year was most of the places already
fully booked before the event
gram was published.
All this makes it clear that the subject
Privacy and the exchange between
representatives of entrepreneurs and authorities
no longer away with the supervisory authority
is to think about!
So in autumn 2020 we will also be the

Continue data protection autumn conference.

that has proven itself -

So I'm staying for the year 2020-

at!

Go on!

1.4 Bodycam - Control visits at

police stations

The Police Act has been in place for a good three years

of the country a legal basis for the

Use of bodycams in patrol duty

the police. After the procurement

suitable devices for some time

has moved, these are now in the

Area largely arrived and in

Mission. Reason enough to practice the

take a closer look at the application.

Our experiences from visiting more

other police stations were mixed:

From the point of view of data protection, the

technical and organizational measures

took no cause for criticism. every butt

lizeirevier has its own devices, each one

Police station locally stores its own

Recordings without third parties, including others

organizational units of the police headquarters

Umm, be able to access it. The roles

are clearly assigned, the processes

structured and transparent. This overall

extremely positive picture was unfortunately tarnished,

as we randomly selected film

show recordings.

To do this, you have to preface that

Police Act sets out clear rules as to when

this technique can be used. It

 A distinction must be made between focal points: come the police

civil servants within the framework of their

patrol service in potentially dangerous

che situations, the first stage of the

Bodycam, the so-called pre-recording,

be set in motion. Vi-

deo sequences with a length of 60

customers in a loop.

That is, the camera draws continuously

always only a total of one minute of

happening on. Visually, this functional

art visible on the camera, always being

it is also pointed out verbally

that a recording is made. Has the-

this low-threshold measure

wanted de-escalating effect, must

the camera can be switched off again

and the recording will start automatically

deletes.

If the desired success does not occur, it can

the permanent one by pressing the button again

Recording and storage of the

hens to be activated. In addition to the last

60 seconds is then saved for

until the camera is switched off again

will be This type of function is also op-

table made visible. However, the

legal hurdle for such permanent

Recordings high: it must be the facts

justify the assumption that the spoke

protection of police officers or

third parties against danger to life and limb

be required. Consequently, recording

men about administrative offenses or

Insults are strictly prohibited.

Recordings are also not permitted

Places that are not open to the public.

During visits by a total of three police

Fourth, a series of bodycam recordings

took a look at. Far

mostly it was situational

tion, which may be physical

attacks had preceded it. for the time-

point and in the course of the recordings

however, these have been completed in any case

and nothing indicated that by

the persons concerned specifically further

Attacks would go out or go out

could. The following examples:

In one case it was a blood draw

me: the person concerned was sitting on one

Chair and discussed with the doctor and

the officials. The blood was taken

te without resistance. In two cases

the only administrative offences

documented: once it was about "wild

pinkler", on the other hand a verbose one

confrontation with a car

rer, who apparently didn't wear the seat belt

had created, but none of them

aggressiveness went out. In another

case a dismissal was documented,

whereby it was filmed how an official in

appropriate distance to the person concerned

son this about several minutes walk

followed. Often were the cases in which

the person concerned already on the

back-tied hands motion-

lying incapacitated on the floor; in one case

officers knelt on the backs of the

met, in the other case he was lying on his back

on the floor of a police vehicle. In

in another case the person sat with

seat belt on the back

seat of an emergency vehicle, had the co-

ne relaxed over each other and

expressed himself (correspondingly) to the effect that

to endure everything else.

In almost none of us in sight

recordings taken we saw those

legal requirements for the

dycam use, as specified in Section 21 Paragraph 6

of the Police Act (PolG) are regulated,

as fulfilled. From this it can be concluded that

many police officers of

apparently not known or at least not

present is that bodycams don't do that

are intended, any police relevant

the legal hurdle for the use of the

body cams is relatively high. the

Video documentation of police operations

using bodycam can not on a

criminal procedural legal basis

will. The prerequisites for this

only to be considered § 100h of

Code of Criminal Procedure

lie regularly

not before.

In addition, the following arises

Problem: Some of the recordings

men inside police vehicles or

in service buildings. The wording of the

law restricts the use of body

cams, on the other hand, on police measures

"in public places". In the

relevant instructions Bodycam

it says: "This means places that actually

are essentially accessible to everyone,

such as B. streets, paths, squares, shop

passages and public transport areas". so

police station buildings and police

emergency vehicles hardly as public

accessible places in this sense apply.

Formally, bodycams are also allowed there afterwards

are not used, although

Background for the legal regulation

actually guaranteeing the basic

legally protected inviolability

Apartment (Article 13 GG) was what was on the

actually not mentioned premises

applies.

A third point, cause for criticism

there is the practical implementation of the

cancellation policy.

bodycam recording

after they have been saved

assigned to different categories,

ever

depending on the purpose for which they

are to be processed. Especially

is it about the use in a

a criminal proceeding or a proceeding

about administrative offences. Besides there

there are still the categories “Protection of private

Third party rights”, which according to match-

not relevant in practice

plays, and "no relevance". In particular-

re regarding the latter category

the law provides that the recordings

“immediately, but no later than four

weeks” are to be deleted. practical

these recordings generally four weeks

stored for a long time, which is partly because

is justified with, one wants the

Give those affected the opportunity to

assert a right to information.

In principle, this is to be welcomed.

Nevertheless, this practice leads to a

reversal of the legislative will, the

the immediate deletion ("immediately") as

rule and the longer saving ("later

testing") as an exception,

where there is one in each individual case

justification required.

In conclusion we come to the following:

Those responsible are obliged to

the police officers

officiate not only once, but re-

gelatinous, if necessary

as part of

of operational training,

in the lawful

Training in how to use the bodycam.

Task of the local data protection officer

carried is to take bodycam recordings

to be checked moderately and to intervene

fen if it is found that legal

conditions were not observed.

The use of bodycams in police

buildings and police vehicles

not permitted under the current legal situation.

The implementation

the storage periods

in practice is to be critically reviewed

fen and by internal regulations

to limit the permissible level.

 Our visits and the gained

knowledge was spoken in the Po-

lick around quickly. As a result, it happened

a meeting with the Ministry of the Interior/

State Police Headquarters. That cleared it up

Interior Ministry one that the police

Practice of camera use, at least in

the cases examined by us, even after

local opinion not the legal

have met the requirements. It was

de a work-up promised,

the result of which we get after a short time

enough. In it, the state police informed us

zeipräsidium with that one extensive

Control measures to ensure

of a legally compliant camera

have caused sentences. That's how you have them

heads of local police headquarters

package of measures obliges the

includes: Clarified again

was that the Code of Criminal Procedure was not

quasi through the back door as a legal basis

position for a sole evidence-preserving deposit

set of bodycams can be used

can; this was already in the corresponding

the service instruction so specified

but probably not always in practice

so understood. Furthermore, the

prompt deletion of recordings in the

Cases where this is not for further

criminal procedural purposes or for purposes

the prosecution of regulatory offences

are needed arranged. With that

te the routine use of the four

week maximum storage period hopefully

belong to the past. In addition to

ner improved documentation and

Control obligation was determined that the

Use of bodycams in office buildings

and company vehicles are not permitted.

Overall, the reaction of the police

guide to our exam results

therefore constructive and goal-oriented. Anew

has been shown that trusting relationships

cooperation between the police

den-Württemberg and my office

tangible results on a regular basis

Sense of a legally compliant handling

with personal data of citizens

and citizens.

1.5 Data Breaches in Medical Offices

A variety of also 2019 at my

data breach report sent to the department

ments concerned medical practices from Baden-Würt-

temberg. An internal evaluation of such

Reports revealed that in a top 7 list

of the most common causes of reported pan-

the wrong postal service ran to number 1

greed, the e-mail misdelivery in 3rd place,

sending an email with an open

address list in 5th place and the fax

misdelivery in 7th place. The fact that

due to incorrect dispatch of doctor's letters, prescription

or X-ray images, often also particularly

the sensitive and worthy of protection health

patient data into the wrong ones

Hands advised gave special occasion to

thorough study of this topic.

Data breaches in which medical practices

from cyber attacks (2nd place)

the top 7 list), are the subject of the

trags "technical-organizational data

protection" under number 1.9 of this activity

performance report.

In force since May 25, 2018

che General Data Protection Regulation of the EU

(DS-GVO) regulates in Article 33

sentence 1 sentence 1, under which conditions

a data breach is reported

got to:

"In the event of a breach of protection

of personal data reports the

answer promptly and as possible

within 72 hours after the

became known last, this according to

Article 55 competent supervisory authority

de, unless the violation of the

not likely to pose a risk to the

Rights and freedoms of natural persons

leads."

reports not required by law,

at least from the point of view of my department

le, not connected: Better a message

too much than one too little.

So the key requirement is

for such a report a “violation

of personal data protection”.

It follows what is meant by this

from Article 4 No. 12 GDPR:

A “breach of security leading to

destruction, loss or alteration

change, whether unintentional or unlawful

moderate, or to unauthorized disclosure

from or to the unauthorized access

leads to personal data,

which is transmitted, stored or otherwise

have been processed".

The reporting obligation under Article 33 paragraph 1

Sentence 1 DS-GVO is therefore broad.

Albeit the Baden-Württemberg ones

Physicians this far-reaching

recognize and fulfill the reporting obligation,

is this gratifying. clues for one

high number of unreported cases

cases I have - unlike my official

predecessor under the application of § 42a

of the Federal Data Protection Act in the

old, valid until May 24, 2018

Version - not (cf. the 32nd activity

Report of the state representative for the

Data protection Baden-Württemberg for the

years 2014/2015, contribution no. 7.10 information

obligation to notify in the event of data protection violations,

Printed matter 15/7990 of the state parliament of Ba-

den-Württemberg of January 21, 2016, p.

129 ff., on the website of my service

position available). On the contrary, they are

non-reportable cases to my office

been reported, for example,

that a patient owns a part

Documents in the waiting room of the practice

left behind.

Serious problems are with such

If a data breach - regrettably -

wise – has occurred and reported

I'm particularly concerned there-

rum that comparable things in the future

the will. According to Article 33 paragraph 3 book

stabe d DS-GVO, the notification must be sent

my office "a description of the of the

taken or proposed

proposed remedial measures

violation of the protection of personal

data and, if necessary, measurements

took to mitigate their possible

adverse effects". There-

can be found in the one from my office

offered – and for use here as well

expressly recommended – form for

Online reports of such breakdowns, e.g.

the question "What countermeasures

have you already initiated which further

countermeasures are planned?”

a generous free text

field. In the event of a fax error,

sands can be entered, for example,

that the recommendations for sending faxes in

my FAQ list on data protection in the

Doctor's office in practice (again) known

made as well as with the fax dispatch

employees involved

trained and instructed accordingly

be sen. In other cases it can

be useful as a countermeasure

to introduce same encryptions and

communicate this in the notification. mistakes,

due to lack of care

are, for example, through establishments

well-structured and controlled

bare routines, clear instructions and

the introduction of the four-eyes principle for

particularly sensitive processes are encountered

the. With all measures taken to

I expect the elimination of sources of error

 also that they are regularly

stood as well as event-related

their effectiveness checked and if necessary

be adjusted.

In addition, in the event of data breaches in medical

xen of particular importance to me,

whether the person affected (in many

cases the patient) is to be notified

and was notified. Article 34

Clause 1 DS-GVO requires:

"Did the violation of the protection of

ment-related data expected

high risk for personal rights

and freedoms of natural persons

consequence, the responsible

che the data subject immediately

of injury."

Such a high risk is according to my

assessment given in principle,

if health data

(in the sense of the definition of

Article 4 No. 15 GDPR:

“Personal data relating to the

physical or mental health

a natural person, including the

provision of health services

gene, obtain and from which information

about their state of health

Action")

Objects of a reportable data breach

no are. Many data breach reports that

such as the incorrect dispatch of a doctor's letter

had subject contained to mine

Surprise the statement, one looks at

the doctor's office no notification

obligation according to Article 34 paragraph 1 DS-GVO,

because the risk is considered low or non-existent

which will be considered. Such succinct

and legally unfounded statements

I have met regularly. N / A-

Of course I am aware of the fact

22

that it is from the mentioned principle of

obligation to notify exceptions

can. For example, if a

unauthorized recipient of misdirected

health data, for example due to encryption

selung and other restrictions that

Don't even take notice of plain data

could. If a medical practice stops

points for having such an

case of acceptance, she can do so in her

Data breach report under representation

of the exceptional

chen facts and their considerations

like to do.

In the case of data breaches in medical practices, it works

typically health data. So-

far about (also) genetic data or

other special categories personal

related data within the meaning of Article 9 GDPR

are affected, this applies here to health

what is said accordingly. which

other categories to consider here

are based on Article 9 paragraph 1

GDPR:

"The processing of personal data

th that make up the racial and ethnic

Origin, political opinions, religious

se or ideological beliefs

or union membership

proceed, as well as the processing of

genetic data, biometric data for

clear identification of a natural

person, health data or data

ten to sex life or the sexual

Orientation of a natural person is

prohibited."

These statements about the notification

obligation under Article 34 paragraph 1 DS-

GMOs apply with regard to health data

analogously also for other actors of the

healthcare, such as

hospitals and care facilities.

LfDI BW - 35th activity report 2019 - 1. Main points Who deepens with the data protection

legal requirements for data breaches

NEN wants to deal with, for example, the

“Guidelines for Reporting Violations

protection of personal data

according to Regulation (EU) 2016/679"

the

ARTICLE 29 PRIVACY POLICY

(a [former] European consultant

body for the protection of

related data and privacy)

study the internet of my

office are available.

1.6 E-mail advertising according to UWG -

an exception in

narrow legal limits

E-mail advertising is basically only with

prior, informed consent

Affected allowed, except that all

Requirements of § 7 paragraph 3 of the

against unfair competition

(UWG) are met. This standard therefore provides

as an exception a legal one

Permission for e-mail advertising without

consent of the person concerned.

advice and complaints practice in my

authority shows, however, that it is the advertising

the company with compliance with

Requirements of § 7 paragraph 3 UWG

often don't take it so precisely - and that's why

against competition law and consequently also

violate data protection law.

E-mail advertising according to § 7 paragraph 3 UWG

only permissible if cumulatively all

requirements of this standard are met:

1. An entrepreneur must, together

hang with the sale of a commodity or

service from the customer of

have received an electronic postal address

(§ 7 Paragraph 3 No. 1 UWG).

2. The entrepreneur uses the address

se for direct advertising for your own similar

che goods or services (§ 7

Paragraph 3 No. 2 UWG).

3. The customer has the right to use

aim not contradicted (§ 7

Paragraph 3 No. 3 UWG).

4. When the ad-

resse and clear with every use

and it is clearly stated that

that he consents to its use at any time

can speak without this

other than the transmission costs

arise according to the basic tariffs (§ 7

Paragraph 3 No. 4 UWG).

To 1.: Existing customer relationship

(existing customer)

There must first be a contract between the

responsible for advertising and the

recruited customers have been closed

be. As part of this contract

the entrepreneur must provide the e-mail address

have received from the customer. Also one

free membership in one

partnership exchange leads to a

contractual relationship for a service

(OLG Munich, judgment of February 15

2018, Az. 29 U 2799/17). behaves the same way

during a trial or sniff

per subscriptions.

The customer's desire to

estimate or get a quote

Wanting is not enough here. Kick the

Customer effectively withdraws from the contract,

falls from this point in time on this legal

basis, also with a successful one

rescission of the contract. § 7 paragraph 3

UWG also does not apply (anymore) if a

Consumer contract (§§ 312g, 355 BGB)

has been effectively revoked.

table".

The person responsible is allowed to send e-mail advertising

for own - i.e. not advertising for third parties

te or for products or services

Third parties - similar goods or services

do-gen perform. The email advertisement

must therefore be closely related

with the purchased product or the received

ten services – in practice

the hardest point.

Section 7 (3) UWG is therefore regularly not

ne legal basis for sending

of a general company news

letters with offers about the whole

Assortment or range of services of the company

company. The "similarity" is rather

within the meaning of this exception provision

to protect customers from unsolicited

ner advertising to protect.

But what is meant by the term "similar"

to understand? To this end, the Thuringia

ger Higher Regional Court (judgment of 21 April

ril 2010, Az. 2 U 88/10): “The

resemblance must refer to the

purchased goods relate and the same

typical use or need

correspond to the customer; possibly it is still

permitted, accessories or supplementary goods

to apply."

An interchangeability, as stated by the Chamber

requested by the Berlin court (decision of

March 18, 2011, Az. 5 W 59/11), so to speak

the highest level of similarity, is legal

of course true, promotionally

but (for both sides) rather less

ressant: It hardly makes sense just for that

to be allowed to advertise a specific product, that

the customer has just bought (and

therefore usually not necessarily a 2.

times required). Hence the law speaks

also of "similar" and not of "identical"

24

Taking into account the above legal

language and relevant literature

opinions and for the purpose of

development of a manageable design

is from the point of view of the state representative

a resemblance of

• advertised goods regularly then

give if

◊ these of the typical application and

Possibility of using the purchased

Goods corresponds or

◊ it is a classic accessory or

Spare parts for the purchased goods

acts or

◊ it is in a narrow application

connection to a traffic

supplementary goods to the purchased

th goods.

• advertised service regularly

then given if

◊ this the typical performance goal of

service provided

or

◊ These are classic accessories too

the service provided

delt or

◊ these are customary additional

or supplementary services

the service provided

del.

Of course, the con-

concrete individual case. The more often a customer

Company different goods and

services, the more comprehensive

Of course, the advertising opportunities are richer

ability.

Examples of goods and services

you can find it in the attachement.

LfDI BW - 35th activity report 2019 - 1. Focus on customer evaluation or customer satisfaction

e-mail inquiries, which are always sent as

Advertising are to be classified – and also

then when these requests immediately

after a product purchase and together

be sent with the invoice

(Federal Court of Justice, judgment of July 10

2018, Ref.: VI ZR 225/17) - do not fall

under § 7 paragraph 3 UWG (because of a complete

lig other purpose) and are therefore without

prior consent always data protection

repugnant (but unfortunately widespread).

To 3.: No existing advertising

statement of the customer

The customer may not accept the e-mail advertising beforehand

not according to Art. 21 Paragraph 2 DS-GVO

the-have-spoken. The customer must

special have the opportunity of this

promotional use of his e-mail address

already at the time of collecting his

E-mail address, i.e. during the

ordering process in the online shop, to object

speak. This is required by Article 13 paragraph 2

the Privacy Policy for Electronic

Communication. You can find out more about this

in the activity report 2014/2015, p. 156 f.

Regarding 4.: Reference to objection at any time

option to claim at normal rates

(opt-out option)

Each promotional e-mail must contain the easily

findable and legible information

ten that and how advertising at any time

be objected to at normal rates

can. At this point, the

offered an unsubscribe link.

It depends on the similarity: § 7

Clause 3 UWG is not a license for general

ne product and service advertising.

For every single customer

must depend on previous purchasing behavior

(shopping cart) checked and clarified

be, for which similar goods and

Services may be advertised.

1.7 The right to information

Article 15 paragraph 1 letter c

DS-GVO: Full transparency for

those affected too

data transfers

The right to information according to Art. 15 DS-GVO

belongs to the central rights of

met. Only if I know which da-

the person responsible saved about me

chert, for what purposes he uses them

processed and where it transfers the data

mediates, I can exercise my rights under

tel III of the GDPR effective and fully

assert initially. Yet there is

companies that have

fenen claim to be able to choose whether

in the case of data transmissions, the specific

Recipients of this data transmit or

recipient categories only.

Especially when the person in charge

transfer personal data to third parties

communicates (e.g. in the course of address trading
rented or sold), the business grows
drive with the person concerned, no longer Mr./
Being a woman about your dates increases that
Risk of no longer knowing who everything is in
owns his data. The person concerned wants
therefore know exactly where which data goes
were given.
With regard to data transfers re-
Article 15 paragraph 1 letter c GDPR applies:
(1) The data subject has the right
a confirmation from the person responsible
to request information as to whether they
process personal data
be killed if so, she has a
Right to information about this personal
related data and the following information

(...)
c) the recipients or categories of
Recipients to whom the personal
personal data has been disclosed
are or will be disclosed, in particular
especially for recipients in third countries
or at international organizations;

Complainants have often complained that

that requested companies in their

in the case of data transmissions only

abstractly the categories of recipients

name the data, but not specifically

the companies would list, too

not upon further inquiry. You mis-

always rely on their statutory right to choose,

either the specific recipient or

just name one recipient category

to be allowed. Partly, such as an address

dealers, the recipients would too

not documented.

The State Commissioner rejects this view

carried off decisively, she is with the DS

GMO not to be agreed. The name alone

Identification of categories of recipients (e.g.

Car dealerships, credit agencies, online

line dealer) hardly helps the affected person

further and has also with the greatest possible

nothing to do with transparency.

If this is a question of voting rights at all

would go, this would stand as well

only to the concerned as it is in this

section of the GDPR for their rights

goes.

It is crucial, however, that it is from the

Principle of transparency out as well

not because of the wording of the regulation

is at the discretion of the person responsible,

how specifically he answers the information.

Insofar as data has already been transmitted to third parties

have been made, these must be specifically

to be called. Are transmissions

seen, it suffices the categories of these

to list third parties, insofar as these

are cash; but this would have to be

from the data protection information according to Art.

13, 14 GDPR.

The right to information according to Art. 15 DS-GVO

is, so to speak, the "royal right" of the

met. Here applies to those responsible

greatest accuracy when providing information

and completeness. This applies in particular

which also includes the concrete and

exact designation of the recipients of data

ten (Article 15 paragraph 1 letter c DS-GVO).

As soon as data transmissions have taken place

have the, the concrete places are closed

name to which data was transmitted.

In the case of planned transmissions, information

about the recipient categories.

A maximum of transparency – as well
in Art. 5 paragraph 1 letter a, Art. 12 DS-
GMO stipulated – is here for the ver-
responsible thus the need of the hour
– and can be massive at his injury
result in fines.

1.8 Art. 15 GDPR im employee context

Through the DS-GVO, the data subjects
extensively expanded rights. Special
The law is important here
information and the right to a copy
Art. 15 DS-GVO, especially in employment
context, too. The right to information
is a fundamental “hinge”
for the further assertion of the remaining
gene rights of data subjects. Only the one who
knows the processing that affects him,
can in a second step
assign his right to erasure (Art. 17
DS-GVO) or correction (Art. 16 DS-
GMO) effectively implement. At the same time
any requests for information from employees
many employers, especially long ones
length of service, above all
challenges.

right to information

Art. 15 GDPR contains three independent ones

Claims that flank each other.

According to Art. 15 Paragraph 1 DS-GVO there is

next the right of the person concerned, from the

responsible body to find out whether they

relevant personal data

be worked.

Furthermore, the person concerned can

future with regard to legal

correct information, such as purpose

processing, categories of processing

personal data, recipients

ger or categories of recipients of

data or origin of the data

(cf. Art. 15 paragraph 1 lit. a to h GDPR).

In addition, according to Article 15 paragraph 3

DS-GVO the right to "copy of personal

personal data that is the subject of the

processing are".

a)

Data in the context of employees

In the employment relationship there are

Numerous data processing, which of

(internal) notes, assessments up to

enough for correspondence. to note

is that the employees

in addition to Art. 15 DS-GVO also labor law

the right to inspect their personal

file according to § 83 BetrVG, which

however, is not as far-reaching as

Art. 15 GDPR - GVO. The right to information

is therefore responsible for checking the legal

of data processing, also in the

work context, essential.

b)

right to copy

From the regulatory

technical control procedures and advisory

questions, it has become clear that

especially that in Art. 15 Paragraph 3 DS-GVO

standardized "right to copy" special

meaning and this from work

pursued with particular vigour

becomes. It should be emphasized that on the part

of the LAG Baden-Württemberg too

decision that received a lot of media attention (LAG

Baden-Württemberg, Urt. 12/20/2018 -

17 Sa 11/18) in favor of a comprehensive

sufficient interpretation of the concept of

pie" was hit. So he has

Employer the stored personal

related performance and behavior

ten available to the employee

place. First of all, the concept of

"Performance and behavioral data" in the

employment relationship very open and

hardly any limitations, on the other hand

played the decision in front of

due to internal investigations

lungs, so that even

long and anonymity of whistleblowers

were affected. The revision is currently in progress

at the BAG under file number 5 AZR

66/19. It remains to be seen whether the BAG

the protection of the whistleblower because of Art.

15 paragraph 4 DS-GVO takes precedence over the

right to information is granted or

follows the opinion of the LAG.

c)

scope and limits of

Right to copy

In practice, on the other hand, primarily general

vague requests for information, in particular

particular small and medium-sized

take on great challenges.

Especially in the employee context

after many years of operation

extensive personal

gene data on a wide variety of

gears accumulated. These records

but are subject to a legality con-

don't troll in the first place, only with that

Reference to the large scope of the

standing databases are withdrawn

the. Systematically flanked and supplemented

Art. 15 paragraph 3 paragraph 1 and nor-

 in paragraph 4 expressly states the

stop the interference of “rights and

freedoms of other people”. if you put it

the above-mentioned goal of legal

Eligibility control of data processing

and this system at the bottom, so will

one in principle of a comprehensive

the right to information and the right to a copy

can go out, which only after a

Weighing the conflicting "law

rights and freedoms of other persons",

possibly through blackening, his

finds limits. Responsible bodies

and addressees of requests for information

must therefore, before the disclosure
and making available the copy
s and weigh up whether rights to
of those people, so if necessary also
the rights of other workers
outweigh the disclosure or you
(temporarily) oppose. Also the
Reasons for consideration of the DS-GVO represent a
Interpretation aid to the side. So should
in accordance with sentence 5 of recital 63
DS-GVO the right to information no "Ge-
trade secrets or intellectual property rights
property and in particular the original
copyright to software".
Again, responsible bodies
before providing information, consider whether your
own trade secrets of
information outweigh. This pre-
however, must be traceable
be documented and must not
result in any information being
scarf is denied.
The right to information and a copy
according to Art. 15 DS-GVO is a basic requirement
for the assertion of further
ren rights of data subjects. The LfDI BW as well

other supervisory authorities and consumers
organizations have for those affected
therefore developed patterns for orientation,
which are available on the websites
are (e.g. at www.baden-wuert-
temberg.datenschutz.de). some
requests for a future place in particular many
le small and medium-sized companies
enormous challenges. The LfDI will
therefore also in the future, both for companies
men in the case of advice, as well as those affected
persons in the event of a complaint, the respective
accompany requests for information.

1.9 Technical and organizational
privacy

Our technical department has in 2019
a total of more than 25 on-site control visits
che and countless written control
procedure carried out. Some of the largest
ten data breaches in Baden-Württemberg,
which is also reported in the media
was - such as the hacks of the State
aters Stuttgart and the State Fair
Stuttgart - were and will be through that
Technical report revised. through the
large number of data breaches we could

gain interesting insights and

identify specific attack patterns

which will be reported below.

Current Threats

Spear phishing and malware

Malware that spreads via email

is unfortunately still a big pro-

problem in practice. Meanwhile there are mails

done so "well" with pests

that it is very difficult for recipients

to realize that this is one

attack. The emails are always

targeted, with correct salutation

see and supposedly come from it

from senders with whom the victims in the

actually been in contact with the past

the. In this connection one speaks

also related to "spear phishing". One of

best-known representatives of malware, the

uses this type of attack, the extremely

On a machine infected with Emotet

not only the address books of the

affected e-mail clients, but also the

E-mail content read out and on a

Server copied by the attackers. With this

these further targeted attacks

lead that with the real email content

appear deceptively real. after one

Emotet incident it is therefore imperative that

all e-mails for sensitive personal

personal data, such as health

data, bank details, application data, etc.

be searched and these contacts

a corresponding notification

a data leak (according to Art. 34 GDPR)

approaches The notification should

if not simply done by e-mail. to

often such emails are classified as spam emails

classified and do not reach either

their recipients or just won't

observed. An email notification

does not represent a suitable form of

notification. Affected persons should

via an alternative communication

way to be contacted: telephone, letter,

etc. Regardless, at one

Emotet infestation always displays an ad at the

Central contact point for cybercrime

be reimbursed by the police.

For malware distributed via email

Word and Excel docu-

ment with macros. as

first security measure should be a

Raising awareness among employees

be led. E-mail servers should also

be configured to potentially

harmful (e.g. macro-compatible .docm,

.xslxm etc.) and obsolete (e.g. .doc, .xls

etc.) Document formats directly from the

refuse delivery. As a further remedy

femeasures comes into consideration, both

E-mail clients as well as Office programs

in containers or virtual machines

operate. In general, it is therefore advisable

that e-mail clients do not

ten management systems

for sensitive

personal data are used

the. I.e. emails, and especially emails

with sensitive personal data

ten, should after the entrance from the

e-mail client in a suitable filing

be pushed. A suitable repository is

e.g. an encrypting document

ten management system or at least

an encrypted file storage. Also with

a continuous end-to-end communication

coding can reduce the risk

that sensitive data after a

successful attack, e.g. B. with Emotet, too

a data breach involving personal

data become.

Attention: Become regular (sensitive)

personal data between companies

companies, medical practices/clinics or

hear, etc. exchanged, so corresponds

E-mail without end-to-end closures-

not state of the art anyway.

The malware surrounding Emotet is

also so dangerous because this mal-

ware has additional functionalities.

This is how closures often occur

development of the affected system and

pressure by the perpetrators: either pays

the person responsible for the ransom, or

he no longer has access to his

no data. In this connection one speaks

menhang also from “ransomware attack”.

It is not uncommon for those responsible to

neither no backup of their data at all

created or the backup was made at the

Attack also completely encrypted

rare So there may be a loss

the availability of personal data

and those responsible make a decision

sometimes also to pay the ransom

 (so were with a similar campaign

using the malware "Gandcrab" in one

2 billion dollars stolen annually). Also "small

ne" companies can

according to the failure of theirs, sometimes lasting several weeks

IT network and the resulting wage

costs, lost orders, penalties

lungs due to missed appointments,

loss of reputation, fines, ransom

demands of the hackers, costs for special

specialized IT companies etc. from a minimum

at least five to six figure damage

go out. The careless handling

with e-mails can therefore quickly exist

become trend-threatening.

Attackers try in an infestation in

usually access to central systems

how to obtain domain controller and the

Malware subsequently on all

spread in closed systems.

Therefore, these must be special and with

other access data can be secured

the. The same applies to backup servers:

Try grab before encrypting

the data first all backups unusable

to make cash. Therefore, backup servers should

ver not to central authentication

services such as Active Directory hanging and

use a different operating system. cli

ents shouldn't have a way of doing that

Destroy or overwrite backups

ben. Increase regular offline backups

the security.

Recommendations:

• Users should be made aware

(it should refer to the current dangers in

reference to spear phishing

will). In the best case, the Nut-

then do not destroy any malicious attachments

more. If an attack is successful

takes place, but users should not

Fear of consequences and her

should report the incident immediately.

It is important that there is a functional

reporting chain there and infested

Systems immediately disconnected from the network

and (in the case of Emotet) afterwards

completely new

to be installed.

• If e-mails with sensitive data are

ben, then these should promptly

be deleted from the mailbox,

so that there are no data protection pro-

comes.

trouble

by malware

• Backups must be separated from the rest of

be separated and backup ser-

ver use their own authentications.

Backups should also be available offline

so that in the event of a

case not be encrypted with . It

should measures be taken

to prevent malware from building up in the internal

network can expand further. From-

macros should be

moderately deactivated.

The BSI has very good recommendations too

provided to this topic.

Inadequate protection of the long-distance

maintenance access

Surprisingly often in 2019 data breaches

NEN reported that about not or not

adequately secured remote maintenance

additions were made. surprising therefore,

as these remote maintenance accesses are permanent

were active and some of the

gangs passwords saved with or

protect access from brute force attacks

were protected. You can do it easier

ultimately not make it possible for an attacker.

Compliance with the base requirements

from the module OPS.2.4 remote maintenance

of the BSI

IT baseline protection compendium

2019 would have prevented such attacks.

Among other things, the following is required: “The

LfDI BW - 35th activity report 2019 - 1. Focus of the

initiation

remote maintenance access

MUST be done from within the institution

gen. The user of the remote administration

ten IT system MUST allow remote access

explicitly agree.” and “[It] MUST

all communication links

completed remote access

(Deactivation).". The state of the art

requires that those responsible for the fulfillment

fulfillment of the obligations according to Art. 32 of the GDPR

not for comfort reasons the risk of one

permanently active (and open) remote

ment access. But not only

Those responsible must take this into account

also processors who, for convenience

set up their customers such a

suggest easy access commit here

a breach of Article 28(3).

Letter f and Article 32 of the GDPR.

Insufficient notification of

responsible by service providers

If a processor reports a violation

tion of the protection of personal data

data, he reports this immediately

the person responsible. This requirement

from Article 33 paragraph 2 of the GDPR

te probably known to all processors

be. Less well known is how this Mel-

appropriate for the purpose

can be led. The responsible

should be able to

relevant measures according to Article 33 f. DS-

seize GMOs and take appropriate countermeasures

to be able to carry out measures. Can

a message about the otherwise for

e-mail distribution list used

measure? No! Should one at all

Use email for notification

become? At least not alone. A

additional call, fax or registered mail

ensures that the message

responsible also really achieved and

ensures that the processor

appropriate notification of

responsible can also document.

It should be in the data processing agreement

be regulated, who and how at a

data breach should be notified.

Hacking of online accounts

by celebrities and politicians

At the beginning of January 2019 it was announced that

several online accounts of German politicians

and celebrity hacked and thereby im

December 2018 lost a lot of private data

were made public ("doxing"). In a

Survey list were 994 politicians and

Celebrities were mentioned overall

but the contact details of much more

people affected. "Hacked" only

a mid double digit number on Social

Media profiles of those affected. Since many

but their address books to the

provider of the social media platforms

loaded, the attacker had access

to the contact details of around 40,000 people

sons. In addition, the attacker has numerous

che private and intimate messages or

Conversations Affected on the

Platforms have led, as well as various

Documents from cloud storage service

published. Among them were

in addition to private letters, bills and

Photos partly also illustrations of

reference documents.

These documents were primarily

various platforms on the Internet

public, relating to the spread of

specialized in illegal content

ben. We were able to partially delete it

of this data also in non-European countries

reach abroad. standing in the room

the high fines were there – too

overseas – often a good argument

for the hosting providers, the platform

get drivers to delete; Further

procedures are still ongoing. Some cases have

out of responsibility to other European

 submitted to the supervisory authorities, al-

however, so far with no showcase

cash result.

The case shows several pro-

blem areas on: That's how sharing is

of address books for social media platforms

forms to be viewed very critically. This

Platforms usually use the data

also for own purposes, for example

for profiling. Is the use of the

platform not exclusively for personal

chen or family activities, is the

Transmission of the address books clearly

within the scope of the GDPR and

requires a legal basis. There comes

usually only the previous, voluntary, active,

separately declared, informed and revocable

consent of those affected - i.e. all

ler contacts in the address book – under consideration.

And usually nobody has them.

Hacker attacks are often carried out

weak or reused passport

words relieved. Our notes on

have secure handling of passwords

we already found in the activity report 2018

thinks. A two-factor authentication

can significantly increase protection. To-

everyone should think about which ones

documents he saves on which platform

chert

Oldies but goldies?

In addition to the "new" samples mentioned above

we also met lemen in the year of the check

back to "old acquaintances", i.e. weak

put those already in previous years respectively

were an issue. Some examples:

Destruction of files/data carriers

Even in times when even discount stores

Office shredder with particle cut (P-

4) offer, there are data breaches

with insufficiently destroyed files and

data carriers. DIN 66399 has been in force since January 1.

October 2012 (see 31.TB) and

still have some responsible

Provide the disposal concepts and

status contracts apparently not adjusted,

which may lead to corresponding fines

drive leads (see also section

"News from the fine office"). loading

special finds were several

Hard drives from the flea market that are neither

were still deleted and send

sible data contained, as well as insufficient

shredded bank records.

After encryption of storage

media to the basic protective

measures heard and the consequences of a

Loss of data in the form of a possible

general data abuse mitigates, should

ideally always be encrypted.

This is necessary if only because

depending on the design or malfunction

no longer residue-free or not

can be recoverably deleted

and thus only the physical destruction

tion as a last resort.

processor)

According to Article 32 paragraph 1 data protection

basic regulation (DS-GVO) has

responsible body (and the possibly

existing

under

Consideration of the state of the art

appropriate technical and organizational

Measures to protect personal

to meet drawn data. As a measure

For example, the encryption is personal

called related data. The encryption

processing of personal data has for

the responsible body and/or the

processors have further advantages

le: If a reportable "data

panne” is present, those affected must also

immediately in clear and simple language

be notified if a high

hes risk to personal rights and

 freedoms arises. A notification

of the person concerned is, however, pursuant to Article

34 paragraph 3 letter a DS-GVO in case of

loss of a data medium on which the data

state-of-the-art

ciphers were usually expendable.

locking technology

During on-site inspections, we

mer again on second key and in

cabinets, IT racks (without special

ßung), in storage rooms (sometimes still with

fire load such as paper/cleaning agents), missing

protective fittings and non-locking

ne doors that just pulled shut

became. The case of an IT robber was curious

mes, whose electric door opener specially

via a code lock for access control

trolley was actuated, its lock latch

(coll. snapper) but also with a larger

can be opened with a paper clip

could.

Keys that are not handed out personally

and thus under sole

are under the control of the recipient

stored so that no unauthorized persons

can have access to it. In doing so,

sen storage type and location dem

correspond to the protection requirements of the key.

In general, missing or insufficient

Key management procedures

add to. The logging of the key

self-pickup and return is recommended

len.

multifunction devices

For multifunction devices, the

Storage of the data locally or on

Network drives as well as those via browser

accessible interfaces checked. Part-

way, files on shared

simply printed out on a network drive

be used, although these are not provided for

were. The found storage

of print jobs over a longer period of time,

was not proven over the years

compels. The web interfaces of printers

and multifunction devices were mostly

from the standard workstation computer via

Browser responsive.

Unnecessary exposure of the devices should

always be avoided. precondition

for the data protection-compliant operation of the

devices is that the security settings

gene is also activated and sensibly configured

will. That means passwords too

to set or change standard passwords

are and the web interface via

Filter rules, e.g. for the network coupling elements

ment only for dedicated administrative

computers are accessible. If device

possible on the other side, is the transport

activation. Besides, that should

Device undergoes regular safety checks

and updates can be integrated.

Documentation of the

chose configuration, so that for example

wise easily checked after an update

can be checked whether all desired security

security options are really still activated

are.

Fines for technical violations

Particularly noteworthy is from viewpoint

of the technical department the fact that

the first GDPR fine in Germany

(still in 2018) due to insufficient

corresponding data security was imposed

("Knuddels" case). Missing data backup

heit is also the reason for in 2019

a large part of the

le imposed fines. This should be as

Signal seen for those responsible

be that data security through the

DS-GVO has gained enormous importance

has and can no longer be neglected

may!

 Overall, this year we also

determined that in particular service

ter – to the smaller sub-

take, clubs and e.g. medical practices

are dependent – far too often neglect

sig in terms of data security

ren. Through a series of data breaches

Service providers experienced large outflows

personal data of data subjects

and in some cases also to damage

gen with those responsible, which the

used service providers. View

of the technical department, there are

rich very large need for improvement.

advisory

In addition to the control activity and the processing

processing of data breaches was the technical

nik department also in the consultation and the

Development of orientation aids active.

Creation of a data protection

assessment (DPFA) for the e-file BW

The obligation to electronic

according to current legislation

Version effective January 1, 2022: From

then according to § 6 paragraph 1 EGovG

BW the authorities of the country their files

to be managed electronically. With the e-file BW

goes electronic data processing

accompanied by a large number of personal

drawn data includes and insofar for

is an important topic for the LfDI.

Last but not least, the LfDI also has to go to one

switch to electronic filing. loading

very early on, the LfDI was

position "Project Uniform E-File"

of the Ministry of the Interior in the examination

nes security and data protection

integrated. This exam was

now largely completed.

There are still open points

(e.g. logging vs. employee monitoring

but these are subject to an introductory

e-File BW initially not in return

gene.

In addition, the LfDI will

data protection impact assessment (DPFA)

for

the e-file BW created. This DPIA is intended as a

Templates used by all authorities

be able. It does not follow from this that all

can use the same DPIA. There-

for are the procedures and type of personal

son-related data in the individual

authorities too different. But the one from

LfDI created DPIA will probably mostly

as a template for the authority-specific

procedures are suitable. As soon as the DPIA is finished

is provided, this should also be made public

be available and can be used as a pattern for private

Companies serve (similar to the BayLDA
Sample at https://www.lda.bayern.de/
de/thema_dsfa.html). The DPIA orientated
conform to the ISO/IEC standards of the 27000
and 29100 series (ISO/IEC 27001, 27002,
27005, 29100, 29134, 29151 and 31000).
When creating the DPIA and the
with associated exchange with the
individual project groups has become exemplary
shown that a DPIA is a very useful
les procedure for identifying risks
and their treatment is. One must have his
Knowing values to make them appropriate
to be able to protect. A suitable one is here
Quoting Bundy McGeorge (U.S. National
Security Advisor): "When we check our dental
brush and diamond with equal zeal
protect, we lose less toothbrush
ten and more diamonds." (Originally:
"If we guard our toothbrushes and dia-
moons with equal zeal, we will lose fewer
toothbrushes and more diamonds."). con
Specifically, this means that with the creation of the
DPIA for the E-Akte BW risks identified
however, problems were also
implementation of individual remedial measures

took. And only if a DPIA before the

Project start is carried out, can

these findings useful in the project

Practice

In practice, the

DPIAs submitted to the supervisory authority rarely

an “Assessment of Risks to Rights

and freedoms of the persons concerned".

as set out in Article 35(7)(b).

c of the GDPR is required. Also the

according to Article 35 paragraph 7 letter d of

DS-GVO required remedial measures

with those of the “rights and entitled

Interests of the data subjects and

other affected parties into account

will" find hardly any recognition in practice

tion. Most of the submitted DS-

FAs a risk assessment and remedial action

took for confidentiality, availability

and integrity, i.e. the “classic” goals

from information security. One

Assessment is therefore usually made from the point of view

of the company - a consideration from

Unfortunately, the view of those affected does not take place

instead of. However, this is precisely what the data

protection just requested.

Video surveillance and doorbells

The advertising says it all: the homeowner

enjoys his life and can

deo transfer and smartphone app off

remotely open the door for the postman

or the alleged burglar

made it clear that he was caught on video

is drawn. So what can be done here?

go wrong? Unfortunately, the security

the video transmission to the smartphone

ne often left much to be desired. Will

asked the manufacturers about the problems

chen, these remain impressive

left - after all, the manufacturers are

not those responsible within the meaning of

GDPR. The person in charge decides

about the purposes and means of processing

processing of personal data and

this is the operator of the camera

ra – and not their manufacturer. Whether the

deotransfer by uncertain (pre)

Settings or errors in the software

thereby publicly available or to servers

be transmitted in third countries is

are the responsibility of the operator.

The operator of the camera must also

be careful not to close any public spaces

capture. Are pictures from public

Rooms transmitted to the Internet and for

every retrievable, this has a fine due

result in the supervisory authority.

What can the responsible person do?

Pay attention to the safety of the product,

do your research before you buy, inform-

be careful during operating hours

possible vulnerabilities and install

you software updates. Disable

the transfer to the smartphone when

you do not necessarily need this function

gen. If you do need this function

If possible, you should contact us

connect to your home network with a VPN

the and only about it with the camera. Of the

Camera should not connect to the

be allowed on the Internet. So silly yourself

that may also read in 2019. See also TB

2018 Chapter 3.2.

Video image resolution, the DIN EN

62676-4 (or DIN EN 50132-7) and

the question of whether video surveillance

per se personal data

be recorded

With the technical data of the Vi-

this question cannot be answered

respond. The answer depends

also from the accompanying circumstances of the vi-

deodorant intake, d. H. the available

standing additional information. To-

but next to the technical data: (1)

image resolution of the camera, (2) distance of

Camera to captured person, (3) angles

son and (4) lighting. For evaluation

the personal reference of video recordings

we proceed from ideal

al conditions, i. H. the person

is captured frontally by the camera and

the lighting is ideal. The above

mentioned points (1) and (2) can be considered as

Summarize "point density" and

that usually comes with video systems

the unit mm/pixel, pixel/meter or pi-

xel/16 cm (face) indicated. examples

from DIN EN 62676-4 are in the table

can be seen in the appendix (images based on

ge from https://www.gov.uk/cast-resource-

ces-for-the-crime-prevention-industry).

It can be stated that from

a point density of 16 mm/pixel, i. H.

one pixel in the image is 16 mm

of the captured object, the represented

Person only with additional information identical

can be verified.

DIN EN 62676-4 therefore defines from which

ter point density monitors people, de-

detected, observed, recognized, identified

or can be examined. As in

the table with the illustrations

is specified in DIN EN 62676-4 from a

point density of 8 mm/pixel a detection

acceptability of persons. So-

far to the technical data. With addition-

know, for example, the site manager on a

video-monitored construction site, the boss in the

office, etc. can also be used at 16 mm/pi

xel comparatively simply a person

reference can be made. If you lead this

Thoughts continue, so is also with

lower resolution, a case-by-case examination

required to determine whether a person

reference can be made. to

care must be taken that a multitude of

number of additional information, such as exterior

appearance, items carried,

unusual behavior and/or

by a combination of place, date,

Time, etc. but a personal relationship

can result. If the case-by-case

conclusion, however, that no

additional knowledge is available,

half a dot density of 16 mm/pixel

of a video surveillance without persons

be assumed.

1.10 More data protection also means

more Europe!

The European staff unit was

year especially in the area of fundamental

questions expanded and strengthened. Next to

the area of European cooperation

men work who is involved in the collaboration in the

Committees of the European Data Protection

committee and the coordination of

cross-border administrative

driving are now also the basic

sentence questions in the national area in the

Affiliated to the Europe department. For the

LfDI is the staff unit the central coordination

ing point of these questions, which the

Uniform application of law within

and secure outside the home. There-

besides she represents the LfDI at lectures

and specialist events.

European cooperation

1.

With the validity of the GDPR, the domestic

international cooperation in data

protection to a new level. A-

common administrative regulations

are just as important here as the efficient

efficient and coordinated processing

cross administrative procedures.

a) Participation of the LfDI in the

working groups of

European data protection

committee

At European level we are in the

Working Committees of the European Data

ische Data Protection Board (EDPB).

the independent European body

for the uniform application of the data

data protection regulations throughout

European Union contributes and the
cooperation between the EU data
protection authorities. The EDPB exists
from representatives of the national data protection
authorities and the European data
Protection Officer (EDPS). Germany
has a seat there. this one
The seat is currently occupied by the Federal Commissioner
te for data protection and information
tion freedom (BfDI) true. The choice of
Deputy, according to § 17 paragraph 1
Clause 1 BDSG head of the
supervisory authority of a country, was until
not yet successful by the Federal Council
carried out. Because this deputy that
right to vote in matters in which the countries
who alone has the right to legislate
ben, or which the facility or that
relate to procedures by state authorities,
should perceive, this choice is for the
effective representation of the interests of
countries are essential – which is why the
deceased election by the Bundesrat
serious and worthy of criticism
represents default.
In the working groups of the EDPB, the

LfDI a permanent position as country representative
in the Social Media Expert Subgroup,
carried out by the European staff unit
men will. This coordinates the position
taken by the German supervisory authorities
and brings the agreed points of view
on a European level. Next to this one
fixed coordination function
LfDI currently in several workspaces
the position as simpler or
the reporter true:
In the Social Media Expert Subgroup of the
EDSA is the LfDI together with the French
Czech Data Protection Agency (CNIL) fe-
the lead rapporteur in an
material subject area. For the creation
of guidelines in the field of
I have work in Cooperation Expert
Subgroup also the lead
reimbursement accepted.
A simple reporter creation has-
I te together with the Hamburgian
commissioner for the creation of an inter-
a paper in the Social Media Expert
subgroup inside. I also share
Schleswig-Holstein in the area of basic

sentence questions such a position in the Key

Provisions Expert Subgroup.

As chairman of the working group

deomonitoring of the data protection conference

I have, with the help of the statistic

by the Berlin representative for

Privacy and Freedom of Information

"Guide line 3/2019 on processing of personal

nal data through video devices".

and these issues at European level

addressed.

The already networked in 2018

investigations initiated by vehicles

were successfully continued this year

guided. Also in this area

I had the German and European

colleagues temporarily as rapporteur

ter supported.

Guidelines and Opinions of the European

Data Protection Committee can be found at:

https://edpb.europa.eu/edpb_de

b)

border crossing

administrative procedure

Are cross-border

carried out, it applies without

according to Article 60 DS-GVO the

operating principle, according to which priority is given by

cooperation, a consensus can be reached

37

LfDI BW - 35th activity report 2019 - 1. Priority areas. But also informal communication

tion mechanisms may in their importance

tion for European cooperation

not to be underestimated. About the platform

form of the Internal Market Information System

tem (IMI) all cross-border

tending administrative procedures and also

handled informal requests that

Exchange of experience between the supervisory authorities

enable that. My authority was 2019

at 123 transactions conducted in this system

driving involved. We have seven of them

as the lead supervisory authority

leads. We were affected in 116 proceedings

ne supervisory authority, of these procedures

48 entered our house and

were with the European authorities

divided. We currently list approx

15 inputs coming over in the near future

the system with the European colleagues

to be shared.

2.

Coordination more uniform

Viewpoints on European

and German level

At the German level, I represent the interests

ressen of Baden-Württemberg in the committee

the independent German data protection

supervisory authorities of the federal states and the

Federal, the Data Protection Conference (DSK).

It has the task of data protection

to uphold and protect fundamental rights,

a uniform application of the European

ic and national data protection law

to reach and together for his

to enter into further development. The data-

protection conference generally meets semi-

annually in meetings lasting several days, whereby

since the GDPR came into force, several special

and interim conferences per year

be led.

You can find the results of the work of the DSK

under:

https://www.datenschutzkonfe-

renz-online.de/

The decisions of the DSK are carried out

Working groups prepared. the business

regulation of the DSK ensures that the

Country representatives, of which the supervisory

authorities of the countries in the european

Working bodies are represented, also in

the thematically identical German

working groups are present. in the

They are part of their European work

to the positions and decisions of the

DSK and the results of the working groups

bound. Is there a uniform

dot on a topic

so this according to the procedure

Section 18 paragraph 2 of the Federal Data Protection Act

(BDSG) are formed. According to § 18

sentence 2 sentence 4 BDSG is in doubt

the simple majority of votes

pale. Through this procedure

uniform positions of the Germans

supervisory authorities and therefore consistency

secured at German level.

3.

consultations and training

the EU department

After the European Office of the LfDI

numerous participants in 2018

has trained participants

the need for lectures on the new

Data protection law under the GDPR as well

not demolished in 2019. Within the

reference period, 39 schools alone

ments of the European staff unit also in this

many interested people again this year

sensitized to the topic of data protection

equipped with expertise. To-

which now also the European

jurisprudence on the subject

set apart (Fashion-ID verdict

dated July 29, 2019), was one of the

score points on training courses in social

Media area and the question of whether and how

social media in compliance with data protection

can be used. Through our active

ve Participation in the Social Media Expert

 data protection officer of the aforementioned

positions and thus obtains the opportu-

heit, everyday problems in the

Implementation of the GDPR and state or

area-specific laws in public

chen sector to discuss and together

with the other participants

to develop full practical solutions.

And last but not least, of course

in our own house again and again

not only the (new) specifications

in accordance with the DS-GVO

put and meet, but also the

current developments on European

level or at the other supervisory

listen to watch in Germany and

flow into the advisory work of the LfDI

to eat. For this reason offers

the European staff unit is also ongoing internally

fend in-house training for your own

Employees in which, on the one hand

possible changes and new

new insights into fundamental issues

of data protection practice.

In this way, uniform standard

Points developed within the LfDI and

especially the new employees

familiar with important issues

power.

Subgroup of the European Data Protection

Committee (EDPB) we can valuable

Work results on the practical questions

gene around the use of Twitter and

Co. and hand them over to the responsible

verbatim in Baden-Württemberg

give. Another focus was the past

year in the non-public area at the

Training for clubs based on

their often small size and manpower

who at the organizational level in the

feld great concerns about the

Realization of the data protection law

had requirements. Through targeted

events in this area

LfDI tries to dispel these fears

gain weight. In particular, our practice

advisor “Data protection in the association according to the

GDPR" (https://www.baden-wuerttem-

berg.datenschutz.de/praxisratgeber-da-

tenschutz-in-the-association-after-the-ds-gvo/)

should, through its specific explanations

gene and clear examples practicable

Show ways how data protection in the

association can be designed.

The public area was

Office for Europe also continues

more trained. He quickly turned

get out that straight in the public domain

often indications for a lawful and

above all practicable implementation of the

data protection regulations

were missing.

Therefore, numerous events

gene specifically for authorities of our country

carried out in which the special

Regulations and needs of data

protection of public bodies

became. Is particularly valuable in this

also the cooperation between

schen the LfDI and the ministries as well

Regional councils of Baden-Württemberg

within the framework of the

set up working groups. In particular in

"Data protection working group" exchanges ideas

the LfDI regularly with the authorities

From January 1st, 2019 to October 31st, 2019

a total of 196 new ones at the fine office

fine pending. The number

of monthly new arrivals has

in comparison to the relevant pre-

period of the year (beginning of June to the end of October

tober) increased by an average of 20%.

obtained search warrants, whose

completion is imminent. In addition

the fine office carried out several checks

len by those responsible, in two

cases led to fines.

(takes into account new entries after the effective date

of the GDPR by the key date of the respective report

went.)

The one from the Regional Council of Karlsruhe

old cases taken over could

be completed in time. To

as before, fines will not apply to everyone

Data breach imposed, but

primarily in the case of more serious violations.

Overall, the fine office imposed

between the beginning of January and the end of October

Fines in 19 notices in 2019

amounting to a total of 242,140 euros plus

Fees totaling 12,107.00

Euro. The fines were aimed at

in the case of both natural persons and

also against small and medium-sized ones

Company. fine proceedings against

large companies are still located

in the investigation stage. In a multitude

of cases, the fine office Ver-

testimonies of witnesses and victims

through, passed in several proceedings

Court orders and with the assistance of

Police seize evidence and

isolated cases

Imposed by decision of April 12, 2019

the fine office a fine in the amount of

EUR 80,000 against a medium-sized company

financial services company. The-

when disposing of sub-

gen, the personal data of two

Customers included, not the required

Diligence to maintain integrity and

Confidentiality of information in terms of

ne of Art. 5 Paragraph 1 lit. f GDPR

to let. So the papers were

previous anonymization by shredding

or blacking out accidentally in general

disposed of my waste paper, where the company

were discovered by a neighbor and

have been sent to my authority. Unfortunately

is the improper disposal of

documents, some of which contain sensitive personal

contain related data, not an isolated case.

Rather, there were several in the year under review

Penalty proceedings for violations of

the integrity and confidentiality of the data

according to Art. 5 Paragraph 1 lit. f GDPR

pending, the majority of which with a

By decision of May 9th, 2019

the fine office imposed a fine for the first time

money against a police officer. Dem was

based on the fact that the official was too private

purposes and using

ner official user ID

the license plate number of a car

dates of a chance acquaintance

asked. With these owner data made the

Officials filed a so-called SARS request with the

Federal Network Agency, thus obtained the

phone number of his casual acquaintance

and then contacted them. The-

This procedure represented a so-called excess,

which the office of the police officer

ten was not attributable. That in § 28

LDSG standardized ban on prosecution regarding

public authorities was not including

gig, because neither was the department for

responsible for the violation, nor was that

Civil servants as independent public

to look at. Rather, it was

to a violation that the official as

Private individual using official

access rights committed. His acting

was therefore to be evaluated according to the GDPR

and was fined moderately

fined in the amount of 1,400 euros. the

Decision shows that officials

public places, as well as employees

non-public bodies, for unauthorized

action in breach of data protection sanctions

can be ned.

Imposed by decision of October 24, 2019

te the fine office a fine in the amount

of 100,000 euros against a medium-sized

Indian food handicraft company

men because this is the personal

Data of his applicants negligently not in

sufficient scope against access

protected by unauthorized third parties. That

company had one on its website

Applicant portal set up, via which

Interested parties their application documents

could submit online. However, that offered

Company neither an encrypted

Transfer of the data to, still done

the storage of the applicant data

encrypted or password protected. In addition

were the unsecured applicant data

with a link to Google

hen, so that anyone with a Google

Research of the respective applicant names

come across their application documents

and these without access restrictions

could call.

fine concept

The work of the fine office of my service

place, together with the legal department of the

Federal Commissioner for Data Protection

and Freedom of Information (BfDI) and the

data protection supervisory authorities of the countries

Berlin and Hesse, led to the development

of a German fine concept for companies

company, which on 16.10.2019 from

published at the data protection conference

became. The concept is provisional

until the adoption of European guidelines and

intended to harmonize the German

sanction practice and transparency

and traceability for the responsible

serve literal passages. Since the fine

83 paragraph 1 GDPR in each

effective and proportionate to the individual case

and had to be deterrent

a concept to be developed which

both the concrete facts and

also the so-called perpetrator-related characteristics,

i.e. in particular the economic

the respective responsible persons

takes into account. A catalog with fixed

responsible for certain violations

with off. The published concept

bears the economic circumstances

already in a first step calculation,

in which the companies – similar

the WpHG fine guidelines II of the BaFin

to be categorized in a next

Step a basic economic value

to build. At this sales-related

Company categorization is the

functional corporate concept

Recital 150 GDPR to be used. in one

further step, this core value will vary

according to the severity of the crime with a fact

gate multiplied and then in a final

th step based on further aggravating

or favorable criteria, including

also the profitability and profit of the

company, depending on the

fits. Previous practical experience

have shown that the concept on the one hand

those of the European legislator

intentional increase in fines

Comparison to fines under the BDSG

a. F. causes. On the other hand, they reach

Fines but not unreasonable

heights and may be subject to

most companies understand

will. The future developments

will show whether and, if so, to what extent

fine concept is to be adjusted.

The practical experiences of the first 18

Months since the GDPR came into effect

show that it is worthwhile to

to accept offers from my office

and to implement legal requirements

to avoid fines. As far as fine

proceedings were initiated, appeared in

many cases due to the good cooperation

tion with the fine office and the prompt

ten implementation of any requirements

no more imposing a fine

necessary so that the procedures

could be provided. The previous

but experience also shows that in such

cases in which sanctions are

ten is the violations with significantly higher

Fines are imposed as under the

old national legal regime.

1.12 Bye Bye Twitter

On December 30 of this year had to

I bid farewell to social media

announce dia platform Twitter. Since

tweeted there at @lfdi_ in November

bw the only German data protection

supervisory authority with an official

count about own news, commented

the

current data protection events,

exchanged in some intense, but

always relevant discussions

the data protectionist swarm on Twitter

out and was also available for immediate questions

responsive.

Since November 2017, the LfDI has been about

3,000 tweets from, the number of followers

of the account grew to 5,500 in the end.

I reached with my short messages

several within the last two years

million Twitter users and received thousands

multiple feedback with suggestions,

Assessments of our work - please

Fortunately, the friendly response outweighed

clearly. At the same time, I used

brisk and above all fast communication

on this platform to join me at the 150

Persons and instances to which I myself

followed, about current data protection issues,

Court decisions and national like

international political-parliamentary

to keep events up to date.

Already with the Facebook fan page decision

decision of the European Court of Justice

5 June 2018 (C-210/16) Eclipsed

the image for users of social media:

The ECJ ruled that the

Operator of a fan page next to the platform

form operator himself as the person responsible

to be considered in the sense of data protection

is - and thus in data protection

no longer bump into the platform alone

refer to their operator and his

can wash hands in innocence. In addition

 was thus made clear that between

the two jointly responsible

a contract is to be concluded (cf. Art. 26

DS-GVO), in which the perception of
Obligations towards those affected
be regulated in a transparent and unambiguous manner
got to. And such contracts were and are
gene until today in a data protection
fair form. That was since the middle
of the year 2018 at least for public ones
and private operators of Facebook fan
pages clear that they - completely independent
from the question of whether the platforms
from members and non-members
process lawfully – their social media
formally unlawfully maintained
whether this legal situation also applies to other
re platforms than Facebook has been
controversially discussed below
in view of the increasing con-
vergence of social media offers (their
Functionalities are becoming more and more similar
the underlying business models
"Economic exploitation of personal
related data of the users" are identical)
however, can hardly be disputed.
Even more precarious – and even clearer –
the legal situation was determined by the
decision of the Federal Administrative Court of

September 11, 2019 (BVerwG 6 C 15.18),

that by way of a preliminary ruling

adopted by the ECJ in June 2018-

ne position in the German legal area

transferred: This was not only the

data protection responsibility

confirmed by the fan page operator, but

at the same time the supervisory authorities

granted at electoral discretion,

of violations of the law during operation

the platform optionally on each of the

responsibile - so also on the user

access: "Even in the area of data

protection it can be the requirement of an effective

active and effective hazard prevention

justify the person responsible

chen to use, its duty

can be affirmed without further ado and the

effective means of stopping the violation

be available."

The Federal Administrative

according to the court on December 10th

2019 published decision

de the possibility of a "regulation to

the corner": The supervisor can

adverse data processing on the platform

form also access the user and

him with measures such as warnings

or substantiate orders. Whether you do that

now selective discretion, hostage-taking or

calls pawn sacrifice is secondary. In the

thing is always about one not

reachable disruptors – the platform operators

ber - via an accessible interferer - the

Account operator – to put pressure,

comply with applicable law.

And why are most operators of

successful and far-reaching platform

form operators "not available"? Thereon

There's a two-part answer: First

once the GDPR ensured that

the new uniform data protection law

Europe is also implemented uniformly

(Keyword coherence method between

the supervisory authorities) and has

the so-called one stop shop

provides that for each data processor one

and only one supervisory authority responsible

is and makes the announcements. In case of

Facebook, Twitter and Co. this is the

sche supervisory authority, which with the

other government agency of the Republic of Ireland

country shares the reputation, particularly

and to act in a business-friendly manner. fact

is that it's Irish counterparts to date

has not succeeded, even one effective

Regulation towards the platform

to meet drivers. That means: others

European supervisory authorities are allowed to

Platform operator not effectively controlled

, but the competent authority provides

no effective control for sure. With that

conditions that the Bun-

of the administrative court on the condition of

exercise of supervisory powers

opposite from places using the platform

has made. This could be considered

Warnings to users (Art. 58 para. 2

lit. a DS-GVO), later also to management

ments or even orders, their ac-

limit or close counts

(Art. 58 para. 2 lit. b and d GDPR).

It's not "beautiful" of course: it's essential

it would be more obvious and "fairer" to

stop violations of data protection at the source

len - especially since the users of the platforms us

assure with great regularity, no

exert any influence on the operators

can (which we can well understand

nen). Nevertheless: It is the users who

these platform operators as service providers

use to their public relations

with the greatest possible range and re-

to operate sonanz (as I do too

previously via Twitter), and thereby

the users zen the basic condition for

that many interested parties click on the social media

slide platforms are lured - and there

their rights may be violated.

Intermediate question: But act now

the platform operators unlawfully,

so treat user data against the

Provisions of the GDPR? For this is to

next to state that there are tasks

be the Irish regulator, this

to identify and evaluate. If this

but does not happen effectively, the allowed

remaining supervisors hands not

sit back and have to – ahead

against the background of social media

tion by responsible bodies, via

which they exercise supervision themselves – a

Get a picture of the legal situation. Thereafter

sees it based on the available

information, in particular the data

declarations of the platform operators,

and subject to other knowledge

the competent supervisory authority

looks like this:

Almost all of the common social media

dia platforms are currently not data-

usable in a protective manner. Many platforms

collect data from registered users

and non-users, on their own

Website, in your own apps and on

Third Party Websites and Apps. you submit

at its own discretion data to third parties

and also reserve the sale of all

data before.

The processing will neither

in terms of the technologies used,

nor the affected data types, processing

processing purposes or recipients specifically

and finally mentioned.

The processing is extensive

without legal basis: one informs

voluntary, prior, active, for the specific

ten individual case and separately explained as well

consent that can be revoked at any time

ligation is not queried. Instead of this

you have to agree when registering

that the data protection guidelines "apply

th". Other legal bases (Art. 6

Paragraph 1 subparagraph 1 lit b-f GDPR) are open

obviously not relevant.

One way, as a platform user, as

Third-party website or third-party app operator

an agreement regarding the

joint responsibility (Art. 26 DS-

GVO) to conclude with the platform

often not apparent.

The conclusions from these

first of all, the responsible

draw yourself and be clear about it

whether they belong to the people they

A bundle is ideal for a wide range

communicative measures: We will

our quarterly newsletter

strengthen, set up your own podcast

and check if we're using a daily

Email Info Service

those feedbacks

previously addressed directly via

Twitter could be given one

Circle of subscribers to our mail ser-

vices can continue to ensure.

So: Even after Twitter, the LfDI will be like this

communicative, creative, responsive and

stay as spontaneous as possible.

We make it!

ten purposes under these circumstances

cial media platforms even further

can zen. It goes without saying

that public bodies subject to the reservation

subject to the law and in particular

re have constitutional ties,

much faster and stricter here

have to go as a non-public body

len, as companies and associations that

on these platforms mostly from

are traveling. The LfDI will

therefore first the authorities of the country,

with whom we have been intensive since mid-2019

conversations are held, their behavior

address them and try to engage in dialogue

to improve the situation

wear. Whatever the positions of the

authorities are involved: the way it is now,

there is no way it can stay.

This also means that the question of alternative

ven addressed - and there it does not see

particularly comfortable: A data

protection-compliant alternative to Facebook

is far and wide not in sight, Facebook

is at least in Europe a kind of monopoly

list, which has a negative effect on their change

willingness to pay. at

There is one on Twitter with Mastodon

functional competitors with

data protection compliant decentralized structure –

however, it still lacks range.

Otherwise there is just in the public

sector the opportunity by building up a

a self-sufficient state platform

and create legitimate alternatives.

Initially, such counter-models

mer a bit awkward – but that has to be

don't stay like that. And towards public

The legislature could

Mandatory use of the public platform

arrange and thus for enough "traffic"

worries.

How is the LfDI going to continue if

he opened his Twitter account at the end of January

2.

2.1. cell query

The Code of Criminal Procedure (StPO) sees in

§ 100g paragraph 3 among those mentioned there

Prerequisites the possibility of im

As part of preliminary investigations all in

traffic data accumulated in a radio cell

to raise.

Under traffic data within the meaning of the

Communications Act (TKG) understands

the data that a telecom

nication arise, for example the

number of the connections involved

such as the time and place of a conversation. In the

Radio cell query require investigators from

the telecommunications providers all

traffic data relating to a specific

ten period in the area of certain func-

cells were registered to offenders

identify. Doing so regularly

unavoidable also traffic data of third parties,

Namely those persons raised who

themselves – without being accused or

times - in the queried radio

cell with her mobile phone

to have. § 101a paragraph 6 StPO sees a

Obligation to notify the parties

ten of the affected telecommunications

before. However, reference is made to the

options according to § 101 paragraph 4

StPO. § 101 paragraph 4 sentence 5 StPO

with the case that the ideas

ity of a secret investigation

person affected by the remedial measure

is known, so a notification

practically can only be done if before

through appropriate research

their identity is established. With that

does the standard not refer to a

denied, whose identity at this stage

of the investigation is already known

is, but on a coincidence of the

mediation concerned, not

suspected third party. Regarding the-

This group of people can investigate

gen the encroachment on fundamental rights both for the

target person as well as for other participants

deepen The legislature therefore has

provided for in Section 101 Paragraph 4 Sentence 5 StPO

a decision to the investigating authorities

transferred, especially since the identity of

affected persons often only with high

hem effort can be determined. Regularly

appeal to law enforcement agencies

to this and waive the notification

due.

In Berlin you can now go here

another, more privacy-friendly one

Path. Citizens should through the introduction

better informed of a transparency system

be mized when their phone data in

investigation procedure was recorded

the. This "cell query transparency"

renz system" (FTS) works in such a way that

one at a specially at the senate

administration for justice, consumer protection and

anti-discrimination information

mation place his mobile phone number in

an "opt-in list" (list of interested

declarations, cf. fts.berlin.de) deposited

can. After registration received

the mobile phone user a notification

about capturing his number if

these as part of a radio cell query

ge by law enforcement agencies

Cellular operator was queried. the

However, you will be notified via SMS

only when the preliminary investigation

has ended, i.e. either charges are increased

or the proceedings have been discontinued

became. The notification contains i.a.

Information about the date, the time, the

approximate place and the basic legal

lay the radio cell query.

 From a transparency perspective, I think so

AGV for extremely innovative and recommendable

urgently, the introduction in Ba-

to examine den-Württemberg seriously.

First contact with

Ministry of Justice gives rise to certain

Hope. From there I was given

shared that they first wanted to experience

report of the Berlin Senate

wait and then “if necessary

in association with the other state judiciary

administrations” to decide. This one

restriction is expected

to a postponement of the deployment

lead the never-ending day. here

I demand more courage from the state government,

to put yourself at the top and in the spirit

a progressive, citizen-friendly one

management to set an example.

2.2 Eurodac

Not only at federal level and at

ne of the countries have security authorities

Files with personal data.

Also at the European level

various purposes information system

teme created the basis for

effective cooperation between

competent authorities in each individual state

form the

That dealings of national authorities

with personal data in the European

cal context also needs to be checked

as with purely domestic processing

gene, is obvious. In certain

the European legislature is sufficient

regular checks by the national

len data protection supervisory authorities explicitly

required. This also includes the

supervisory authorities of the federal states are affected,

as far as the use of these databases

ken goes through the respective state police.

In order to comply with this control obligation,

my office has first of all

European

fingerprint identification

ment system Eurodac.

To help identify the

Responsibility according to the so-called Dublin-III-Ver-

ordinance that regulates which Member State

the EU for the implementation of an asylum

responsible for driving, was established in 2000

the establishment of the fingerprint data

bank Eurodac decided the 2003 den

started operation. The two EC regulations

the Eurodac procedure

were regulated in 2013 by the from the

Regulation (EU) No.

603/2013 of the European Parliament

and Council of June 26, 2013 on the

Set up Eurodac for matching

fingerprint data for the purpose of

effective application of the regulation

(EU) No. 604/2013 determining the

teria and methods for determining the

Member State responsible for examining a

by a third-country national or

stateless person in a Member State

applied for international protection

is responsible and above the security

and law enforcement requests

Security and Law Enforcement

authorities of the Member States and Europol

on the comparison with Eurodac data (OJ

L 180 p. 1; hereafter: Eurodac-VO).

The primary purpose of the Eurodac Regulation is to

determining the identity of persons,

who have applied for asylum or who

galen crossing the external borders of

EU were picked up and to determine

ment, whether a third-country national or

Stateless person residing illegally in a

member state is already in another

applied for asylum in another Member State

Has. In Eurodac are essentially

Fingerprint data saved. On to-

question can the information be given whether

the requested person is already in one of the

Member States submitted an application for asylum

would have.

Eurodac-VO extended so that

also the law enforcement authorities

Access to the Eurodac database

Purposes of criminal prosecution and

defense was made possible, as far as it is

to terrorist offenses or otherwise

serious criminal offenses (Article 19

sentence 1 in conjunction with Article 1 paragraph 2

Eurodac Regulation). In individual cases, the

ask a reasoned request that the

formal and content-related requirements

of Article 20 Paragraph 1 of the Eurodac Regulation

Fulfills:

• Formally, other data must first

(national fingerprint data

vi

queried

share

tenbanks,

sa information system)

("query cascade").

PRÜM research,

• The content must be about terrorist or

other serious crimes (1),

• the

adjustment

got to

concrete

be required (2) and

• there must be sufficient reasons

genes, which allow to assume that the

soon become essential for prevention,

uncovering or investigating any of the

contribute to the offenses in question (3).

The existence of these conditions

is the responsibility of the data

protection supervisory authorities (Article 30

sentence 1, Article 32 paragraph 2, Article 33 paragraph

sentence 2 Eurodac Regulation).

As part of our exam, we let ourselves

from the Baden-Württemberg State Criminal Police Office

save the (standardized) requests

Eurodac research from 2018

submit. It is a total of

16 operations. In neither case did they arise

for us indications that cast doubt on the

are the legal requirements for

would have justified the database comparison:

• In all cases was before the application

the

Run through "query cascade".

been. In terms of content, it worked in all cases

to law enforcement measures.

• The requests

lay

the following

based on: Participation in a

ner

Union,

terrorism, gang theft, human

trafficking and homicides (1).

criminal

• The comparisons were made on a case-by-case basis

genes, with sufficient reasons

de passed for the assumption that

the comparison provide information

that might be essential to the pursuit

of these offenses would contribute (2).

.

• Finally, in all cases, the

justified suspicion that the

assign a person category

arrange goods by the Eurodac Regulation

are recorded (3).

The result was the handling of the police

with this information system therefore

not to complain about.

2.3 Insulting songs in the

Football stadium

Anyone who watches football matches on TV

looks, gets next to the actual

play on the lawn regularly

also a glimpse into the spectator

behavior – in picture and sound. stadium

viewfinders are so far for an unlimited

Generally recognizable and

in case of doubt also identifiable. image and

Sound recordings of sporting events

are an integral part of the offer

public and private television stations.

No stadium visitor would think

 such transmissions under the

from the point of view of data protection in question

to deliver. But sometimes it is different

then seen when a club

dionhappens optically and optionally

also acoustically documented, or if

this is done by the police. It says

the not unjustified concern in the background

reason that these recordings are

case disadvantageous for the person concerned

measures are used. So too

in a case where we deal with a

difficult had to deal with, in which it was about

the image and sound recording of "slander"

sang" in the stadium of a football club

the 1st Bundesliga went.

A Baden-Württemberg football association

one managed in the past too

because of the financial commitment

a private person promotion to the 1.

Bundesliga. This was repeated in the

criticism and leads to massive hostilities

of the patron by fans of guest

one who engages in foul insults

expressed. Neither the club nor the

Addressee of the insults wanted this

continue to accept. In order to prefer

hen, were image and sound recordings that

during the game with appropriate

technical facilities of the association

were made, used. For this must

you know that the German football

bund the clubs of the 1st and 2nd Bundesliga

as well as the 3rd league and the regional leagues

Provision of a video surveillance system

ge committed in their stages, which of

Police made available for use

must become. Not mandatory and

Microphones, on the other hand, are not common. That

one in the present stadium

is installed appears to be related to the local

some special features together. like that

be it, in any case it came with a foot-

ball game back to the - unfortunately usual

- foul insults. The police took

this for the occasion, from the video recordings

of the guest fan block individuals who

participated in the insults

pick out and their data both

the club as well as the injured

to share. The club then imposed

Stadium bans and the injured posed

prosecution for insult.

It is a matter of data protection law

the image and sound recordings for personal

name-related data. For personal

zug it is sufficient that a person whose

specific identity is not (yet) certain,

by linking with additional information

functions can ultimately be identified

can. In the present case, the police

individual people from the guest fan block,

which can be seen in the insults

involved, with the help of so-called scene

other visiting club officials are investigating

could. Participation in the insults

gene could be detected by

the sound recordings with the lip movements

were compared. The club and

the injured person then received the information

from the police so that they can

could assert claims. Of the

Personal reference of the image and sound recordings

here for all three responsible

chen be accepted as they each

had legal means at their disposal that

allow the persons concerned

based on additional information about the

Third party (officials or police with knowledge of the scene)

decreed to have it determined (on this:

ECJ, judgment of October 19, 2016, C-582/14,

Celex no. 62014CJ0582, paragraphs 47, 49).

For the question of data protection law

Justification of this data processing

the following was determined by the police

to deliver:

The police take on both tasks of

driver defense and criminal prosecution

true. In one case, the basic

Police Act, in the other case according to the

Code of Criminal Procedure. In individual cases

dual-purpose measures

the (recognizable) reason or aim of the

police action and, if

if to determine its center of gravity,

whether the disputed measures of

security or law enforcement

served. In this case, that was something

complicated, which is because the police

show law at football events though

basically image and sound recordings

leaves, but only for the purpose, in

to be able to intervene in good time in the event of

to ward off the danger. Now was-

de on the part of the police but admitted, at

Insults during football game

not wanting to intervene immediately

as this increases the risk of escalation

hold. The sound recordings were pure

criminally motivated. on the police

law as the legal basis for the sound

so you couldn't take it

appointed. Rather, the extent to which

Investigation general clause of § 163 of

Criminal Procedure Code (StPO) turned off, the

according to the police also fundamental

ge can be for sound recordings. This is

not without controversy, but could of

are not completely excluded from us.

In particular, from our point of view, the

Special regulation of § 100f StPO (acoustic

cal surveillance outside of residential

space) not relevant here, since it, as

the diatribes were recorded, yet

no accused in the legal sense

no. However, since the initial

suspicion of a criminal offense (insult) im

room was against § 163 paragraph 1

Sentence 2 StPO (“Investigations of any kind”) as

Basis for the sound recordings nothing

to remember. The (optical) video surveillance

Investigation as such, on the other hand, could refer to § 21

Paragraph 1 sentence 2 number 2 of the police

set (PolG) ("if on

due to the type and size of the event

genes and accumulations according to experience

significant dangers to public safety

safety can arise").

On the part of the association was of the following

to go out:

According to Article 6 paragraph 1 subparagraph 1

Letter f of the basic data protection

ordinance (DS-GVO) is processing

lawfully if they are to uphold the

legitimate interests of the person responsible

chen or a third party is required, so

far not the interests or fundamental rights

and fundamental freedoms of the persons concerned

son, the protection of personal

Data require prevail. Here came

we came to the conclusion that the association

was required, image and sound recordings from the

dion happen to produce and from the

police to collect the names of those

who violate the stadium regulations

had.

The club has the domiciliary rights at the stadium

on site to. It includes the power

to decide who is in the stadium

on area stops. The owner of the

right is therefore entitled to its

safeguard necessary measures

seize, d. H. to refer interferers and

them entering for the future

state that a house ban

speak. An observation on perception

Agreement of domiciliary rights serves both one

preventive as well as a repressive one

Purpose by firstly violating

the house rules or even criminal offences

the area by deterrence

hinders and on the other hand the persecution

civil claims or the criminal

tracking by evaluating the recorded

footage taken for the purpose

be made possible for the preservation of evidence

(OVG Lüneburg, judgment of September 29

2014 – 11 LC 114/13 –, juris).

51

LfDI BW - 35th activity report 2019 - 2. Internal security The interest of the association in being

Being able to exercise house rights can

recognized as legitimate in this sense

will. According to § 11 number 7 letter

d of the General Ticket Terms and Conditions

ments (ATGB) of TSG 1899 Hoffenheim

are (among other things) obscenely offensive or provocative

offensive slogans are prohibited. ver

The association can object to this in accordance with §

11 sanction number 9 and 10 ATGB,

up to a stadium ban. By-

Setting the domiciliary rights requires the

Processing of personal data in

a form that is appropriate to the proof

to obtain legal certainty of the infringement

bring. So it is crucial

the result of a balancing of interests

on. It should be said that the interest

especially of those who intentionally

lich against those known to them and by

terms and conditions accepted by them

violate it, in the event of a violation

against sanctions

to remain, rather to be rated as low

ten is. That image and sound recordings on

take place on the stadium grounds, § 11

Number 8 ATGB pointed out; this is the

known to every stadium visitor

attributable. Also, the fact that

video surveillance in football stadiums

takes place, generally, but at any rate

regular visitors to football matches

len, are assumed to be known

(Recital 47 of the GDPR). To the

to others, the insults are

public and for an indefinite circle

perceptible, which incidentally

is intended and in this respect leads to a

general reduction in the need for protection

leads (cf. also: BVerfG, decision of 9

October 2002 - 1 BvR 1611/96 -, BVerfGE

106, 28-51; ECJ, judgment of 04.05.2017,

C-13/16, Celex no. 62016CJ0013). In addition

are insults criminal

did. The fundamental rights to privacy and

Privacy are not a cloak, under

basically follow the violation of the law

loose could be committed.

The injured person was also there

to assume that he has the data of those

against whom he has filed a criminal complaint for insults

wanted to ask, on the basis of

Article 6 paragraph 1 subparagraph 1 letter

be f DS-GVO could legitimately raise.

The power of the police to name the

the club or the injured party

ten, we took §

475 paragraph 4 StPO or §§ 406e, 385 paragraph

Clause 3 StPO.

Ultimately, we came to the conclusion that

none of those responsible

has acted incorrectly under intellectual property law.

2.4 Checking the implementation of

divisions of the prosecutor

about the outcome of the

according to § 482 StPO

(MiStrA No. 11)

Since the storage of personal

Data in police files in proceedings

rens settings regularly subject

data protection checks

is our authority and we in the

past in the context of case-by-case

several times data storage

ments in the police information system

POLAS were able to determine the due

the public prosecutor's office

disposal should have been deleted,

we decided to use the police

security and deletion practice of such

Procedure based on random samples once

to look at more closely.

Case files should be included in our examination

are included, which are

authority according to § 170 paragraph 2 of the penal

innocence or were hired because

because no criminal offense was committed. To

§ 482 paragraph 2 sentence 1 StPO informed

the public prosecutor's office the police

en who dealt with the matter

about the outcome of the proceedings. On-

Based on this notification, the

Police on further storage in

police information system POLAS. the

Storage of data from investigative

however, moving in POLAS is only permitted

if a suspicion is justified

can. This is not the case when fact-

suspected by the public prosecutor

decision has been cleared.

For the storage of data from

mediation procedure is primarily § 38 of the

Police Act (PolG) is decisive. In from-

Sentence 2 says there: “For preventive purposes

Combating criminal offenses is the

protection, modification and use of

personal data up to a period of

he required two years if on

Reason actual evidence of

there is a suspicion that the person concerned

son has committed a crime. Such a

There is no suspicion if the affected

ne person in criminal proceedings legally binding

acquitted, the opening of the main

proceedings against you incontestably

refuses or the proceedings are not only provisional

fig is set and himself for the reasons

the decision shows that the affected

fene person does not or does not commit the offences

committed unlawfully."

files sent to government offices

However, there are also procedures that follow

§ 170 paragraph 2 StPO were set,

but because the factual

unlawfulness or guilt

could be proven. Since in this

sen cases of suspicion that the offense

was committed, usually not

is cleared and a residual suspicion according to §

38 paragraph 2 sentence 1 PolG

can, with this type of setting is a

Storage of the data for a period of time

allowed for two years. If actually

There are indications that the

continue to commit a crime in the future

is, the data according to § 38 Ab-

Clause 3 PolG also stored

be cherted.

Since we are from a public prosecutor's

finally sent procedural files

were terminated on the grounds

were det that factual,

unlawfulness or guilt after

were instructable, we demanded of this

another ten more files with the

hiring justifications to be examined

after. A few were among the

from the other prosecutors

sent files but also procedures,

due to a procedural obstacle

have been set, e.g. B. because no penalty

application has been made or is already

tion had occurred. A procedure was

according to §§ 374, 376 StPO due to lack of

the public interest on the private

dismissed.

For our test we requested

a total of five prosecutors each

ten case files from the area

of the general departments that are in

the months of September to November

2018 most recent (overall and final)

terminated for the above reasons

became. Among the officials

We decided not only to

finally based on our test criteria

speaking events at the police headquarters

sidien to ask, but us incidentally

also see how the police in the

whose operations with regard to a further

ren data storage had decided.

Of the 60 sent

 driving files we closed in advance but 16th

Cases out because the criminal charges are not from

the state police but by others

authorities or private individuals directly

the public prosecutor's office were sent

the public prosecutor's office itself

had initiated treatment procedures or because

the investigative procedure only

directed towards unknown persons

te. With regard to the remaining 44 procedures,

we turned to a total of six

liceipraesidien with the request to provide us with information

about existing data storage

these processes as well as the respective

to give storage modalities.

Among the 44 requested procedures,

29 cases were found, which due to

dismissed innocence or therefore discontinued

were noisy because the displayed behavior

the public prosecutor no criminal

stood had fulfilled. From these procedures

were only total on the part of the police

18 operations by means of a criminal complaint

presented to the public prosecutor,

ter also three traffic offences. In the

other procedure was apparently already

assumed by the police

that no criminal liability of the accused

or there was no criminal offense and the report

only in the form of a report by the public prosecutor

shank submitted, so no at all

data storage in POLAS

became. Traffic offenses are

additionally not saved in POLAS.

Fortunately, we were able to

that none of the requested investigative

procedure, which is due to the operative part of the

public prosecutor’s recruitment

cannot be stored further

allowed, was stored in POLAS.

For other reasons for hiring

ment procedures were

mainly data storage in POLAS

against which there are basically no objections

de could be collected. However, fell

also here again that sometimes too long

ge storage periods were assigned, in particular

special if the preliminary investigation

in the compound file "Kriminalaktennach-

white” (KAN) were saved. About the-

We already had this problem in ours

34. Activity report related

with the control of the allocation of the

lung support note "HWAO"

reported. For the cases now identified

a ten-year storage

frist fixed thing in view of here

underlying facts and

especially due to the statements in

the public prosecutor's office

disposal was disproportionately long. So

became e.g. B. in the case of a displayed cor

perjury offense in the hiring

stated that not

could be made whether the accused

attacked or just against one

attack defended. In another

case was the accused of extortion

solution has been reported. In the

the cessation order informed the state

to ensure that the news

would have contained hints that

indicated that the accused had

may attempt to recover the injured party

to blackmail or at least to force

however, the content of the messages is not

been clear. In another case

for aggravated extortion

the public prosecutor stated

that the statements of those involved

verbal and the information of the business

some of which were not credible.

Due to the underlying material

behave and in particular the formulation

We see the public prosecutor's efforts

a ten-year storage period in these

cases as disproportionate. In the

Decision about the storage period must be made

always consider the individual case

files sent to the public prosecutor's office

we could see that in most

th procedure an MAV with reasons

the police were ordered to

are in the still saved cases

but only then a justified

there was a court order if the order

affidavit in paper form. In the

majority of the procedures

only sent electronically and

a setting abbreviation is transmitted, which

ches in the cases concerned

reason for the position "procedural obstacle" or

“Factuality, illegality

or guilt cannot be proven". Ie

only in one case was it reported that

in addition to the electronic MAV also an in

paper form was received.

Our examination has shown that at the

Implementation of the MAVs no fundamental

problems related to the

temporal storage in POLAS and

the preliminary investigations that are due to the

public prosecutor’s recruitment

addition no further storage authorization

were also deleted from POLAS.

However, it turns out again and again that

for determining the storage period each

individually evaluated and checked

whether the specified storage period

based on the special circumstances of

is really proportionate on a case-by-case basis. in the

Doubt should be

order of the public prosecutor

was not transmitted, this requested

and included in the decision

will.

even if for extortion de-

likes according to § 38 PolG i. V. m. § 5 paragraph 2

Number 2 DVO PolG basically one

ten-year storage period would be permissible.

We informed the two responsible police

zeipräsidien our view regarding

of the selected storage periods with and ba-

about the allocation of storage periods

to be critically examined again. a butt

license head office has already informed us in writing

that it shares our opinion and

a reduction in the storage period

let have. The written reply of the

their police headquarters is currently standing

still out.

The cases mentioned show that

the storage of procedures by the part

be hired by the public prosecutor

often also the justified adjustment

disposal may be relevant to at the

determination of the storage period

to maintain moderation. The transmission

a reasoned hiring order

on the part of the public prosecutor's office, however

not intended in every case. In § 482

Paragraph 2 of the Code of Criminal Procedure states that the state

administration: "She informs the police

hear in the cases of paragraph 1

the outcome of the proceedings by

division of the decision formula, the

outgoing body and the date and

the type of decision. The Übersen

the notification to the Federal Central

gister is permissible if required

also of judgment or one with reasons

provided hiring decision."

The question in which cases the transfer

reasoned hiring instructions

tion appears necessary is open. in the

We were interested in the context of our examination

therefore whether the MAV on the part of the state

administration electronically or in paper form

sent by the public prosecutor

was and whether the hiring order

3.1 Everything ready for the inspection? – video surveillance in fitness studio

There are numerous recurring

complain about cameras in gyms

bye. Even in changing areas

which still have cameras attached. the

written control five randomly selected

selected companies confirm the impression

a comprehensive monitoring of the

Hobby athletes, however, only partially.

Already in the 33rd activity report we

in detail about the legal framework

monitoring fitness studios

directs. The high number of complaints

gave the impression that in almost all

Studios surveillance with cameras

takes place. were checked without cause

now five randomly selected studios and

different size, position and orientation

tion.

Three studios told us no over-

use surveillance cameras. in one

small gym in a rural area

with only four full-time employees, a large part will

of the training area is permanently monitored.

Whether the monitoring of recreational athletes

is also required is not yet clear. the

Reasoning, after which a waiver

on the cameras an additional personal

workload of up to 560 hours per week

would arise and ultimately the

drive would have to be adjusted, could

not convince us. Is privacy for

the operators a foreign word? - Whole and

not at all. The exchange with the data

protection officer shows that

one feels very comfortable in the small company

dealt with the new law

Has. There may be a mis-

understanding of range

the traffic safety obligation. For protection

the customer from any inconvenience

safety and every imaginable misfortune

Neither do gym operators

obligated. So always be careful

yourself when you exercise!

At the fifth controlled studio,

if it is a franchisee

with 24-hour operation. First had

we wrote to the franchisor.

Their lawyer referred us to the

franchisee. Contractual requirements

with regard to a possible video

guards would not be made. If a

franchisee of his client video

use cameras or not, don't lie in

the sphere of his client. The answer

the franchisee is still pending. It

wouldn't surprise us if we

soon a letter from an old

would get to know: The one already mentioned

Lawyer, this time under the letterhead

a data protection Gm-

bra. According to the website

is the data protection officer

borne by the franchisee.

The GDPR includes the framework for fines

data breaches increased significantly.

This appears to be happening in the fitness industry

but not yet to have got around-

ben. We continue to receive complaints

those of athletes who use video surveillance

in changing rooms. One

Surveillance reaches into the private sphere here

the athlete one, which is why it is one

of the most intensive interventions in personal

property rights. The ones worthy of protection

The interests of those affected prevail

these areas. A data processing

is therefore also in the case of documented

guardianship interests unlawful.

 Even if there are still many complaints

received, show the already carried out

ten checks: the operators of fitness

studios are in terms of data protection

not all top fit, but capable of learning. we stay-

ben on the ball.

has mostly not taken place. mostly are

Information signs available. However

these do not usually address the

demands of the supervisory authorities.

Result of the written checks:

3.2 Our daily bread –

video surveillance in

bakeries

There have been complaints about the for years

Video surveillance of employees in

bakeries with us. have this year

we took a closer look: at controls

on site and in writing.

We were unannounced in 26 bakeries

on site. At fifteen companies we have

written checks carried out. When

is surveillance allowed? a

buyer explained it to us as follows:

"I always thought it was for safety

may be monitored. But if

I'm being mugged now, then help me

not that either. This is way too slow.

It's always like, 'You have to

sign that now'. But I think-

I don't have to. But what

should you do it at work? I

always say: trust is part of it."

With that she summarized the most important aspects

short and concise together. Detailed

and in technical language you will find more about this

in our publications on video

monitoring.

Result of the on-site checks:

The purpose of the surveillance

was mostly unclear. the behavior

and performance monitoring and education of

employee theft was only

cases expressly stated as the purpose

give. Information for employees

Almost all establishments that use cameras

want to use the recording

investigating crimes committed by employees

ren or pursue. Documented

starting points for a specific suspicion

have not yet been able to

be rejected or are completely inadequate

according

Smaller bakeries often do without

Cameras – even if the

boss is not always on site. a

buyer explained to us: “We don't have any

Cameras and we even need them

Not. Our boss trusts us. We have

a great boss.” For lack of

for a violation we have the content

Unfortunately I didn't get to know her. if its

Employees speak of him like that, he has to

be a very happy person.

In some establishments with many branches

regular monitoring of employees

right system. A company in the field of

Security technology is on surveillance

specialized and has several branches

alkettes to its customers. Instead of his

Customers explained to us the manager

the necessity of its products at the

lefon: "Simple housewives should

don't reach into the cash register. Frequently

the one left by the man. If

If you have children, you have to think about

whether you buy the milk for 1.10 euros or for 80

buy cents. These are people who are financial

need. They take money out as best they can

goes. She thinks: It doesn't hurt anyone

the boss comes with the Porsche anyway-

hazards. When it comes out, excuse me-

to be reported." The statement presented here

general suspicion against all employees

run into the businesses of his customers

is of course anything but that

legally required to document

the indications for the justification of

a suspicion. And out of responsibility

are the bakeries with a position

action by the security company, of course

Not. Responsible in terms of data

General Protection Regulation is and will remain the

bakery itself. As far as an order

processing agreement has been submitted,

are also here very important

gene left open: technical-organizational

rical measures to protect the data

- None. The controlled establishments

must assume that we are with

not be satisfied with such answers.

Some customers draw consequences.

A customer informed us as part of her

Complaint with: "For several weeks

I will not buy from this bakery again

a. Before that I was there almost every day."

While many small, owner-managed

can do without supervision,

relies on a whole series of branch

operated on questionable business model

le of security technology. employees

are under general suspicion for no reason

placed. We counter this with supervisory

legal measures and in some

Cases also with fine proceedings.

3.3 Legitimate Interests

Prepared for operators of video cameras

it rarely troubles an interest in

to monitor people

wear. Do you often want to

breakage, theft, vandalism or

protect against attacks. Many operators do

find it very difficult to

legitimate interest towards the supervisory

authority to justify and

to explain.

A requirement of a lawful

video surveillance is that the

security measure of maintaining a

legitimate interest of the person responsible

chen or a third party. under consideration

here comes the protection against burglary,

theft, vandalism or assault.

These are common goals of a video surveillance

watch. As a legitimate interest

for the operation of a video surveillance

investment ideal, economic or legal

can be of a nature, these interests are

also generally worthy of protection. Justified

is a surveillance interest only

then, if lawful, sufficient

clearly formulated and not purely speculative

is (cf. Opinion 06/2014 of the Arti-

kel-29 data protection working group on the concept of

legitimate interest of the processing

processing of those responsible in accordance with Article 7

of Directive 95/46/EG (WP 217), p. 32,

p. 70.). The Federal Administrative Court

leads in its judgment of March 27, 2019

(Az. 6C 2.18, Rn. 28) from:

“The viewpoints of prevention and

Investigating criminal offenses generally requires

legitimate interests within the meaning of § 6b paragraph 1

No. 3 BDSG old version (editorial notes

kung: The legitimate interest is found

now in Art. 6 Paragraph 1 Letter f DS-

GMO). You can set up video surveillance

but only then as objectively justifiable

justify if a dangerous situation

exists, which over the general

risk goes beyond. Such a hazard

can only be derived from actual

nits yield; subjective fears

or a feeling of insecurity

not from."

For video surveillance operators

Incidents in the past or others

Events that constitute a dangerous situation

can justify tiv, must opposite

be proven to the supervisory authority

the. Such evidence can only

from a specific description

speaking incidents arise. At least

should include the nature of the event, the location,

the timing and frequency of

cases to be specified. A description

exercise should be as accurate as possible

for example with date and time.

Also specifying the amount of damage, a

description of the damaged object,

Damage reports to an insurance

tion or reports to the police

the importance of one's own

to justify surveillance interests and

for example compared to mere trivial

delimit crimes. Concrete Incidents

do not have to be with the monitor

themselves have taken place. in certain

ten cases, a dangerous situation can arise

also result from the fact that - with certain

temporal connection - comparable

incidents or assaults in the immediate

close proximity have taken place

ben. Here are incidents to prove from

which a temporal, factual and

local connection to own surveillance

development interest. Only in exceptional

case is evidence of a purely abstract

dangerous situation sufficient. For example

if there is a situation which after all

common life experience typically

is dangerous. For example in shops

shops that sell valuable goods

(e.g. jewellers) or those with regard to

property crimes, especially

are endangered (e.g. petrol stations).

Subjective fears or a feeling

of the uncertainty justify

no legitimate interest in a

ner video surveillance. As a feeling, "Si-

security" incomprehensible. Feelings can

cannot be quantified or empirically

point. A person can join one

certain places feel unsafe, though

a danger does not actually exist or

is rationally justified. The one who is unsure

cher "feels" cannot be automatic

the right to be granted, quite real

encroach on the personal rights of third parties

fen. Would an immeasurable feeling for

such an intervention might suffice

Monitoring measures continuously

sharpens and video surveillance boundless

be extended to public spaces.

The right of data subjects to information

self-determination would almost

evaluates. A sentimental assertion

would be enough to limit it.

The interest, the felt security

increase, can therefore only

materially justifiable interest.

For the same reason also justifies

an apparently deterrent effect

taken by video surveillance

men no permanent and occasional

encroachment on the rights of third parties.

A legitimate interest in a video

monitoring must be concrete and

be demonstrably justified. incidents

events and damage are therefore

to be documented (date, type and place of the

incident, amount of damage, etc.). criminal record

gene and insurance notifications should

to prove the monitoring interest

be kept.

3.4 Guidance on

video surveillance

The operator of a video surveillance

is obliged to comply with the

to comply with data protection regulations. The legal

Testing of an installation is case by case

different and not necessarily easy.

The operator must have indefinite legal

identify the interests of those affected

and this in individual cases with his own

balance surveillance interests. Around

the operators to comply with legal

cher regulations to facilitate and them

ways to use it legitimately

video cameras, publish

and revise the supervisory reports

constantly hear guidance on the

different topics. Especially

the nationwide working group on video

surveillance – under the direction of Ba-

Württemberg stands - delivers in its

constantly new in a work area

and updated information material.

Video surveillance by public

Jobs in Baden-Württemberg

graffiti on the town hall wall, a damaged

park bench or a littered school

court. Improper Conduct or Vanda-

ism causes costs and is – often

also for residents - annoying. To dem

to meet, is often and quickly the in-

installation of a video surveillance system

considered or even in general

so decided. "What's that talking?

versus? Cameras monitor us too

otherwise at every turn.” like each other

decision makers think.

A public body must

be aware that they are equipped with video surveillance

genes in fundamental rights of filmed persons

intervenes. This intervention can only

be done cheaply when a data processing

the requirements of a legal basis

ge fulfilled. In Baden-Württemberg since

June 2018 the admissibility of a video

surveillance of publicly accessible spaces

regulated in § 18 LDSG. The norm gives way

in some places from the previous

write off. On our website we have

an orientation for the application of the regulation

published. She supports

public authorities in the process of

monitoring in accordance with the

according to the DS-GVO and § 18 LDSG

judge. The rules are explained

the requirements of a transparent

Information signs shown and on

technical and organizational protective measures

took pointed out.

Use of bodycams by private individuals

security company

Prepare private security companies

their employees now with mobile

common body cameras, so-called body

cams off. Lead as surveillance purposes

they protect employees from over-

seizing or obtaining evidence

for civil claims. vi-

le hope for a deterrent or

de-escalating effect of the cameras. Of the

private use of bodycams entails

some privacy risks. at

use in public places

there is a risk that those affected by their

fundamental rights only to a limited extent

make need. In addition, passers-by have to

detailed film or sound recordings

fear if equipped with bodycams

te security forces patrolled on a

to do in a well-visited area

or crossing a crowd.

Depending on the attachment and use of the

Camera can also covert it

data processing and monitoring

measures come. The use of a

Bodycam by private security company

accept is Art. 6 paragraph 1 letter

f GDPR to measure. What from the point of view of

supervisory authorities in the case of such

set of body cameras should be noted,

you can in our guide

read. This is on our website

released.

Committee on Video Surveillance

watch

At the European level, the European

sche Data Protection Committee in July 2019

a guideline on video surveillance

taken. After the procedure for

Public participation completed

is, the content of the guideline will be

monitoring systems throughout Europe

turned. The guideline becomes the interpretation

the GDPR

for video surveillance

have a significant say. The document

is published on the website of the data

reference

(www.datenschutzkonferenz-on-

line.de) published.

video surveillance through

non-public bodies

To the European guideline on video transmission

wachung will change in the coming year

Release of an updated Fas-

the orientation guide "Video transfer

monitoring by non-public bodies"

connect. The guidance will

the regulations of the BDSG, the DS-GVO

and current court decisions

thematically and practical hints

wise for examining the legal facts

give stocks. She will beyond

a large number of individual cases

included and the requirements of a

video surveillance in employment

handle.

61

LfDI BW - 35th activity report 2019 - 3rd video surveillance 62nd

LfDI BW - 35th activity report 2019 - 3. Video surveillance 4. Traffic

4.1 Traffic

In the field of transport is mainly after the

Introduction of the General Data Protection Regulation

tion (DS-GVO) an immense increase in the

Complaints about fine procedures

been listed. Sensitized by

the DS-GVO have not a few bur-

asked for the first time whether the

authorities against data protection regulations

lungs violated when they affected

by means of speed monitoring

record locations or if the municipal

che enforcement service for illegal parkers

License plate photographed.

The data processing of the fine

le is done for tracking purposes

and punishment of administrative offenses

in this area is not the data

tenschutz basic regulation, but the

Directive RL (EU) 2016/680 relevant,

which, unlike the GDPR, does not immediately

applicable, but only in domestic

had to be properly implemented. the

was set by the state data

Protection Act for Justice and Fines

hear (LDSG-JB) from May 15, 2019. The

State data protection law for the judiciary and

Fines regulates that particular

Federal or state legislation

country. The administrative offense

procedure is special in law

on administrative offenses (OWiG)

applies and this in turn refers to the

provisions of the Code of Criminal Procedure. In-

provided that the fine authorities and the

Employees of the regulatory office similar

powers such as law enforcement

the. You can identify a fact

and gather evidence.

As annoying as the nodules are, don't

any data acquisition that the citizen does not want

collection by the fine authorities

also a data breach. the radar

speed measurement controls

and also the photos are of illegal parkers

through the investigative principle of fines

monetary authorities covered.

4.2 Authorities rely on postcards

The driver's license office of a district office

probably sent mail for reasons of cost

cards to applicants. on this post-

cards were not just the file number

and the name of the clerk at the

driver's license office, but pre-printed

and to tick which sub-

were still available at the driving license office

to put on This ranged from medical

Certificates of Eyesight

up to other medical certificates

genes and expert opinions for granting or

Renewal of driver's licenses

the driving license regulation. handwriting

Lich could still open fees and

further notifications to the applicants

to be entered.

It was particularly piquant in the case that most

Ner authority was reported that the

Applicant handwritten on the post

card was informed that he could not as

Accompanying person for accompanied driving

be entered.

Through the open postcard, the

confidential transactions between

citizens and the administration

processed in a way that

Acknowledgment of uninvolved third parties

enabled by this procedure. With that

de the confidentiality and integrity of

particularly sensitive health

data violated. The regulations of the data

General Protection Regulation state that

only process data in the manner

tet may be the one appropriate

Security of Personal Information

measures to be taken are ahead of a

unauthorized access to the data

te protects.

It is actually obvious that

confidential information in public

return in principle in closed letters

envelopes to be sent.

My authority has not in this case

asked for an opinion, but that

District office immediately instructed that

communication of administrative processes

from now on only before the

carried out protected against third parties and

for notices to stakeholders in one

administrative procedure closed

NEN envelope to use as well as from the

Refrain from sending open postcards.

The district administrator immediately implemented this instruction

set.

4.3 Development of Artificial

Intelligence (AI) in the field

Traffic

The first data protection impact assessment

who accompanied my authority, found

lots of traffic.

An automotive supplier developed for its

ne customer algorithms for the autonomous

Drive. However, in order to train

are real driving and traffic conditions

required. Otherwise it comes to

System errors, resulting in fatal errors

of autonomous vehicles

can.

In our case, video data from Au-

tos taped out. be here

inevitably personal data

summarizes, be it people on the sidewalks

and to traffic lights, cyclists or others

Road users, as well as license plates

chen. Although an identification of the

sons or the car owner at all

is wanted, the data collection cannot

without a legal basis for the data

collection take place. The admissibility of

Data processing arises in this

special individual case from an interest

sen or fundamental rights and freedoms

prevailing over the data subject,

legitimate interests of the automobile

supplier within the meaning of Article 6 paragraph 1

Subparagraph 1 letter f GDPR.

In the balancing of interests in favor

of the automotive supplier found many

gates into account, such as

the personality relevance, the temporal

and spatial extent, an only small

authorized group of people that the

data will not be given to third parties

the as well as the technical ones used

and organizational measures. important

tig for the weighing of interests was still

that the rights of those affected are protected

den by using the recording vehicles

Camera icon and information about

are identified to those responsible.

In this way, the affected traffic

participants of their right to object

make use of on site by the Se-

can be deleted directly in the vehicle

the. The deletion of the video data is also

afterwards when specifying the place and time

possible.

The implementation of a data protection

assessment is also included in the

include food considerations.

The development and research of

new technology should not affect data protection

fail, however, is the development and

research is also not a free ticket, because

data protection principles and rights

managed to throw overboard. Will

64

LfDI BW - 35th activity report 2019 - 4th traffic data protection principles, which

comply with the General Data Protection Regulation

pretends to us, heeds and they are part of the

research project and process

(Privacy by design), then this can do that

confidence of citizens in

strengthen new technology and become one

not to be underestimated competition

lead advantage.

65

LfDI BW - 35th activity report 2019 - 4th traffic 66th

LfDI BW - 35th Activity Report 2019 - 4th Traffic 5th Justice

5.1 How do notaries fulfill their data

intellectual property information

and documentation requirements?

- Control campaign

To find out how responsible

verbatim with in the basic data protection

ordinance (DS-GVO) contained information

information and documentation obligations

deal with, my department has

of an unprovoked control campaign

No in May 2019, so after almost one

year since the General Data Protection

ordinance, twenty selected at random

notaries are asked to

instruct how to fulfill their information obligations

compared to that of a data collection

Data subjects pursuant to Articles 13, 14

comply with the GDPR and on the other hand,

their record of processing activities

to be submitted in accordance with Article 30 GDPR.

Procedure of the control campaign:

The obligation to my department

requested documents on request

increase, results regarding the directory

se of processing activities from the in

Article 30 paragraph 4 GDPR expressly

mentioned obligation to submit and regarding

Data protection information according to the

Items 13, 14 GDPR from the general

Obligation to support § 26 state data

tenschutzgesetz (LDSG), which also includes notaries

obliged to cooperate.

As already mentioned, the

mentioned information and documentation

duties at the beginning of the control action

on for almost a year. Think

department is therefore assuming

gene that the notaries - the organs of

Administration of justice and carrier of a public

office are – the relevant documents

already months before the control action

created by my office, so that

them to mine without much effort

Department can send and this

due to their, my department against

over existing support and

do the obligation to submit.

In fact, fifteen of the twenty

Notaries within the of my service

set a three-week deadline or

a few days later the requested documents

submitted.

Of the five other notaries, three have

within the deadline for a deadline extension

tion requested, but only in one of these

Cases were the documents within the

submitted an extended deadline.

Two of the notaries responded to the request

tion of my office at all

reacted and had to get to work

be inner, which then in one of

both cases also took place immediately.

Even in early November, so more than

5 months after the first request

my office, despite several

liger memories recalling the

Obligation to support in two cases neither

the data protection information according to the

Articles 13 and 14 GDPR nor the

record of the processing activities

according to Article 30 GDPR and in one case

only the list of processing

activities.

Regardless of whether the delayed pre-

depended on it in the individual cases

can be traced back to the fact that the notaries

according to the General Data Protection Regulation

existing information and documentation

mentation obligations or "only" most

ner office compared to existing

No obligation to provide support or submission

in the event of significant violations of data

protective obligations. Since against

Public bodies according to § 28 LDSG none

fines can be imposed,

against the above-described violations

data protection regulations

individual notaries as bearers of a public

chen office and judicial body

no administrative offences. There a

such behavior is not acceptable

table, I have both the Ministerial

for the judiciary and for Europe as supreme

Supervisory authority of the notaries as well as the

Chamber of Notaries Baden-Württemberg

calls for ensuring that the

Notaries in future both their information

and documentation obligations as well as the

to my office

meet the obligations.

Content control of data protection

information for data subjects in accordance with

Articles 13 and 14 GDPR:

The circumstances outlined above, that

the notaries the requested documents

late or even months after arrival

demand by my office yet

had not submitted, and thereby

resulting delay have

leads that so far only the content

Review of data protection information

ions for those affected under Article 13 and

14 DS-GVO could be carried out,

the examination of the directories of the processing

work activities that are very extensive

are, but only in the course of 2020

can be done.

The information obligations of responsible persons

Bodies pursuant to Articles 13 and 14 GDPR

GMOs that go far beyond the previous (national

nale) go beyond the legal situation, form the

Basis for exercising the data subject

property rights. Only if an affected person

son knows that personal data

processed through it, it can be yours

Affected rights, such as B. your information

exercise properly, also sensibly and effectively.

About what to inform those affected

are, results from the collection of personal

personal data at the concerned

Person from Article 13 DS-GVO and, if

the personal data is not included

the data subject himself but with

third parties, from Article 14

GDPR.

In both cases, if none

Exceptions apply, e.g.

• the name and contact details

the person responsible

• the contact details of any data

data protection officer (whereby notaries

always have to order one),

• the purposes for which the data

are to be raised or raised

have been used, as well as the legal

basis for processing,

• if applicable, the recipients or cate-

gories of recipients of per-

sun-related data,

• the planned storage period or, if

this is not possible, the criteria for

the determination of this duration and about,

• the rights of those affected (right to information,

correction, deletion, restriction

and objection rights as well

the right to data portability)

be specified.

When reviewing my office

data protection information submitted by notaries

information is mainly the following

favor:

LfDI BW - 35th activity report 2019 - 5. Judiciary With some of the notaries the

submitted

Privacy Information

only on the collection of personal

gener data in connection with

accessed the notary's website. Which he-

collection of personal data

the notary as part of the actual

tar activity, i.e. in connection

with the creation of draft documents,

the certification and execution of deeds

customer transactions or implementation

of consultations by the Informati-

obligation of Articles 13 and 14 GDPR

is also recorded, was in these days

data protection information, however,

spoken.

In addition, it appears mainly to

Topic data protection officer unclear

to give. So were in several

the submitted data protection information

regarding the data protection officer

only the general e-mail address/

Telephone and fax number of the notary

ats specified, so that an immediate

re contact of a person concerned

not with the data protection officer

it is possible. The data protection officer

However, te must be contactable directly.

Therefore, in the data protection information

at least one separate, directly dem

Data Protection Officer

assigned

to provide an email address.

In some cases, as a privacy

commissioner one notary colleague in

mentioned within the same law firm.

Notaries in a law firm or a

However, ro community can not

each other as data protection officers

to name. A notary as responsible

can also not in its own right as

Appoint data protection officer. This

would lead to conflicts of interest

to lead

and could not be with the function and

Task of a data protection officer

agree (Articles 38 and 39 GDPR).

Notaries in a law firm or shared office

shank are both for the area of their

Office as well as for the economic

and organizational area responsible

literal passage. A mutual naming

tion as data protection officer

in the economic and organizational

Area cause the respective active

future data protection officer at Er-

fulfillment of its duties as data protection officer

representative for one colleague at a time

also advises or controls itself.

For example, if questions about data

processing in shared data processing

working system treats or does it work

to have an implementation in common

IT system used, a member can

of the partnership/office community not free

advised by their own concern or

check. Here are independent and

technically experienced own data protection

instructed to order.

Since the control campaign was not

plans to be completed in 2019

could, but also because of already now

identified data protection violations

my office in 2020

deal more with notaries.

5.2 Implementation of the Directive (EU)

2016/680 in the judiciary

Already in my last activity report

I mentioned that the data

basic protection regulation for criminal

che and regulatory offenses

Procedure none and also in the area of

penal system only extremely rarely

tion finds, and that for these areas

instead, Directive (EU) 2016/680

contains data protection regulations.

A guideline must - unlike our

indirectly applicable basic data protection

order – transposed by national law

are set, insofar as this is not the case

carried out by federal law, by state

At the state level, this implementation is for

the judicial and fine authorities in particular

by the effective date of June 6, 2019

State data protection law for the judiciary and

fine authorities and by the same

amendment of the

Correctional Code takes place.

State data protection law for the judiciary

and fine authorities (LDSG-JB)

The state data protection law for judicial

and fine authorities is applicable to

the data processing of the ordinary

courts in criminal matters, the state

administrations and also for the processing

processing of personal data for

formation of administrative offenses and for

enforcement of fines by all

responsible public authorities

of the country. Contrary to what is sometimes assumed

the law applies in the area of fines

therefore not only for data protection

che offenses, for mine

office is responsible.

The state data protection law for

tiz and fine authorities also regulates the

Jurisdiction and powers of my

Office within the scope of the

law.

About the implementation of the Directive (EU)

2016/680 but contains the law

also regulations that are not immediate

serve to implement the directive, such as

e.g. B. under what conditions

Video surveillance in prisoner demonstration

areas of courthouses

is and a provision that it is in foreign

serving judicial officials under

permitted under certain conditions

Hazardous situations Devices with a

to use hearing function.

As in my last job

area, my orders were

think about video surveillance in-

arrested persons who because of a

Prisoner transport negotiation

of the correctional facility in the demonstration

le of the court, thence to the courtroom

and have to be brought back

sen, partly already in the revised

Draft of the state data protection law

for judicial and fine authorities from July

2018 considered.

At the time of the last activity

I wasn't aware of that,

that my demand was also met

men was the one provided for in the draft

Reference to the use of video technology

nik to specify in accordance with the guidelines.

In § 5 paragraph 6 LDSG-JB it is now

correspondingly expressly to §§ 55

and 56 of the Federal Data Protection Act

referenced in which the directive

(EU) 2016/680 information

and notification requirements implemented

have been.

Against the

seen legal basis for use

a monitoring function for mobile alarm devices

advise the lawyers working in the field

tiz employees (e.g. bailiffs)

should allow, in dangerous situations

their protection by means of suitable devices

to secretly make sound recordings

I also expressed serious concerns

(cf. 34th activity report, 5.1.1).

Unfortunately, the regulation is not without replacement

been deleted. Compared to the

draft version are the admissibility requirements

requirements for the production of secret

chen sound recordings in the now applicable § 6

LDSG-JB, however, has been considerably tightened

the.

 Since both the state data protection law

for judicial and fine authorities as well

the amendment of the prison law

books have only been valid for a few months,

can - due to the little experience,

that are currently available with these laws

– no statement made about it yet

whether the change made

implementation of Directive (EU) 2016/680 or

the adaptation to the data protection basic

regulation in practice or,

whether or in which points further changes

there is a need for change.

While provided in the initial draft

was that in the presence of a no closer

specific danger to protect the

judicial officers covert sound recording

Men made on site and sent to a

control center can be transmitted, re-

according to § 6 LDSG-JB, that judicial employees

only in the case of an urgent danger to life,

health or freedom exclusively

For your protection, audio recordings at the scene

Prepare and transmit to a control center

be able. The measure may - unlike

envisaged in the initial draft - however

only be carried out covertly

if there are indications that

the purpose of the measure would be jeopardized,

if the person concerned at the beginning

or in the course of the measure above in-

would be formed.

Amendment of the Correctional Act-

book

The judiciary is carried out for the purposes of

Enforcement and/or Protection

against and averting dangers to the

public safety. In this way it serves

to which Directive (EU) 2016/680

applies. Especially about this one

Implementing it in prison was one

Amendment of the Correctional Code

necessary. Sometimes one processes

prison but also to other

other purposes personal data.

In these rare cases, the da-

General Data Protection Regulation application,

why that

Correctional Code

also to the General Data Protection Regulation

had to be adjusted.

The amendment to the Correctional Act

buchs is also - like the country

of the data protection law for judiciary and penitentiary

monetary authorities - effective June 6, 2019

kicked.

6.1 The “List of Conspicuous Ones”

Through corresponding press reports

tion, we became aware that

the city of Tübingen "creative" ways in

dealing with migrants. These were

namely, if the city hears

comes that people from this group

pe get in trouble with the law, in

a so-called "list of the conspicuous"

recorded and stored. who on the list

te stands, must expect the more frequent

having to change accommodation and at

Contacts with authorities under special

attention to stand.

In order to be able to check whether this particular

re form of data processing the data

fulfills the legal protection requirements,

we turned to a detailed

Questionnaire for the city. their position

ment was anything but gratifying

enough Not only were some wrong

Legal bases stated. As far as

appropriate to the regulation of the state

tenschutzgesetzes (LDSG) regarding the

Data processing for other purposes

(§ 5 LDSG) was referred to, this

se misrepresented and regarding

of their application requirements

aptly rated. What the facts

te is concerned for inclusion in the list

lead remained unclear what the city about

under “Hazard reports” or “Incidents

with risk potential” understands exactly.

When asked where the data came from,

it said: “It is exclusively about

Information available to the administration

gene". At one point it was stated

that disclosure of information

from the list no successes, at other

It says that the integration

nagement in the accommodations

will. On the question of whether those affected

been informed of their data protection rights

the city referred to alleged

restrictions on the right to information

"according to Art. 15, paragraph 1 lit. c) and e) [DS-

GMO]”, which does not exist at all. One

according to Article 35 paragraph 3 letter b of

General Data Protection Regulation (GDPR)

mandatory before creating the file

required data protection impact assessment

tion was only promised.

The supposedly existing entry in the

List of processing activities

was given to us to this day, despite being asked to do so

not submitted.

In another letter we asked

the city to rely on a legal basis

to be determined and the existence of

to prove suspensions. from ours

View came at most § 5 paragraph 1 number

2 2. Alternative LDSG under consideration, after which

personal data belonging to a

specific administrative purpose

were, deviating from this, also used

may be used if this is “for defence

a serious impairment

the rights and freedoms of another

person is required". The city did

claims that the migrants included in the list

posed a danger to employees

the city. Our question went

whether there are concrete indications

for admitting that the listed persons

towards city officials ever

had become noticeable. in her answer

the city did not respond to this and

referred only to statistical surveys

genes about the probability of recurrence

in violent crimes. On our other

Questions, however, were no longer

gone After we compared that

Lord Mayor complained and on the

legal obligation of the city

had to support us in our work

zen, we received surprising news-

a letter from the mayor

he complained verbosely about us: We

would always ask more questions

don't be for the professionals in his house

more recognizable what answers we

expected what we wanted to be legal

not permitted and not dependent on the effort

Afford. We were imputed by

the city's approach to

compliance with data protection regulations

check fonts and thus our

comply with legal mandate

we endanger city employees.

This is absurd. Rather, it is true

that to this day because of the uncooperative

ven behavior of the city incapable

are to determine specifically whether what

going on there, is legal, or the city

to be available for advice,

for lawful data processing

to make possible.

The city's attitude of denial is

not only incomprehensible, she also gives us

Reason to take further measures

according to the basic data protection

order are available. The thing

may need some clarification.

6.2 Community Network

privacy

It was celebrating its tenth anniversary

Municipal Network Privacy at the

Administrative College Kehl. The network-

werk is a nationwide collaboration

closure of municipal official data

protection officer who has been since

2009 twice a year for a conference

meet at college.

In the beginning there were only about 20 people,

there are already more than 120 members.

They come from smaller communities

den as well as from big cities, rural
council offices and independent authorities
such as a port administration.
Although experts in data protection have
always new data protection problems
learn and questions. They discuss these
next in a specialist group, try
chen these to solve before you contact the
LfDI turn. "Old hands" with years of experience
Practical experience can thus newcomers
help and get into the difficult
facilitate matter.
There are also working groups
at the municipal umbrella organizations.
But overarching practices meet
women and practitioners only in this
ler network. Especially the experience
exchange regardless of the size of the
Authority is very profitable.
Such a network can also serve as a model
for other organizations and
associations (clubs, schools).
Important element of networking
is the one created by the conferences-
de personal contact. That's how they swap

the members permanently via an intra-
net portal of the network. On the-
sem will be specifically information for
municipal data protection officer
in
Baden-Württemberg held ready. the
Documents come from the members
and can be uploaded by them
become the
The LfDI supports to the best of its ability
the work of this network. He gives the
Possibility of selected questions in the
circles of conference participants not
could be answered, at the LfDI
suffice. As far as possible for the LfDI
was, his authority also sent reference
and speakers at the conferences.
LfDI BW - 35th activity report 2019 - 6. Municipal carrier of the network is the Kehler Aka-
demie e.V., one of the two training and
educational institutions of the university
throat.
75
LfDI BW - 35th activity report 2019 - 6th municipal 76th
LfDI BW - 35th activity report 2019 - 6. Municipal 7. Health and social affairs
7.1 Caution when shipping
emails

In addition to the legal question of whether e-mails

with personal data – if the

data subject has consented to this -

may be sent unencrypted,

care must be taken when shipping

of e-mails special care

is brought.

My department had

period with several complaints in

related to the delivery of

to receive e-mails from social service providers

grasp.

In one case, a job center had

on a case-by-case basis – upon express request

a benefit recipient due to the

Urgency of his matter - one

Notification via (unencrypted) e-mail

want to send to the service recipient.

Because of that email addresses

are often underlined

was made by the employee of the Jobcentre

ters an underscore in the email address

not recognized and the e-mail address

by misspelling. This "wrong"

E-mail address existed, so that a (un-

well-known) namesake of the performance

recipient received the e-mail together with the decision.

The authority concerned has the expertise

taken as an opportunity to

to issue the “Privacy Policy” directive and the

employees on the subject of "e-mailing".

inform to raise awareness of the

improve data protection.

In another case, an employee

of a youth welfare office by e-mail via

change of responsibility within

informed by a department. Unfortunately wrote

he indicates all recipients as "open" instead of this one

to put in "Bcc". So all recipients could

recognize who else received the e-mail

hold and thus also who had contact

to the youth welfare office.

Here, too, the authority concerned has

the consequence the employees regarding the

topic sensitized.

A third case was about that

a youth welfare office sent a message by email

to a parent and for information

a youth commissioned by the youth welfare office

gendhilfeträger had sent. So became

the commissioned youth welfare agency

Email address of parent known –

the parent had not consented to this

lit.

So quick and easy to send an email

is, this uncomplicatedness also

know risks. Therefore, when shipping

emails due diligence. through

E-mails can be encrypted, e.g. B.

in the case of the job center, can be prevented

that third parties

can be.

7.2 Privacy in the outpatient

and inpatient care

Home care

In the reporting period we were with the

Question concerned to what extent within the framework of

home nursing for billing

a complex wound care

sible health data such as photos of the

caring for the wound to the health

se may be transmitted. Furthermore was

to clarify whether this data is solely from so-called

"wound managers" of the health insurance

may be scored without the medical

nical health insurance service (MDK)

turn on.

LfDI BW - 35th activity report 2019 - 7. Health and social affairs Home nursing according to § 37 des

Fifth Book of the Social Code (SGB

V) includes the individual

che basic care, treatment care and

Domestic supply. on medical

among other things, the wound care

tion as treatment care by a

performed outpatient care.

The nursing service calculates the

th services then within the framework

of the contractual agreements with the

the patient's health insurance.

When it comes to wound care, however

between a regular supply to

distinguish that an average

Lich requires a lot of effort, and one

complex care that requires a time

requires intensive effort. for one

so-called "complicated wound care".

the contractual agreements with

health insurance company offers a higher reimbursement.

Accordingly, the billing

ment of this more complex service as well

a meaningful proof.

As a contractual billing basis

for the higher remuneration of a

tive wound treatment has been used up to now

concrete between health insurance and

the nursing associations

application form. This form saw i.a.

provided that an "extraordinary

vigorous representation of the elaborate

wound care as part of a

appropriate wound management".

becomes. This has been reported by some outpatient

ten care services understood that

them along with the application form

at the health insurance as proof of a

complex wound treatment

submit extensive documents

would have to typically the care

served in addition to wound findings, wound

also log photos of the wound. For

the transmission of the "necessary

lay" the application form provided that

the nursing service from the insured

obtaining consent. The care

dienst evaluates the documents sent

Health insurance then usually with the help

by her employees, specially

trained, so-called "wound managers". One

Forwarding to the medical service

the health insurance (MDK) finds only

as an exception.

In this regard, hired us

providers of outpatient care the question

whether this procedure complies with data protection law

be permissible.

We then discussed the process

the relevant health insurance company. Our

examination led to the following essential

technical data protection considerations:

It is doubtful whether the

de Collection of social data at all

in the form of a declaration of consent

can be justified. The regulations

of § 284 SGB V regulate conclusively, in

which cases the health insurance

is required to collect social data. one over-

Going beyond data processing

the basis of consent is

against - what the national legislation

In accordance with Article 9 paragraph 2 letter

a) and paragraph 4 of the basic data protection

ordinance (DS-GVO) for special cases

categories of personal data, in particular

special for health data

can - excluded. However,

the provisions in § 284 paragraph 1

Sentence 1 number 4 and number 8 SGB V

the collection of social data insofar as

than this to check the obligation to perform

the health insurance company or for billing

with the service providers is required

is. In the case of billing of a

walled wound care requires the

Health insurance company the additional data to

determine whether instead of a regular deed

a costly wound care

 was required and was carried out

with the consequence that she is the nursing service

to pay a corresponding

correspondingly higher remuneration

tet would be. The obligation to reimburse

usually results from claims

stipulations, the reason and the

amount must be available. The question in

what amount the health insurance company pays

is obliged to pay a surcharge

therefore from the authorization norms of § 284

Paragraph 1 sentence 1 number 4 and number 8

SGB V includes the provisions of

General Data Protection Regulation as a specific

cal member state provisions

pursuant to Article 6 paragraph 1 letter e) and

Paragraph 3 sentence 3 DS-GVO and according to Ar-

article 9 paragraph 2 letter h) and paragraph 4

Specify GDPR.

Furthermore, we presented to the

Health insurance regarding the scope of

data collected clear that the survey

of purely medical data to determine

ment, whether complex wound care

is present, at least not with the permission

offense of § 284 paragraph 1 number

Mer 4 and number 8 SGB V justified

could become.

In the course of our examination, it turned out that

the health insurance company if an application for

determination of a complex wound

is provided, to whose belief

liability exclusively nursing

Information on wound care awaits

would. These are statements like that

Number and extent of the wounds, the

Time required for changing the wound dressing

sel, cleaning and disinfection as well

the implementation of the wound dressing. kei

If not, she would

require information from the nursing service,

within the framework of home health

care only from the prescribing doctor or in

to assess difficult cases by the MDK

be.

Because of this, we had the

checkout abandoned in the used

Application form to clarify that they

as further information only the nursing

technical aspects of wound care

performance appraisal required, not

against further meaningful documents

about medical aspects. In addition,

we the health insurance company our opinion

sung that they have this additional information

not on the basis of consent, but

on the basis of §§ 284 paragraph 1

Number 4 and number 8 SGB V in conjunction with

Article 6 paragraph 1 letter e), paragraph 3

Sentence 3, Article 9 paragraph 2 letter h),

Paragraph 4 DS-GVO can raise.

The health insurance has on our instructions

the application form, the subject of

re contracts with the nursing associations,

in coordination with their contractual partners

changed.

The form now says-

special - which we expressly welcome

ßen – to clearly state that:

• the health insurance company to check whether a

complex wound care required

lich, no additional documents

in the form of wound protocols or even

Photos of the wound needed and that

• the health insurance under "significant

ge representation of the complex wound

supply as part of a

according to wound management" information

to the number of wounds whose

stretch, the time required and care

technical aspects such as cleaning,

infection and the implementation of

wound dressing expected.

However, contrary to the announcement

of the health insurance company on the

ten customized form still

obtaining a declaration of consent

intended. This will be the subject of further

The procedure of the health insurance company that

basically with

her employee so-called

“Wound managers” check whether dem

Nursing service a higher remuneration for

require complex wound care

and only in exceptional cases the MDK with a

commissioned with an appraisal

Incidentally, no cause for criticism: One

Health insurance is according to § 275 paragraph 1 SGB

V although obliged in certain cases

an expert opinion of the MDK

to catch up However, it follows from this

not that they are part of the exam

question whether complex wound care

ment is required, always such a

order an opinion

would have to. The health insurance has rather

a margin of appreciation that it her

allowed the participation of the MDK on the

to limit exceptional cases in which

difficult medical questions

and the examination in

easy to carry out cases

men.

request for personnel lists

the home supervisors

An association that also represents the interests of

care facilities, has us in the

Reporting period asked the practice of

Baden-Württemberg Home Supervision

authorities to check, after which these

from the inpatient care facilities

as part of their auditing work lists of

the nursing staff working there

request their real name and qualification

other In this connection it was questionable

also hang whether the home supervisors

this kind of personnel lists not only in the

Annual or event-related

gene quality tests, but also

as part of the semi-annual

may request so-called change notifications.

80

The home supervisors have after the

Provision of § 10 of the Baden-Württemberg

German Housing, Participation and Care Act

(WTPG) including the task, the personal

and technical suitability of the in a static

onary care facility employees

to check. In order to

to be allowed to operate the facility

the operator of the facility ensure

that the number of employees and their

personal and professional suitability for the
activity to be performed by them is sufficient
(cf. § 10 paragraph 3 number 3 WTPG). So-
far this is not guaranteed, have the
Home regulators to the statutory
Order, appropriate measures after
Housing, Participation and Care Act to be
take effect, e.g. a ban on employment
pronounce
That for the home supervisory authorities
permanent Ministry of Social Affairs and
integration presented us conclusively
and convincingly show that for the tasks
compliance with home regulators
Personnel lists are required, which are not
only the initials of the employees, but
then the clear names and the qualification
of employees included. the home
supervisory authorities would have to
fung whether an inpatient facility
Requirements of the housing, participation and care
fulfilled the law, also the provision of § 4
Paragraph 1 of the State Personnel Ordinance
include. Thereafter, persons
who are in an inpatient facility
are busy, there are no facts,

which justify the assumption that they

for the activities they carry out

are personally unsuitable. Not suitable

is, in particular, who because of (in the country

despersonalverordnung described in more detail

bener) criminal offenses have been finally convicted

has been.

LfDI BW - 35th activity report 2019 - 7. Health and social affairs The home supervisory authorities receive over

the so-called notifications in criminal matters of the

judge or public prosecutors knowledge

about criminal convictions that the

personal suitability of employees

ner inpatient facility in question

(cf. § 13 paragraph 2 sentence 1, § 14 paragraph 1

Number 5 of the Introductory Act to

Judicial Constitution Act and No

28 of the order of the Federal Minister

about the judiciary and for consumer protection

and the state justice administrations

the communications in criminal matters of 27.

March 2019) excludes. These communications

the home supervisory authorities

then with the available personnel lists

and then take action if necessary

the necessary measures. lay the

Home supervisory authorities, however, do not

lists of the individual institutions

Clear names before, so would be an assignment

of the messages to the individual

ments or facilities not possible. Us

moreover, plausible

laid that home supervisors

an equally suitable and milder means,

to the monitoring obligations from the

Housing, Participation and Care Act according to

come, is not available.

So far, the question of whether

the Baden-Württemberg home shows

supervisory authorities are entitled to

nallists from the facilities not only

as part of the annual or

quality check according to § 17 WTPG

to request, but also within the framework of

Change notifications according to § 11 paragraph 3

WTPG representing the Ministry of Social Affairs

and integration according to its orientation

assistance for the home supervisory authorities in Ba-

den-Württemberg at least every six months

expected. In this regard, agreed

the Ministry of Social Affairs and Integration

on with the home supervisory authorities,

that these within the framework of the

show according to § 11 paragraph 3 WTPG for the time being

– that means in any case up to a possibly

speaking legal clarification in the

Housing, Participation and Care Act – none

Personnel lists with names and qualifications

on of the employees would request.

7.3 The information obligation in the case

the collection of personal

ner data at the affected

person through social security

eng: The innovations of the GDPR

The data protection law

information

on duties form the basis for the

Exercising the rights of data subjects (in particular

in particular Article 15 et seq. of the data

General Protection Regulation [GDPR]). Only

if the data subject knows that

process personal data about them

be processed, it can exercise these rights as well

exercise Or as the recital

60 of the General Data Protection Regulation

mulated: The principles of a fair and

transparent processing make it

required that the data subject via

the existence of the processing operation

and its purpose is taught. in the
Area of social law count about it
information, advice and
come anyway to the basic obligations of
Service providers (cf. §§ 13-15 of the first
Book of the Social Security Code [SGB I]).
Fulfillment of data protection regulations
Information obligations through social
therefore comes an important
importance to.
Even before the General Data Protection
regulation there were information obligations
the social service provider: It used to be
however sufficient if they have the
Purposes of the collection,
processing or use, the identity of
responsible body and, if necessary, via category

 gories of recipients informed; on-
otherwise it was only to be pointed out that
whether the person concerned is obliged to provide information
tet, the provision of information requires
for the granting of legal
share or the information is voluntary (cf. §
67a paragraph 3 of the Tenth Book of the
zialgesetzbuch [SGB X] in the up to 24.

May 2018 valid version). The one in the

regulated by the General Data Protection Regulation

Information obligations are essential

beyond the previous legal situation.

With Article 23 GDPR, the data

General Protection Regulation, however, too

opens up the possibility through legislation

exercise measures – to a certain extent

– Restrictions on the obligation to provide information

to undertake. From this possibility

has the federal legislator for the

rich use of social data protection

made, namely with the regulations of

§ 82 SGB X in relation to the information

obligation in the case of the collection of personal

personal data at the concerned

Person (Article 13 DS-GVO) and with § 82a

SGB X in relation to the information obligation

in the event that the personal

Data not obtained from the data subject

be lifted (Article 14 GDPR).

Not only the welfare agencies had

with the presented legal

to deal with innovations, also for mine

office was in the area of social

data protection, the topic of information

tion obligations (especially in the case of

Collection of personal data

at the data subject [Article 13 DS-

GMO]) since the General Data Protection

regulation a focus:

My office had several

difficulties regarding the fulfillment of

processing obligation to inform. The

So ma will definitely be in public

perceived. With the complaints

it was primarily about the fact that the

answer no information at all

had created.

In addition, the topic was one of the

Main points of two of my service

place checks carried out at a

social welfare office and at a pension office.

Dealing with the information obligation

ten showed that the creation more correct

and at the same time for the person concerned

understandable information not quite

is easy.

Because of the knowledge gained

my office therefore has the contribution

"Particularities of the information obligation

according to Article 13 of the General Data Protection

regulations for social service providers"

to those responsible for the creation

to make the information a little easier.

The article is on the website

available from an office.

On some details of the information

obligation according to Article 13 DS-GVO should

to be discussed briefly:

Article 13 paragraph 1 letter a GDPR

GMO: notification of the name and the

Contact details of the person responsible

and, if applicable, his representative

ter

It is the person responsible

not about the (entire) city or

District or - as partly in the of

information checked by me

was - to the (official) data

protection officer. Who Responsible

is initially in Article 4 No. 7 GDPR

defined by law. For the area of

There is also social data protection

a special provision in § 67 paragraph 4

responsible for the service providers

(cf. § 67 Paragraph 4 Clause 1 SGB X). Important

is the regulation of § 67 paragraph 4

Sentence 2 SGB X:

costume. During our exams,

that only the "old tried and tested" regulations

were mentioned in the social code,

while the "new" regulations of the

General Tenant Protection Ordinance "forgotten"

became.

"Is the service provider a regional authority

perschaft, the responsible persons are the

Organizational units that have a task

after one of the special parts of this

carry out the Code functionally."

This can be, for example, the job center (for

the area of the second book of the social

statute) or the housing benefit office (for

the area of the Housing Allowance Act).

With the according to Article 13 paragraph 1

stabe a DS-GVO to be named representative

Incidentally, he is not the head of the

job centers or the head of the housing benefit

body meant, but the representative in the

Within the meaning of Article 4 No. 17 GDPR. This

is a company established in the Union

natural or legal person pursuant to

Article 27 GDPR was ordered. arti

kel 27 DS-GVO provides that a not in

responsible person based in the Union

cher or processor if necessary

Representatives in the Union as contact persons

names. This rule should therefore

the processing of social data

public bodies have no meaning.

Article 13 paragraph 1 letter c GDPR

GMO: Communication of the purposes for which

the personal data

are to be worked, as well as the

Legal basis for processing

As the legal basis for processing

occurs with social service providers in particular

special Article 6 paragraph 1 letter e

and Paragraph 3 DS-GVO in connection with

Provisions of national law in

Furthermore, it is important at this point

tig, the regulations in national law

(e.g. in SGB X) as precisely as possible

admit. Now there are cases where it

is not possible, in an understandable way

all legal bases in one overall

to provide information. Then you can

by way of example with the information

Article 13 DS-GVO a more general citation

wise suffice with a reference to the

Specification of the exact bases in the

forms, e.g. B. in the following way:

"Data processing by the social

office relies in particular on Article 6

Paragraph 1 letter e and paragraph 3 DS-

GMO i. V. m. §§ 67 ff. SGB X as well as on

special legal regulations. The exact

The legal bases can be found in the

individual forms."

In the individual forms are then the

appropriate legal norms

to name.

Article 13 paragraph 1 letter e GDPR

GMO: If applicable, notification of

Recipients or the categories of

Recipients of personal data

ten

Who is the recipient is in Article 4 No. 9

DS-GVO defined by law. After that is

the notion of "recipient" broader than that

of the "third party" (Article 4 No. 10 GDPR).

In particular, the order processing

beiter "recipient" and therefore to be specified.

 This information also includes the

(on the opening clause in Article 23 DS-

GMO-based) special regulations

in

§ 82 paragraph 1 SGB X to be observed.

Article 13 paragraph 2 letters b and c

GDPR

Here it is recommended to always use the

applicable article of the General Data Protection

ordinance (e.g. when

right of future

person

Article 15 GDPR), so that the affected

ne person if interested even more details

can read.

affected

the

Article 13 paragraph 2 letter e:

whether the provision of personal

personal data by law

or contractually required or

required for the conclusion of a contract

is whether the person concerned

tet is the personal data

provide, and which possible

Consequences of non-provision would have

The regulation corresponds to that of

§ 67a paragraph 3 sentence 3 SGB X in the up to

24 May 2018 version applicable.

As part of our consulting work

we were also on a special

Clarification needs of the service providers in the

field of child and youth welfare

with regard to the extent of their information

made aware of their obligations. here

seemed questionable to them whether § 62

clause 2 clause 2 of the eighth book of the

cial Code (SGB VIII) their information

tion obligations conclusively regulates or whether

the further regulation in Article 13

DS-GVO takes precedence over national regulations.

The regulation in § 62 paragraph 2 SGB VIII

reads:

"Social data can be obtained from the person concerned

to lift. He is on the legal basis of

84

Collection and the intended purpose

the collection and use

to the extent that these are not obvious."

The regulation has not been changed

den, although the Eighth Book of the Soci-

al code since the validity of the data

basic protection regulation and even more so

since it was issued, several changes

experienced. In particular sees

which has meanwhile been approved by the Bundestag and

second law passed by the council

Adaptation of data protection law to the

Regulation (EU) 2016/679 and for

implementation of Directive (EU) 2016/680 (in

Article 129; Draft law: Bundestag printed paper 19/4674,

p. 1 ff.) only editorial changes

of § 62 paragraph 2 SGB VIII. demge

on the other hand, Article 24 of the Law

process to change the federal pension

law and other laws of July 17

2017 (BGBl. I 2541, 2558) before the

Entry into force of the data protection principle

ordinance applicable general provisions

ment in § 67a paragraph 3 SGB X a. F. (p.

to her already above) on the obligation to provide information

in the case of the collection of social data

Affected with the justification (see

recommendation and report of the

Committee for Labor and Social Affairs, BT-Drs.

18/12611, p. 102 f.) repealed that

the content of the regulation there in the future

Art. 13 GDPR applies directly. This

You could legislate to that effect

understand that the legislature by having

§ 62 paragraph 2 sentence 2 SGB VIII despite the

other changes made

has maintained the

application of Article 13 GDPR, for example

Look at the opening clause in Article 23

DS-GVO wanted to exclude.

In particular with regard to the changes

62 SGB X through the second da-

data protection adjustment and implementation

However, neither the wording of the EU law

the amended regulation nor the

 regulated information obligations of the

high performers go a long way

ly about the requirements of the early

legal situation. This is the

Creation of correct and at the same time for

the data subject understandable

formations not easy. also is

the competition of regulations of the

zialgesetzbuchs with the regulations of

General Data Protection Regulation

at times

difficult to solve. is particularly important

In my opinion, in any case, one if possible
precise indication of the legal basis for
the data processing so that the data subject
understand fene at least to some extent
can whether the data processing by the
social service provider is legal.
Founding of the draft law (BT-Drs.
19/4674, p. 397) such a statutory
objective, the information requirements
from Article 13 DS-GVO to restrict
remove. Rather, it should be with the
Changes to § 62 paragraph 2 SGB VIII
according to the explanatory memorandum
to an editorial adjustment “to the
Definitions from Article 4 of
Regulation (EU) 2016/679”. To-
immediately adds the second data protection adjustment
and Implementation Act EU (by
Art. 129 no. 5 letter a bb) in § 68 paragraph
Clause 1 SGB VIII expressly a passage
a, according to which the information requirements
according to Articles 13 and 14 GDPR in the case
the data collection by assistance,
Official guardianship or official guardianship
should only apply to a limited extent, where
expressly in the explanatory memorandum

on the requirements of the opening
clause in Art. 23 GDPR for this case
constellation is received (BT-Drs.
19/4674, p. 398 f.). From this one can
reverse conclusion that the law
Generally also in the area of
Eighth Book of the Social Code of
the validity of the information obligations
General Data Protection Regulation.
In any case, there are doubts that a general
my exclusion of the information obligation
according to Article 13 GDPR by the current
Version of § 62 paragraph 2 sentence 2 SGB VIII
the requirements of Article 23 GDPR
to a permissible restriction
chen, so that's why not
by a corresponding will of the
legislator can be assumed.
Fulfillment of data protection regulations
Information requirements comes in the area
of social law is of great importance
to. The question of sufficient data protection
legal information is quite here
object of public perception.
Those in the General Data Protection Regulation

LfDI BW - 35th activity report 2019 - 7. Health and social affairs 8. Schools and universities

8.1 Terms of Use for the information technology in one school

Telecommunications secrecy versus school law.

Can a school save which pupil who visited which website? Around Here to avoid pitfalls should be every school care about this issue.

I was asked whether a shoe le may save which student or which student is accessing which website is looking for, so whether the Internet use relevant traffic data (also "connection referred to as “deployment data”) are stored allowed to.

If a school within the meaning of the telecom Communications Act (TKG) service bidder, it must do so under Section 88 TKG Telecommunications secrecy in accordance with Article 10 sentence 1 of the Basic Law. Included it should be noted that a violation of Telecommunications secrecy in accordance with Section 206 of the Penal Code (in the more detailed written forms of inspection) with a

punishable by imprisonment of up to 5 years

can be. Telecommunications secrecy

subject to the content of the telecommunications

tion and its circumstances; added

hear in particular already the fact whether

someone at a telecom

gang is or was involved. the telecommunications

secret is already at each save

affected by traffic data, in particular

so when storing the information, who

when visited which website

or – if the school teaches the students too

E-mail addresses – who assigns one to whom

wrote email.

It can be assumed that a

le then to the service provider within the meaning of

Telecommunications Act will, if

they use the private internet or e-mail

information about the school

technology allowed or tolerated. For this is sufficient

it already if they have internet access

makes the private

te use is not expressly prohibited.

At least that's how it works

partly business-like at the inheritance

provision of telecommunications services

With. For a businesslike delivery

of telecommunications services is namely

according to the Telecommunications Act

no profit necessary, otherwise

because a sustainable offer is sufficient

of telecommunications for third parties (cf. § 3

number 6 and 10 TKG).

Does a school grant the private use

or are there no explicit regulations

If this is the case at the school, the

School maintain telecommunications secrecy

and must not, in principle,

save data. Such saves

may only be carried out to the extent

when they are exceptionally exempt from §§ 96 et seq.

TKG to be approved, for example because they are part of the

development or to maintain the

lekommunikation, for payroll accounting

or to eliminate faults

are required. Are these particular

whose purposes exceptionally connect

ment data stored, may after

data protection purpose limitation

principle (Article 5(1)(b))

DS-GVO) in this data as well

can only be viewed to the extent that

than this for the pursuit of precisely these purposes

cke is required.

Now, however, the teachers are following suit

Section 38 paragraph 6 of the Schools Act Ba-

den-Württemberg (SchG) the immediate

pedagogical responsibility for the

 education of the students. The school-

management in turn directs and manages

§ 41 SchG the school and is subject to instructions

right towards the teachers. Out of

these responsibilities can

founded individual cases (from §§ 96 ff.

TKG not covered) educational needs

for checking communication data

arise, e.g. who when which in-

ternet site visited.

However, the school cannot meet this need

comply if they comply with the telecommunications

subject to mystery; the obligation to

Compliance with telecommunications secrecy

then rather meets the requirements

of the School Act to the school.

This dilemma between educational

Responsibility and Telecommunications Secrecy

can be dissolved if the school fails

as a service provider within the meaning of the telecom

munikationsgesetzes occurs and thus

no longer comply with telecommunications secrecy

§ 88 TKG is subject. Once school

explicitly give the students private communi-

nication is prohibited (and neither is this

tolerated), it is no longer available as a service

bidder within the meaning of the telecommunications

look at the law. As a result, allowed

the students the information

technology of the school only in the framework

use for school purposes.

For implementation towards the students

ers and students is a usage

tion required by the school, which the

private use prohibited. The

School to fall back on § 23 paragraph 2 SchG

fen and a corresponding school regulation

enacted, in which further

can be counted.

To the teachers (and others

school staff) applies with regard to

of telecommunications secrecy, by the way -

same: As soon as they are granted private use

believes or it is tolerated, is subject to the

School of telecommunications secrecy with the

consequences described above. For teachers

employees and other servants can

especially the use of information technology

not on the basis of § 23 paragraph 2

SchG are regulated; find this norm

as a general clause only for measures in

Area of "educational tasks"

and thus only in relation to students

Application. A prohibition of private

ten use towards teachers

however, by way of service instructions

take place. However, if the service

be permitted for private use,

without the school on the basis of §§ 96

ff. TKG permitted processing of the

binding data should be limited, so

it is advisable to have an appropriate

Service agreement with the staff council

hold true. It can regulate

the fact that a teacher

school technology can also be used privately,

if she assures in writing, with the

Storage of the connection data

to be understood. That would have to be settled

further, when in individual cases to which

previously defined purposes an insight

by whom in which stored connections

tion and inventory data under which

further conditions should be allowed.

Even if a storage of

Connection data (e.g. due to

end of private use in the user

regulation) is generally permitted,

are in the specific processing of

data further data protection

to comply with requirements. This is the information

Notification according to Art. 13 or 14 DS-

GMOs to consider. In addition, the

maximum storage time at the required

to the amount associated with the storage

be purpose oriented. Access to

the data may only be as small as possible

holding group of people whose

relevant (e.g. school management and administrator

nesters). Access may only be

attention to data economy both in

factual (which data types?) as well

in terms of time (will be used throughout

“History” researched or just regarding

a certain "criminal period"?)

gen. The secret access is only allowed
then take place if with the open
the intended purpose was not achieved
can be; becomes the secret access
made from this point of view
men, usually has an afterthought
Notification to be made as soon as this
is possible without defeating the purpose.
A usage regulation for the information
on technique is a must in a school,
to solve the dilemma between telecommunications
mystery and educational responsibility
to dissolve the school.

8.2 Revision of the brochure
"Privacy in childcare
directions” with regard to the
General Data Protection Regulation

“Data protection is fundamental rights protection. There-
Tenant protection is child protection.” That's what it says
Slogan in the foreword of the Ministry of Education
published around Baden-Württemberg
Brochure “Data protection in day-care
facilities". The Kultusmi-
nisterium together with us and the
including for Baden-Württemberg
Responsible regional manager for

the data protection of the Evangelical Church
in Germany with regard to the new
provisions of the General Data Protection Regulation
updated.
With regard to the processing of personal
data obtained from day-care centers
our office continuously receives numerous
any requests for advice and complaints.
From this it is already clear that in
considerable uncertainties in this area
certainties in relation to the requirements
of data protection. In order to
The Ministry of Culture had to act against it
already in 2012 together with free
supporting associations, the church data
protection officer and my department
le a much-requested brochure "Da-
protection
in day-care centers”
published, last in the third edition
in 2015 (for the first edition see already
the 31st activity report of my service
stelle 2012/2013, No. 8.1.1, p. 115).
The changes that the data
brought with it the General Protection Regulation
also have an effect in the area of children

the day care centers. emphasized at the same time

the General Data Protection Regulation to many

bodies that require special protection

ability of children with regard to

data protection (see, for example, the recitals

38 and 75 and Art. 6 paragraph 1 letter f)

last clause DS-GVO). Therefore appeared

it commanded the brochure with regard to

the innovations of the data protection basic

to revise the regulation again.

The new version of the brochure retains the

proven structure in information for

Parents, information for educators

and educators as well as information for the

Providers of day-care centers

but in each case on the new legal basis

gene a.

In the new edition, the

Parents, as before, especially about theirs

Data protection rights towards children

daycare clarified:

• What personal data is allowed

raise the day care center and

when does she need consent?

have to

this

Data

be deleted again?

• What right to information about

the data of the children have the parents?

In addition, the brochure contains

training for educators

come to support their work in the

day care centers. treated

the u. the practical questions, what

in the admission or care contract

may be asked how with observation

forms and the education and

development documentation, sound and video

handle records as well as photos

is under what circumstances lists with

the contact details of the children or theirs

Parents are created and published

may and which personal

Data between day care centers

and school exchanged or at authorities

passed on to or other third parties

that may. Were newly inserted in this respect

Comments on the special categories

ria of personal data and to the

Obligations to report data breaches.

The information section for the

Daycare providers includes how

previous comments on what was recorded

me or caregiver contract

must be taken and how the carrier dem

Parents' right to information about stored

data can follow. New

Explanatory notes have been included

List of processing activities

and data protection impact assessment.

Should be particularly useful in practice

the revised templates for consent

gen (for posting, for forwarding and

for publication of photos, for publication

disclosure of other personal information

data, for the collection of data for

and development documentation

as well as to audio and video recordings)

be. With regard to the obligation to

in particular from Article 13 paragraph 2

and Article 14 paragraph 2 DS-GVO

day-care centers also a newly

worked sample leaflet for information

about rights under the General Data Protection

regulation provided.

The brochure is electronic and in pa-

pierform via the pages “Kindergartens

and other day-care centers in Baden-Württemberg"

available from the Ministry of Education.

Data protection and pedagogy complement each other.

Both in data protection and in the

pedagogy stand for the dignity of

according to Article 1 of our Basic Law

(GG) and the free development of the

personality according to Article 2 GG in the center.

Therefore supports the newly released

Brochure the day care centers

and the educators at

data protection and thus also offers set-up

stuff for the pedagogical work with the

Child.

8.3 Revision of the administrative

regulation on data protection

through in public schools

the ministry of culture

Baden-Württemberg and their

implementation

After the country the country data

protection law to the basic data protection

regulation, could do that

Ministry of Education the administrative

writing about data protection to public

rework schools. According to § 26

Paragraph 2 of the LDSG, the Ministry of Education

rium involved in good time. While

I the revision of the administrative

regulation and the inclusion of my

Office of the Ministry of Education

Nevertheless, there are still significant deficits

in the implementation of the administrative regulation

and especially in the scope of the

Schools to comply with data protection

legal requirements available

determine resources provided.

With the enactment of an administrative regulation

about data protection to public

Schools (hereinafter: VwV) supported

the Ministry of Education the schools by

it the data protection regulations in

Reference to public schools specified

and thereby standardized their actions

as well as simplified. Most recently, the

Ministry of Education the administrative regulation

effective January 1, 2015

(cf. the 32nd activity report

2014/2015 of my office, No. 8.1 /

p. 141 f.). The entry into force of the

basic protection regulation and in its

Follow the new version of the country data

protection law brought the necessary

of a revision of the administration

regulation with itself.

That's the Ministry of Culture with that

Decree of the 4 July 2019 new

administrative regulation, in which

sen draft it me properly

has integrated, complied. Of the

The need for change was considerable; only

as an example, significant new

enumerated:

• The explanations about

the information obligation in the data

survey (number 1.2 VwV). A

Most of the master data is already

upon admission of the students

students raised. The newly created

ne Annex 2 to the administrative regulation

gives the schools the template for this

a school admission sheet to the

Hand to which the schools refer

Number 2.2.1 (penultimate sentence) to

have orientation. There are located

Statements on the fulfillment of the

data protection law

information

duty, which is still by a separate

– also newly developed – feature

sheet “Rights of the Affected” is added.

The pattern also pre-

pictorially identified, too

what information the parents of the

are obliged and which investors

are only to be made voluntarily.

• Fundamentally revised or re-introduced

the notes on the

Admissibility of data processing

(Number 1.1 VwV), for processing

special categories of personal

gener data (number 1.4 VwV), to

Data Erasure and Restriction

processing and data transmission

(number 1.5 VwV) and for

right of future (number 1.6 VwV).

• They receive helpful explanations

schools by the administration

also write to the directory

of processing activities (number

mer 1.8 VwV) including a

listing of regularly at least one

to be carried

computer programs

(Number 1.8.3 VwV), for the necessary

capacity and implementation of a data

protection impact assessment

(Number

1.9 VwV) and to report data

break down (number 1.10 VwV).

• I consider them to be particularly important

arrangement of a regular

teaching of the entire college of

School on data protection, which after

Number 1.7.2 VwV once a year

must follow. To prove the

tion, a form will be sent to the schools

Appendix 3 to the administrative regulation

provided.

 However, I see the implementation

improve the administrative regulation

potential:

• As stated in the administrative regulation (Number

mer 1.11.3 and 1.11.5 VwV) mentioned,

is it public according to Article 37 GDPR

union bodies prescribed, one

to appoint a data protection officer

and to report this to me, whereby the

le z. B. use my online portal

can. Unfortunately, however, an

rating that I only from a good 800 public

public and private schools such

reports are available, with around 3800 public

public and about 720 private schools

in Baden-Württemberg (Statistics

State Office, General Education Schools

or vocational schools, overall

view school year 2018/2019). That is a

very small proportion and becomes control

actions of my authority.

• The data protection declarations of

verse websites of the schools

do not contain information according to article

13 paragraph 1 letter b DS-GVO to

Data Protection Officer. Such

gave in the Internet appearances of

However, schools could also

increase data protection in schools

hen, v. a. as this allows me to

that of parents, students or

better with students or teachers

the data protection officer together

could work. By specifying

the contact details of the data protection

can order on the website

also those affected more easily

contactable with the data protection officer

contact the school

which, being closer to the school, frequent

quicker than I could understand the data

can fix problems.

• Already in my last job

2018 I am in chapter 8.1 on the

missing human and financial

Resources when ordering from

Data Protection Officer

received

(Activity report 2018, p. 111).

In the position plan of the supplementary budget

2018/2019 of the Ministry of Education

(Chapter 0404 State Education Authorities

Title 422 01) there are now 26 new ones

Place

for data protection officers,

which are located at the school offices

should be. About new positions for

I am pleased to be the data protection officer

very. But assuming that

the school authorities for around 3100 public

schools are responsible (statistic

State Office, general education

Schools, general overview of the school year

2018/2019; for grammar schools and professional

che schools are not the school authorities,

but the regional councils

responsibly), is an average of one

this data protection officer for approx.

120 schools responsible if none

data protection officers from the

legium of schools were named.

If the data protection officer takes

ne tasks according to Article 39 GDPR

seriously, he must call the teachers

sen around 120 schools on data protection

sensitize, advise and protect

and compliance with the data

General Protection Regulation and others

school privacy policy

monitor and he must be in early

all with protection personal

data related questions

to be involved. In addition,

persons affected by him, d. H. here

Parents, students and

Teachers at these around 120 schools

to all persons involved in the processing

related data

take a guess. Such a load of work

 is from the currently ordered data

cannot be managed by the protection officer.

With a large number of schools in

the responsibility of a single

data protection officer therefore exists

a contradiction to Article 38(2).

DS-GVO, according to which the person responsible

the resources required to fulfill

must provide sources.

For the sample that is still available here

Lematics of the conflict of interest (cf.

Article 38 paragraph 6 GDPR) for the

Employees of the school authority in the radio

tion of the data protection officer

school I refer to chapter 8.1

nes activity report 2018 on p. 111.

The data protection administrative regulation

public schools facilitates school

the implementation of data protection. Al

However, the schools have to continue

significantly more resources for implementation

be made available so that

especially those required by law

data protection officer effective

employed

can become.

93

LfDI BW - 35th Activity Report 2019 - 8th School and Universities 94th

LfDI BW - 35th activity report 2019 - 8. Schools and universities 9. Private data protection

9.1 Temporary employment –

Processing on behalf?

Order processing in accordance with Art. 28

DS-GVO is between responsible

often agreed (unfortunately) to

supposed requirements of the GDPR

to comply, even if specifically

Case no order processing at all

present. If employee data from

different companies raised or

transmitted, with a view to the

employ data protection the data processing

particularly sensitive and precise

regard.

As part of an inspection visit,

nes personnel service provider described us

the company data protection officer

subsequent problem that we at the

Correct the on-site inspection immediately

could:

The business model of the responsible

such place is the so-called "personnel leasing",

i.e. as a "lender" the employee

leasing of temporary workers

according to the employee transfer

sungsgesetzes (AÜG). In the course of the

of temporary workers at other

other companies, the "borrowers".

often in the past

working agreements in accordance with Art. 28

DS-GVO on the part of the hiring company

been sent in order to

property rights requirements of the DS

GMOs against the background of labor

to suffice. According to Article 88

GDPR i. V. m. § 26 Paragraph 8 No. 1 BDSG

are employees within the meaning of the law

“workers,

including temporary workers

and temporary workers in relation to

borrower". This is to make it clear that loan

not just towards employees

your employer, but also against

about the company they work for

are used, under data protection law as

employees apply.

This is due to the fact that it

to a variety of processing, between

transfer to the "lender" and "borrower".

the temporary workers come and

both therefore adhere to the prerequisites

88 DS-GVO i. in conjunction with Section 26

sentence 1 BDSG. That means

but also that order processing

agreement in accordance with Art. 28 GDPR

not at all popular with “personnel leasing”.

question comes. The "Lender" processes

no personal data on

sung, under control or for purposes of

Borrower, as required by Art. 28 GDPR

would put.

The opposite is the case: “borrower” and

"Lenders" process the personal

drawn data temporary workers

mostly for their own or common

me purposes and intentions and thus straight

de not on behalf of or on the instructions of

other contracting party. "Lender" and

"Borrowers" are thus themselves

responsible persons or

jointly responsible.

For the implementation of employee

leasing of temporary workers

comes an order processing association

28 DS-GVO between

“Lender” and “borrower” out of the question.

The companies involved must

(intended) processing of personal

personal data of employees

independently for their legality

check and take appropriate precautions

meet gene

private companies

A within our area of responsibility

resident company monitors federal

as far as compliance with the usage

regulations of private parking lots and

parking garages. Keep turning

Persons who, because of a “parking violation”

used by this company

be taken to our authority because

they see this as a data protection violation.

Such a complaint is fundamental

technically permissible. However, we can

Matter only data protection law

check over. Whether the - alleged - Forde

tion of the company is justified,

may have to decide the civil courts.

The surveillance company can

Vehicle owner data one in his opinion

illegally parked vehicle

the Federal Motor Transport Authority or the

get a job. To do this,

be held liable that the owner

of the parking space may be a legal claim

in connection with the operation of

vehicle. The surveillance

company may use this information

or let it be used in order to – supposedly –

lichen – to enforce claims. That is

permitted under data protection law.

In the event that a person has been proven

"wrong" parked, the un-

take a reasonable time this

Process even after completion of the cost

save the collection procedure in order to

Severe sanctions if repeated

to take or from goodwill decisions

to foresee. But it has to do that

Art. 21 paragraph 1 of the EU General Data Protection Regulation

regulation in case of contradiction of

data subject prove that this

actually one managed by the company

has wrongly used the tenth parking space or

that damage has occurred as a result.

The driver of the vehicle can

gel can only be used

when he's driving into the parking lot

Terms and Conditions that

a contractual penalty for unlawful par-

ken provide, has tacitly accepted.

The existence of a claim against

the owner who does not own the vehicle

turned off, presupposes that the internal

holder of the parking space according to §§ 861,

823 paragraph 1 of the Civil Code

there is concrete damage caused by the

seat confinement" of the parking lot arose

the is.

Can the driver or the holder

such claim cannot be proven

den, their data are after termination

of the recovery procedure in the file,

on which the employees

of the monitoring company for processing

handling such cases

able to delete. The continuation of

Storage for a reasonable time

room is only allowed if the claim

was founded and the company itself

has reserved, in case of recurrence one

to demand a higher contractual penalty or

to refrain from making a goodwill decision.

Notwithstanding, the company

committed even after the final

Completion of the process the data still for

a reasonable documentation period

locked, because the EU data

protection law distinguishes between data

erasure and data destruction. Latter

is only permitted if there are no queries

or legal disputes due to the

data processing are to be expected

or national storage regulations

no longer provide the information

prescribe. However, these may then

only be stored in such a way that

responsible data protection officer

can take hold of. The information may

then only for the tax office, for

data protection controls or for expected

de judicial proceedings are used.

These cases show that companies

not prohibited by data protection law

claims to which they are entitled

to enforce in civil proceedings, but that

data collected for this purpose

additionally no longer processed

may be allowed if the procedure

finally decided. The mooring

"Black lists" is through the EU data

prohibited by data protection law.

9.3 Data Protection Laws

responsibility

In practice, more and more original

the responsibility of the person responsible

transferred to external service providers.

Difficulties often arise

with regard to the delimitation of

verbalities. The data protection law

Responsibility of a service provider for

Document shredding is not inevitable

to deny.

the purposes and means of processing

of personal data

det (cf. Art. 4 No. 7 DS-GVO). violates

he violates the GDPR, so he cannot

only addressee of fines and other

sanctions (Art. 83 and 84

DS-GVO), but is liable to the

or the persons who are

hits a tangible or intangible

ellen damage (Article 82 paragraph 1

GDPR). This claim for damages

is directed primarily against the responsible

literal, but may in some circumstances

also meet the processor, too

if his liability is based on Art. 82

Clause 2 was restricted:

Any person involved in processing

responsible is liable for the damage that

by a non-compliance with this regulation

speaking processing was caused

en. A processor is liable for the

caused by processing

damage only if he uses his spe-

specifically imposed on the processors

ten obligations from this ordinance

complied with or under non-observance

compliance with lawfully issued instructions

of the person responsible for data processing

verbatim or contrary to these instructions

acted.

cause for renewed debate

with this topic was a data breach

message asking whether

a document shredding service provider

when setting up a throw-in container

must check for himself that this ver-

closed is placed or whether it is always

it is the customer's responsibility to

to check the container.

Addressee of the General Data Protection Regulation

tion is primarily the person responsible, so

the natural or legal person,

hearing, institution or other body that

alone or together with others

For the question of liability, it is therefore

dend whether a person responsible or a

carrier caused the damage.

There is no possibility of an exemption

finally the processor of-

fen. Although the processor

clear in principle from the person responsible

is to be separated, can be in borderline cases

quite difficult delimitation questions

place.

Processor is according to Art. 4 No. 8

DS-GVO a body that

ne data on behalf of the person responsible

processed. According to Art. 29 DS-GVO, a

personal

Data only on the instructions of the person responsible

process. The up-

carrier only a very limited one

Freedom of design in a data transfer

work available. Basically

the order processor is not given the

assigned task, but only

an auxiliary activity. Therefore, the processing

processing activity of the processor

in principle to the person responsible

expected. This arises in particular

also from Art. 28 DS-GVO, which

those responsible for checking the suitability

safety of the processor.

Common prime example of existence

an order processing is the addition

contracting a service provider for the filing

destruction. The deletion of magnetic

physical and optical data carriers (e.g.

magnetic tapes, diskettes, CDs, DVDs,

sticks) or the destruction of data

gladly of all kinds, especially of no more

required paper documents, represents a typical

picical data processing. Since

When the GDPR comes into effect, there is a

increasing number of service providers, which

DS-GVO-compliant document destruction

to offer. In particular, it is

that "everything is taken care of".

Small and medium-sized companies in particular

accept understand this offer

Luckily, in order to at least

no worries about data erasure

to have to do more. will be forgotten

doing that the person responsible even then

responsibility for compliance

data protection regulations carries if he

a processor with the destruction

of data carriers with personal

Genetic data commissioned (Article 5 paragraph 2

GDPR). He is responsible for checking and

Compliance with the requirements of the GDPR.

He only succeeds in doing this if he

given clear instructions regarding

of deletion, but also regarding the

Interim storage and transport (up to
for destruction) as well as place and time
of destruction (e.g. on site at the
responsible or in the business premises
of the processor). Are
this information with the service provider not
or difficult to negotiate, must itself
let the person responsible ask the question
whether there is still an order processing
may be spoken and whether he
select a suitable service provider
Has. The less is to be noted here
well-known Art. 28 Paragraph 10 DS-GVO:
Without prejudice to Articles 82, 83 and 84
a processor in breach
contrary to this regulation the purposes and
means of processing, in
access to this processing as the responsible
more.
A service provider who independently
decides how to destroy the data
tet, stores and/or transports, embarks
himself in the position of a responsible
chen. He can feel responsible
ness even if
formally an order processing contract

is closed, but in reality

is not "lived". Such a contract

may put a legal bill though, that

speaks for order processing

but not constituent. Means: Man

cannot use this contract to

create a carrier that actually

none is – but the role of the

has taken responsibility.

The facade of the prime example of

carrying processing is crumbling.

In the meantime

there are some indications that no longer

the service provider also “only”

worker is. What matters is who

actually the type of to be performed

Data processing and handling

new data. The less influence

the company or authority

has the service provider, the less can

one speaks of order processing

chen. That this trend is quite critical

can be seen is obvious: the principle

vialloy for data transmission from

Company or authority on the

Service providers would be omitted, it is therefore necessary

an independent legal basis.

Possibly would even be a joint

Responsibility (Article 26 GDPR).

think. The LfDI advises clear regulations

to meet and these for both sides

to avoid unfavorable legal situation.

9.4 Data protection at the

property management

Property management companies process a variety

number of personal data both

by homeowners as well as by

tenants. Especially with regard to the

community of owners

reigns

administrators often have the view that

Owner data generously passed on

should be, because in the housing

community of owners no data protection

right. This view is incorrect.

Sharing of data within a

homeowners association

The homeowners association

established between its members

civil law obligation with

mutual rights and obligations. Since the

homeowners because of this

contractual legal claims

can arise against each other

they will be able to precede each other if need be

to sue in civil courts.

Every apartment owner therefore has one

legitimate interest, the names and

summonable addresses of all others

obligated,

to find out about co-owners. The administrator

is due to his with the apartment

community of owners

closed

Administrator Agreement

each

Co-owners upon request a list

the names and addresses of the others

to provide co-owners.

No consent is required for this

the individual co-owners one more

decision of the owners' meeting.

The situation is different with the e-mail ad

ress and other contact details of

apartment owner. These are

for

legal disputes between

not to the members of the community

necessary. The transfer of this data

ten by the administrator is therefore neither

to fulfill the management contract

to protect the legitimate interests of

co-owner required. The administrator

must therefore not without the contact details

consent of all concerned owners

pass on.

This also applies to forwarding

E-mails in the context of discussions

and disputes within

homeowners association

U.N-

ter participation of the Administrator. When a

Owner email the manager

draws attention to a grievance, dem

he remedy or in the owner

meeting is to be discussed, so

the question arises as to whether the administration

ter this e-mail to the other co-owners

mers, disclosing the identity of the

may forward the sender after

result of the balancing of interests

Article 6 paragraph 1 subparagraph 1 lit. f GDPR

GMO. Even if the forwarding

be of the non-anonymized email text

should be permissible in individual cases

Transmission of the e-mail address itself in the

Doubt without the consent of the person concerned

owner illegal. Here, too,

 sen the property managers very carefully

look.

Telephone number stored for this purpose

readily required.

Disclosure of data to external parties

Make like artisans

In practice, the property manager often

fig also contact data to external bodies

further, especially to craftsmen. To this

way to ensure that the

ser with the apartment user, be it a

Owner or a tenant, promptly one

repair date can be arranged. Frequently

however, if the transfer occurs to the affected

fenen person to displeasure, about because this

although would have agreed

by telephone, but not by e-mail

craft business to be contacted.

The transfer of contact details takes place

their legal basis regularly in Ar-

article 6 paragraph 1 subparagraph 1 lit. b DS-

GMO, i.e. the transmission must be for the

Fulfillment of a contract, the contractual

party the data subject is, required

be lich. Is it the affected

Apartment users around the owner, so

the administrator contract comes into play for this

costume. So that the administrator in accordance with the contract

initiate a timely repair

he gives the phone number of the egg

owner to the craft business

which he received from the owner at the start of the contract

received for this purpose. in the

within the framework of its information obligations

Article 13 DS-GVO, the administrator must

Owner already when collecting the

Telephone number on the possibility of

Passing on to craftsmen for association

notification of repair dates.

On the other hand, the administrator, if he is in

E-mail from the owner over time

receives, whose e-mail address is not without

the consent of the owner

Craftsmen pass on, because such

Passing would be given on this

The problem becomes clearer with the

Rental Management. The prospective tenant shares

the lessor, who

broker or to whom the tenant

election preparatory house manager often

a variety of communication data

with, in order at all in the selection of tenants

to be taken into account. is that coming

The tenancy is then established

Administrator owned each of the official

and private landline and mobile numbers

mer of the tenant and his e-mail address

resse and, if applicable, the fax connection number

his parents. Will be in the apartment

Repair due, the administrator chooses

unfortunately often "on target" that contact

tum from under which the tenant concerned

is hardest to reach or him

completely dispenses with the selection and

immediately gives all contact details without

agreement of the tenant.

Here too, passing on a contact

datum required, namely for fulfilment

of the between tenant and landlord

concluded rental agreement. Is required

but only the contact date, under

which the tenant can be reached and reached

want to be cash. If the manager has more

previous contact details, he may not use them

all forward but must focus on

the limitation necessary for the purpose

know On which of several of the

walter available contact details this

applies, he has by virtue of his

liability under data protection law

determine. For this purpose it recommends

himself, simply to ask the tenant under

what contact date he for craftsmen

wants to be reachable. Only if the administrator

ter to this question in a reasonable time

does not receive an answer, he may

divorce what contact date he dem

Notification according to Article 13 GDPR applies

also towards the tenant.

The property manager has the transfer

of contact details of the apartment users

Principles of Necessity and

consider data minimization.

Appointment of a data protection officer

carried by an apartment owner

community

Property managers offer the

affiliated apartment owners

communities at times, for you next to

the administration of the residential complex also the

Tasks of a data protection officer

to take over. The resulting ones

costs should then be fully

be imposed on community. This pre-

walking requires critical consideration.

A homeowners association

is regularly not to name a

nes data protection officer committed.

In particular, in the community in

usually just not ten or more

People constantly using the automated

processing of personal data

busy what according to § 38 paragraph 1 sentence

1 BDSG trigger a designation obligation

would. This should also usually be the case

then not be the case if the

owner has not appointed an administrator

have, but the common

manage property yourself.

Orders the condominium community

schaft, however, an administrator, so is

this self-responsible person in the data

protective sense. Neither will he

as a processor for the community

active, because the administrator is subject

according to the usual contract design

the instructions of the apartment owner

community and is also supported by it

not monitored. The administrator is processing

personal data therefore not in the

Mission of the community for this,

under their own responsibility to carry out

running his own business.

For example, due to the number of

usually constantly with the administrator

the processing of personal data

ten persons employed the naming

required by a data protection officer,

this obligation does not apply to the housing

community of owners, but the

walter himself.

An administrator who, due to legal

appointed a data protection officer

called to ensure compliance with data protection

zes in his company,

therefore has no reason whose actions

activity towards the homeowners

to be declared as a service for them

and they stand out from the community

to be compensated. Neither does

it seems appropriate if the administration

ter other expenses that the

compliance with data protection regulations

serve as part of its business activities,

of the community as a privacy service

billed.

The homeowners association

should always check whether they themselves

appointment of a data protection officer

is obliged.

9.5 Data protection in the

credit industry

Photocopies of ID cards

credit institutions

The practice of credit institutions in which

opening an account the identity card

to photocopy the customer

len for a long time for irritation. The-

 this procedure is also not included

Application of the GDPR lawful.

By having the bank

and keep the copy, process

use the ones printed on the ID card

personal data. By article

6 Paragraph 1 lit. c DS-GVO is such

processing lawful, among other things,

if they are to comply with a legal

obligation that the person responsible

succumbs, is required. The authoritative

legal obligation is the money laundering

schegesetz (GwG). credit

According to § 2 paragraph 1 no.

1 GwG to the bodies, the obligations

subject to the Money Laundering Act.

According to § 10 Paragraph 1 No. 1 and

Paragraph 3 sentence 1 no. 1 the contractual partner

when establishing the business relationship

to identify. The verification

verification of the identity data in accordance with Section 12

Clause 1 Clause 1 No. 1 GwG based on an official

identity card, such as in particular the

identity card. § 8 paragraph 2

Sentence 2 GwG makes it clear that the bank

has the right and the obligation to

pien of the identity verification submitted

to prepare identification document or it

fully optically digitized.

The copies are according to § 8 paragraph 4 sentence 1

to be retained for five years.

In this context, not

should be mentioned that § 11 paragraph 4 No. 1

GwG names the data that is used within the framework of the

collect identification of the customer

are. Some of the ones on the identity card

information printed on it, e.g.

per size and eye color, as well as those for

the use of the online function at

access number required under

don't listen to it. It is therefore often pointed out

pointed out that the complete copy

of the identity card without

tongues of individual unneeded information

102

the principle of data minimization

Article 5 paragraph 1 lit. c GDPR contradict

che. This objection is correct, but it stands

as a result of the applicability of Section 8

Paragraph 2 clause 2 of the GwG. That is

enjoys the General Data Protection Regulation

including the principle of data

minimization fundamental application

priority over regulations of the

national right. The obligation to copy from § 8

However, AMLA serves to implement

article 40 paragraph 1 lit. a of the Fourth Money

cal directive (2015/849). Adjust accordingly

the Member States that credit institutions

a copy of the identification

tion of the documents received by the customer

make and store. Since the ideas

tification based on an undarkened

identification document has taken place,

with even just a full copy for

the fulfillment of the retention obligation

under consideration. Article 40 paragraph 1 lit. a of

Fourth Money Laundering Directive is to that extent

in relation to the basic data protection

order a priority special regulation.

The bank therefore does not need any redaction

individual details in the ID copy

accept. Although it is from the point of view of

not gratifying that companies

also such personal

store identification data that is used for your

business activities are not readily

are required. In view of the aforementioned

legal situation, the data protection

but the complete

Copy of the identity card

Banks as part of the identification

accept under the Money Laundering Act.

At the beginning of the transaction, bank customers must

business relationship accept that the

bank a complete copy of their personal

national identity card prepared and stored.

LfDI BW - 35th activity report 2019 - 9th working environment credit checks in the

insurance industry

Just like other companies are too

Banks and insurance companies entitled

before completing a financially risky

contract with a credit agency for a bonus

to obtain information about your customer.

The existence of the corresponding risk

However, the location must be checked carefully.

Get an insurance company one

credit report on a customer,

to draw from his financial performance

ability to persuade, that's how it processes

personal data worthy of protection

Data. Such processing is after

Article 6 paragraph 1 lit. f GDPR lawful,

if they are used to protect the legitimate

interests of the person responsible or one

Third party is required, unless the

interests or fundamental rights and fundamental

freedoms of the data subject who

Protection of personal data required

other, predominate. A legitimate internet

esse of the insurer comes regularly

only considered if this is through the

Credit check before a credit check

wants to protect against the risk of default, i.e. if he

he wants to create his own

sustainable performance not without sufficient

prospect of receiving consideration

customers. The relevant

che performance of the insurer not only

payment in the event of damage. Much more

the abstract insurance

protection from the start of the contract period

performance of the insurer, independently

of whether there is a damaging event

and as a result to a claim for damages

performance by the insurer.

A predominant protected

interests of the policyholder

is usually not given.

There is a risk of financial default

but not the insurer if the

policyholder his premium payment

payment fully in advance. This is

usually the case with liability insurance

security for mopeds. Here the insurance

Protection only for one year. the insurance

policyholder receives for this period

an insurance indicator, whose

Validity already on the font color

be clearly recognizable. Should the

collateral taker therefore after expiry of

insurance period without liability

insurance ride a moped, like that

liability of the insurance

company not considered. Whose

financial risk is therefore due to the im

Premium payment paid in advance

covers. Under these circumstances, the

insurer no legitimate interest

remember to get a credit rating from a credit agency

information on the policyholder

call.

The data protection supervisory authority will

Obtaining creditworthiness information for

continue to critically accompany future bureaus.

scoring

According to the findings of the consumer

it is central in times of low interest rates

apparently widespread to buy on credit

fen and to get into debt. This

attitude brings the risk of massive

ven over-indebtedness. That again-

order prompts the companies to step forward

Contract conclusions by obtaining a

Score of the creditworthiness of the

to convince the contractual partner. This

should use a complicated calculation

something about the future

Payment behavior of the data subject

statement.

Art. 22 paragraph 2 DS-GVO allows that

Decisions about the conclusion or

the fulfillment of a contract is excluded

calculated score values are met

the. Also can score values together

with other parameters for extraction

such a prognosis can be used

if for such a procedure in concrete

ten case a legitimate interest i. p. des

Art. 6 paragraph 1 lit. f GDPR exists.

The calculation or use of a score

rewertes is lawful only if the

Data protection regulations both at

the bodies that calculate the score,

with those who have this information

transmitted, as well as with the

responsable, which ultimately determines the score

use, be complied with or

have been held. That's why the

Inclusion of unlawfully processed

data and such whose storage

between has become inadmissible, basic

additionally not allowed. This applies in particular

special highly personal information i. s.d

Art. 9 GDPR. The information must also

be correct in terms of content. is problematic,

whether data from social networks

may be included. This is al-

if necessary, to accept information

which the data subject himself "for

dermann accessible" on the internet

or the authorities and courts

could publicly announce

(e.g. list of debtors of the full

Extension courts according to § 882 f paragraph 1

Sentence 1 No. 4, Section 882 g Paragraph 2 No. 2 ZPO,

Decisions in insolvency proceedings e.g.

B. § 30 InsO).

For the calculation of the score value

fen only data are used that are necessary for this

based on a scientific

ly mathematical-statistical

rens demonstrably significant and suitable

are. The procedure must be consistent with

the state of the art for the analysis

se whether the data subject due to their

Characteristics of a specific comparison

group whose creditworthiness is known,

be fit. The statistical

cal comparative values must be up-to-date. Further

must have sufficient factual

position for the prognosis exist.

The determination of the probability

value must not be decisive on so-called

font data. Meant are the

Characteristics of the residential building (age

and type), as well as the payment history of the

residents of the street and the building,

where the affected person lives.

If a responsible person makes an automatic

ted decision i. p. of Art. 22

Clause 2 lit. a GDPR, i.e. exclusively

based on a score value, the

affected person according to Art. 22 paragraph 3 DS-

GMO the review of the decision

including the used Sco-

rewertes under statement of their own

position by a natural person

to demand.

Otherwise the following applies:

With regard to credit agencies, the

affected persons according to Art. 15 paragraph 1

DS-GVO, recital 63, require

to be informed about which data

ten for the calculation of

the score values are stored and where

since the company has received them

(Article 15 paragraph 1 lit. g GDPR). Included

can the credit agency not deal with

suffice, merely the category to which the

belong to stored data, to name

(cf. Art. 15 Paragraph 1 lit. b DS-GVO).

After the in accordance with Art. 22 paragraph 3

DS-GVO standing, so far for scoring

case law of the Federal Court of Justice

there is a right to information which

specific individual data are stored,

thus erroneous information even before her

Usage corrected and misunderstanding-

se can be enlightened, what at the

that would not be possible.

According to recent case law,

also value judgments a verifiable,

apt core of facts.

To do this, the digits, the score values

calculate or use, at least

state which circumstances are relevant

were that the person concerned was not considered

rated "unconditionally creditworthy".

became. Also is on request about it

to inform what dates in already

calculated score values received

have, to whom so far which score values

have been transmitted, which is why the

stored or used information

should be suitable, a realistic

to determine score value, and which

legitimate interests for use

information from social networks

ken should exist.

According to Art. 18 Paragraph 1 DS-GVO, the

data subject the right against which

saved for the score calculation

th data at the credit agency objection

to raise and demand that this

be checked for accuracy.

The credit agency cannot verify their accuracy

prove the information must either

corrected according to Art. 16 DS-GVO or after

Article 17 paragraph 1 lit. d GDPR deleted

will.

Due to Art. 21 Paragraph 1 DS-GVO

the data subject can process

object to the processing of their data. Does she want

that in connection with a

value calculation, she must counter-

substantiated about the person responsible

present matters worthy of protection that

the calculation and transmission of a

Score value can be violated or

became. A score violates the personality

right of a person or his

Right to exercise freely

of his profession according to Art. 12 GG, if the

Rate the inaccurate impression

conveys that the person concerned is not

unqualified credit, although it

no grounds for such an assumption

are. The data subject can claim

make that calculation result

evidently incorrect or that not

current, incorrect, objectionable, for

the calculation is inadmissible or inappropriate

specific information or previously illegal

processed data are used or

have been. The score value

invoice the factual basis is missing if

insufficient data to

available or if important relevant

te facts, e.g. B. Freedom from debt - au-

stay or have stayed or

if (partial) value judgments, estimate data and

Blanket valuations are not viable

facts are based. Furthermore, a

be contacted, the credit agency is missing for

the processing of knowledge

the social networks the justified

interest or it would

giving too much weight to data

be sen. Last but not least,

be gene, act in the calculation

it is a fantasy product because the

Credit agency don't see themselves in a position to do that

Coming into existence of the calculation after

to explain fully. In case of an

such objection, the responsible

literal according to Art. 21 paragraph 1 sentence 2 DS-

GMO refuting the objections

prove that there are acceptable reasons for

the contested score calculation gives,

which the interests of the persons concerned

son predominate.

The data protection supervisory authority will

be very careful in the future

that the requirements of the EU data protection

basic regulation when calculating and

use of score values should be observed

the.

protection instructions using the example of

Raffle tickets and prize

play on websites

The practice of the supervisory authority shows

that many sweepstakes unfortunately often

to collect personal information

data are used. According to Art. 6

Clause 1 letter a DS-GVO is used for the

Collection of personal data

also in sweepstakes

consent of the person concerned required.

Therefore, the sweepstakes will also be held in

usually with the consent to advertising

advertisement, e.g. directly on a postcard,

printed.

Obtaining consent in accordance with Art. 7
DS-GVO is based on the
principles of Article 5 with EG 39 as well
as Art. 12 GDPR. The starting point
thus forms the transparency of the data
processing. Furthermore, by means of
neter technical and organizational
Measures according to Art. 24 and 32 GDPR
consent to advertising is sufficient
from the consent to participate in the
win game be delimited. ideally
The customer can choose which ones
Topics he on what ways advertising
want to receive.
The sweepstakes and consent must
therefore meet certain requirements
len, so that the consent to advertising
according to Art. 7 Paragraph 2 DS-GVO
can be generated. It must be in understandable
cher, easily accessible form and in a
clear and simple language as well as trans-
parent and understandable.
In the checks carried out and
numerous inquiries in the context of
winning games are the following data-

problem areas relevant to intellectual property law

noticed:

Return in an envelope:

Once personal data on

a lottery ticket that is about

the bare address should get out that

lottery participants clearly point out

be pointed out that data protection

an envelope for legal reasons

should be used to

authorized inspection of the address and

the other personal data

of the competition participant

other Of course, it's better to have one directly

return envelope for the one to be returned

attach answer.

Font size:

In the regulatory

checks are also numerous

che consents and sweepstakes

a font size in the millimeter range

noticed. Instead, the consent

commitment to advertising transparent and

take place regularly. This includes

of course an appropriate one – even without

Magnifying glass readable – font size. According to the

DIN 5008 standard, it is in favor of reading

even useful, in the body of the text none

font size smaller than 10 points

turn around. A clear contrast and a

sufficient sharpness, i.e. a black,

clearly visible writing, are for readers

availability just as imperative. At least in

The font can be used on the internet

increase by hand.

Consent to advertising and raffles

sung, simultaneous consent for

the entire advertising space on all

Contact ways:

The separation requirement was made by a judgment

of the BGH (1.2.2018 - Az. III ZR 196/17)

unfortunately canceled recently. previously

te man (mandatory) between the individual

n contact channels and advertising fields

Select. Nevertheless, should also after new

Legal position of the lottery participants

tion channels and individual advertising fields

be able to swipe or select individually

to. Often the consent should

ment for advertising at the same time for SMS,

Calls to landlines, calls to the

Mobile phones and advertising mails are carried out.

Consent to Advertising and

Raffle, legally binding:

If the consents on the postcard

for the sweepstakes from the consent in

data processing for advertising purposes

are not clearly separated, according to Art. 7

sentence 2 sentence 2 DS-GVO this consent

ineffective. One way to win

to separate the game from the advertising consent

are different boxes that

ticked by the contest participant

can become.

Consent to advertising is

voluntarily:

The GDPR understands "consent".

in accordance with its Art. 4 No. 11 each freely

willingly for the specific case, in inform-

way and unequivocally

given declaration of intent in the form of a

statement or any other unequivocal

confirmatory act with which the

affected person indicates that they

with the processing of the data concerning you

consent to personal data

is. Art. 7 f. GDPR is decisive,

recitals 32, 33, 38, 42, 43,

65 and 171 as well as §§ 27, 51 BDSG.

A consent is therefore only effective,

if they are based on the free decision of the

data subject is based on the

the purpose of the collection, processing

or use and, insofar as after the

states of the individual case required or

upon request, the consequences of refusal

the consent was pointed out

(So already on the old BDSG: OLG Frankfurt

am Main, 01/24/2018 - 13 U 165/16). the

Consent must therefore always be for the con-

specific case and with knowledge of the facts

be granted (Federal Court of Justice, judgment of 25.10.2012,

I ZR 169/10, juris para. 24; to the old

right) to be effective.

Transfer of data to third parties:

Should the consent be extended to other

men are extended, these must be in

the declaration of consent with names and

address must be listed explicitly, otherwise

– especially with a large number of favorable

companies – the possibility of

withdrawal of consent at any time

inappropriate to the advertiser

sen is limited (OLG Koblenz, Urt.

v. March 26, 2014, 9 U 1116/13, juris para. 39

m.w.N.; to the old law). flat fee

declarations of consent meet these requirements

at least not demands. Also the

number of beneficiary companies should

remain manageable.

Privacy notices for

Sweepstakes:

As part of the data processing for

Implementation of the competition meets the

responsible body already at the time of collection

of the personal data the information

13 DS-GVO. Hence

must read the privacy notices alongside

of consent are printed. Leaves

This is about due to the scope

not show on a postcard is a hint

refers to the data protection notices on the

Website of the provider (e.g. as a link)

by way of a so-called "media break".

fundamentally conceivable in today's opinion.

It should be clear to the customer

what happens to their data and when

these are deleted again. The data-

protection notices for the sweepstakes should

its own section in the general

data protection notices of the responsible

verbatim received.

In order to draw attention to health problems

agree to a cruise prepared

be, a tour operator wanted to

inquire about the state of health of the passengers.

The search for a legal basis for

this processing was more difficult than

waits.

A Baden-Württemberg travel company

company that offers, among other things, cruises

tet, wanted a few months before the departure of the

ship a questionnaire to the

greed ship on the different

answer questions about the state of health

should be spoken. The questions were

partially openly formulated, for example

flat rate after operations and inpatient

ren treatments in the past

five years and after regular medication

comment intake asked.

The reason given was that the

Cruising to remote waters

lead and a medical evacuation

tion (e.g. by helicopter) for days

could be impossible. Therefore it is necessary

agile, the state of health of the

to be checked in advance and any precautions

to meet. Also must before departure

of the ship to be checked whether special

medication must be carried.

Since health data to the particularly

sensitive data according to Art. 9 DS-GVO

len, both had a legal basis

according to Art. 6, as well as according to Art. 9 DS-GVO

present. Art. 9 paragraph 2 DS-GVO offers

here are different options:

• The processing is for the purpose of

health care on the basis

location of the European or German

(excl.

s

further

or

necessary

Requirements),

To the right

• the processing is to protect life

important interests of the person

and the person can be physical

or legal reasons currently no

give consent, or

• there is consent.

In addition, there are other regulations for

different cases, but none here

role played.

Our examination revealed the following:

Processing for the purpose of health

health care was certainly present here. Al

however, no (European or

find German) law that allows travel

prescribes the health

to check the condition of their customers. Also

Inquiries at the maritime medical service in

Hamburg and a shipping company surrendered here

no further insights.

Although the travel company is obliged

tet, its customers “in trouble […]

to grant assistance" (§ 651q BGB), this

does not mean, however, that this

there is already an obligation for the customer,

disclose health information. sufficient

It would be much more appropriate if the customer

before the start of the journey has the

willing to provide certain information.

The second option wasn't here either

applicable. It might be possible

comment that processing for

Protection of vital interests needed

would. However, the passengers are

able to give consent

ben (if you want it) because you

are neither unconscious nor a particular

their legal situation. A be-

special emergency, in which one

So this is where consent could go

not before.

 The only legal basis remained

with the consent according to Art. 9 paragraph 2

Letter a DS-GVO left. The travel

company has agreed to do so

implement.

Finally, it should be noted that

Travel companies should pay attention to

their customers in advance about possible

to clarify health risks and help,

advice or other support

to offer. Whether and to what extent

takes up this offer, stays

but then leave it to each individual.

If a travel company in front of a

Cruise Health Data of the Passover

greed comes as a legal

basis currently only a voluntary and

informed consent (Article 6 paragraph 1 sentence

1 letter a in conjunction with Art. 9 Para.

sentence 2 letter a DS-GVO) in question.

the transmission of a responsible

in the EU to a processor

ter in a third country (Decision 2010/87/

EU standard contract for order data transfer

arbeiter LINK) are transitional

until modified or revoked

the Commission continues to apply (Art

46 paragraph 5 sentence 2 DS-GVO), record these

However, this constellation is not. Instead of this

do they presuppose that a responsible

cher in the EU a processor

in a third country directly

applies. For a permit-free

Transfer of personal data in the

it is the constellation described at the beginning

therefore required that the responsible

In the EU, the processors im

third country commissioned and with these

– if necessary represented by others

Processors in the EU - the standards

standard contract for contract data processors

completes.

9.8 News from the area

international traffic

The DS-GVO supplements the already from the

instruments known to date

for a transfer of personal data

to countries outside the EU (third-party

der) about new approaches and instruments.

Themes from previous years settled down

continues, such as the EU-US Privacy Shield.

We still reach us again and again

Consultation requests for the following constellation

tion from the field of international

Order data processing: A responsible

literally in the EU or the European

European Economic Area (EEA).

a processor in the EU or

the EEA, which in turn has a sub-contract

processor in a third country

want to switch. The standard contract

clauses of the European Commission for

For the interpretation of the case groups of the Arti-

Article 49 of the GDPR (e.g. third-country

transfer based on consent

ment of the data subject or to safeguard

compelling legitimate interests of

those responsible) meanwhile exist

a working paper of the data protection

committee that provides valuable information on

of Article 49 (Guidelines

2/2018 on the exceptions under Article 49

of Regulation 2016/679).

Binding internal data protection regulations

ten (binding corporate rules or

BCR) are enjoying ever-increasing numbers

Popularity as a tool for transfer

personal data in third countries

within a group of companies.

The GDPR stipulates that BCR in cohesion

procedure by the data protection

Committee of all European

be dealt with by the supervisory authorities. Around

to take this into account, the

 Long-agreed informal procedures of

adapted to mutual recognition.

All data protection supervisory authorities

and the Secretariat of the European Data

Tenant Protection Committee now receive

the draft of the BCR with the

already available for content review

Opening of the actual coherence

driving The state representative for

Data protection and freedom of information

In the reporting period, Baden-Württemberg

raum as the lead supervisory authority

and as a co-examiner at several BCR

drive contributed.

The GDPR provides in Article 46 paragraph 2

lit. e and f with approved codes of conduct

regulate and approved certification

mechanisms new instruments for one

transfer to third countries, which the European

sche data protection committee currently

the creation of corresponding work

still full of life. On January 23rd

In 2019, the European Commission

Involvement of the Data Protection Committee

an adequacy decision for yes-

pan enact. The third common

review of the adequacy

Application for the USA (EU-US Privacy Shield)

by the European Commission and the

American side with the participation of

European regulators in the fall

this year has made progress on the one hand

result - so find about on the part of

American supervision increasingly

independent controls at the (self)

certified American company

men instead - on the other hand there are others

numerous open questions and significant

need for improvement. For example, the EU

European side so far no access to

all information and documents

ten that make a reliable statement about that

functioning of legal protection mechanisms

allow for those affected from Europe

would.

The coming year just promises

in relation to the international data

transfer to become exciting. late 2016

had one Irish and two French

Civil Rights Organizations Complaints

gene the adequacy decision

the EU Commission on EU-US Privacy

Shield raised. During one of these

meanwhile rejected as inadmissible

assigned (Digital Rights Ireland, Az.

T-670/16), La Quadra-

ture du Net (Az. T 738/16) still attached

gig. Also 2016 brought the Irish

data protection supervisory authority

standard contractual clauses of the EU Commission

for contract data processors before the

permanent Irish court (High Court). Of the

In mid-2018, the High Court presented the European

ical Court of Justice (ECJ) questions on the

Standard contractual clauses before (preliminary

Divorce request dated May 9, 2018, file no.

C-311/18). These relate to the

Use of Standard Contractual Clauses for

Data transfers to the United States. Also in

this procedure is in the foreseeable future

with a verdict that may go far

far-reaching statements on the admissibility of the

Data transfers to third countries included

will to count. not unlikely

that all parties involved have a "Safe Harbor II"

threatens…

The March 2018 by the US Congress

passed the so-called Cloud Act

does it allow US criminal prosecutors

authorities under certain conditions

stipulations, disclosure from outside

customer data stored in the USA

to require US providers. The European

sche data protection committee on 10.

July 2019 a first statement and

legal assessment of the effects

of the Cloud Act on data processing

tion in Europe. After that lie

for challenges based on the Cloud Act

demands that do not lead to an effective

a mutual legal assistance agreement

can, the conditions for a

Third-country transfer according to Chapter 5

of the GDPR and the general data

protective requirements for the

lawfulness of data processing,

in particular according to Article 6 DS-GVO, al-

if necessary in exceptional cases.

Data transfers to third countries

with risks for the informational self-

determination of those affected.

Therefore, data processing agencies should

len carefully check whether they have benefits in

claim that with a trans

transfer of personal data to countries

outside the EU and the European

economic area are connected.

In any case, we recommend at one

Transfer to third countries urgently for which

technical and organizational security

measures to the highest standards, e.g. Legs

strong encryption

and data protection declarations on Art

and manner and scope

ner data processing in third countries

to read carefully. Remain open in this respect

Questions, we advise against using such

offers from.

10.1 From the office

In the last activity report, I presented the challenges that this

Effective date of the General Data Protection Regulation (GDPR) and entry into force

of the State Data Protection Act for the agency as such and in particular

entailed for the employees. We've pretty much gotten along by now

consolidated and able to work in all areas.

But that doesn't mean we can sit back and relax. Next to

the still high number of cases in the specialist departments, which need to be processed in a timely manner

demanded everything from the colleagues, was also in the areas of personnel, household and

Organization of 'business as usual' no mention at all.

My goal is to ensure more staff turnover so that my colleagues can too

get to know the world outside of data protection and, in addition to personal

development, including the requirements for taking on management

creating functional functions was fulfilled more quickly and extensively than expected. That

is certainly also related to the fact that data protection in times of digitization

tion has meanwhile acquired a different status – and probably also with

our better "visibility". So it's no wonder other bodies are looking to us

and our work - and try to use our know-how (and

unfortunately also to participate in our excellent "staff"). deputy

to federal ministries and administrative courts, as well as transfers

Universities and other state authorities show that there is a change in mentality here

the other public bodies, but of course also among the employees of the service

place has occurred. As much as I hate to let my colleagues go - for them

Of course, those affected also make me happy, and I see it as an opportunity for our here

disseminate the acquired data protection competence by means of such multipliers

gen – a 'win-win situation'!

Like the state administration as a whole, we are also feeling the development

ments on the labor market, in which the public service and the economy around the

best minds competed. However, this shows that the interest in the topic of data

protection, not least fueled by the General Data Protection Regulation, some

but leads to lucrative private offers in favor of an exciting and responsible

eloquent task in a socially relevant area of the public

Turn right – the department was able to hire eight new employees in 2019

register. And with that we are completely occupied.

With a view to the fact that the state parliament of my department with the double budget

2020/2021 again awarded 10 positions, for which I am extremely grateful,

I am optimistic that I will find more colleagues to work on this task

to be able to

Speaking of the budget: My wish, which has been expressed many times, that my department for

increased

Parliament now complied. The approach was increased by EUR 75,000 for the years

2020/2021 also increased by an additional EUR 20,000 each. It does this now

possible to make urgently needed investments on a reliable basis.

Furthermore, personnel expenditure budgeting was introduced, which

ral budget responsibility extended to the area of personnel expenses and additional

creates opportunities for flexibility. We will use that intensively.

In addition, with a view to the move to new premises in 2020, we

opportunities are adequately covered with appropriate material resources. With that they can

Service and event rooms in the new domicile are modern and employee-friendly

to be equipped. This certainly contributes to increasing the motivation of colleagues

agree, especially with the space situation created by the constant increase in staff

has now reached the limit of what is reasonable.

A lot has also happened in organizational terms. In preparation for the introduction of

national E-Akte BW in the office, the introduction of the national

uniform filing plan as a prerequisite for this. The implementation that now

in January 2020, also accelerates the processes in the registry of the service

position that is particularly burdened by the high number of cases. Their relief by

Changes in the process organization, in particular through digital measures

men, was another focus of the work in the organizational area.

All in all, digitization does not stop at my office. the

Participation processes internally have been converted so that they can be paperless,

Telework has been institutionalized and expanded, and most recently mobile work too

introduced. Furthermore, the range of electronic administrative services
expanded on the department's homepage and initial preparations for the migration
the IuK of the Baden-Württemberg IT department (BITBW), which will take place in 2020
begin and should be completed by Q1/2021.
The office of the state administration has also turned to other things and is taking
at the existing interministerial working group meetings on cross-cutting issues
part. I find the exchange very profitable and would like to take part in it
thank the ministries for making the agency and its staff so
were openly admitted to the circle of the supreme state authorities. We will
contribute constructively and helpfully to these positions as well.
You can find our agency statistics in the appendix.

My office for press and public relations also provided information in the reporting
on the one hand, those interested in data protection and freedom of information about current and
publicly relevant topics. On the other hand, it is the central point of contact for jour-
nalists to answer current questions. But also inquiries from the population
especially when data protection issues are dominating the headlines
are answered here.
press work
The increasing number of inquiries from the media in recent years, be it
Interview requests, data protection issues or a request for a current position
application, proves the increasing importance of data protection. Not only takes
The number of inquiries is constantly increasing, and the range of topics is also becoming ever broader,
about which my department is asked for information or an opinion. This related
are primarily based on questions about fine procedures, the number of complaints and

Inquiries, evaluation of the GDPR, patient data protection and hacker attacks.

Press releases on privacy-related topics and events were also published

announced to the public through press releases in the year under review. In relation

the press releases were mainly influenced by the results of the municipal survey

important topic, but also communications on artificial intelligence (AI), the first

Fine against a police officer as well as our control measures have become one

led to great press coverage.

Press conferences were also held on February 4, 2019 and November 4, 2019.

The thematic hooks were the presentation of the 34th data protection

ness report and the presentation of the results of the data protection survey at the

Municipalities in Baden-Württemberg.

Surname

The results of the municipal data protection survey by the LfDI are available

Results of the community survey

Presentation of the results of the community survey

Brochure Municipalities (December 2019)

04.11.

09.10.

On the use of cookies and cookie banners

09.09.

Data protection officers strengthen companies

08/19

Artificial intelligence - and its consequences

07/31

Municipalities in Baden-Württemberg need more support in implementing the

data protection

07/30

Data breaches are a growing concern

28.06.

Data breaches in registration information

06/18

First fine against police officers

03.06.

Cinema session with the state representative

05/24

The first IFG-Days Baden-Württemberg

04/22

More light! – Design shared responsibility in a meaningful way

09.04.

Transparency protects academic freedom

08.04.

Control measures for the GDPR are in place

20.03.

Discussion with Federal Minister of Justice Katarina Barley

03/11

School lessons of a different kind

02/28

LfDI Baden-Württemberg imposes a fine on former Juso state boss

116

LfDI BW - 35th activity report 2019 - From the office 14.02.

Students develop solutions for data protection

02/11

Keep cool during cold Brexit

04.02.

LfDI Dr. Stefan Brink presents the 34th activity report on data protection

01/30

Nationwide cooperation between supervisory authorities supports BvD initiative

01/22

Clean up after the political hack

117

LfDI BW - 35th Activity Report 2019 - From the website department

The website of my office is obviously used nationwide and allows,

after feedback from users, the conclusion to be greatly appreciated.

In addition to retrieving current information, brochures and leaflets are available

all things also our contact forms are used actively:

Incoming figures online complaint form:

118

LfDI BW - 35th activity report 2019 - From the incoming figures "Notification of a violation of the protection of personal data

according to Art. 33 DS-GVO" May 2018 to December 2019:

Contact details of the data protection officer:

Since May 2018, my department has received around 32,000 contact details using an online form

reported by data protection officers.

FAQs

So that you can quickly and easily get an overview of our topics

we have frequently asked questions in a separate section on our website

summarized with the corresponding answers:

• Data protection in the doctor's office

• Cookies and tracking

• Photography and data protection – We are in the picture!

•

• Municipalities

• Data protection in nursing

Freedom of Information

• Societies

• Publication of photos specifically for clubs

More FAQs will be added to this section on a regular basis. So it's worth going here

keep checking back.

newsletter

The newsletter of my office is published several times a year and has

currently more than 3,500 subscribers.

You can subscribe to the newsletter here:

https://www.baden-wuerttemberg.datenschutz.de/newsletter-anmeldung/

publications

In the past period, important new brochures and samples have been

public. On my website under the heading "Infothek" you will find numerous

rich various materials with explanations, definitions and references to the

individual regulations and their implementation.

I would particularly recommend reading the following guides from my official

Job:

• Brochure "Order processing according to DS-GVO"

• Brochure "Persons' rights"

• Practical guide "The Commissioner for Data Protection" - Part I and Part II

• Brochure "Photography and data protection - compact and practice-oriented"

• Guide to employee data protection

• Orientation guide "Data protection in the association according to the DS-GVO"

• Practical guide for clubs

• Video surveillance by public authorities in Baden-Württemberg

• Brochure "What you can do against unwanted advertising"

We are always open to your feedback on our press and public relations work

Ear! My team will respond to the comments at the email address pressestelle@lfdi.bwl.de

take up, comment on the proposals and suggestions and answer questions.

With the support of the users, we not only want our digital offer to be good, but

to do better.

structure of the office

The Office of the State Commissioner for Data Protection and Information

heit has 53.5 permanent positions and is divided into six departments and the European staff unit

articulated. The respective leaders and their main topics are the

can be found in the overview below. If you have any questions, please contact our

telephone exchange (0711 / 61 55 41 – 0).

Switchboard: 0711 / 61 55 41 - 0

The switchboard is open Monday to Friday from 9 a.m. to 12 p.m. and Monday to

also manned on Thursdays from 2:00 p.m. to 3:30 p.m.

Fax: 0711 / 61 55 41 - 15

Email: poststelle@lfdi.bwl.de

designation

complaints

-□public area

- non-public area

controls

-□public area

- non-public area

consultations

-□public area

- non-public area

2016

2017

2018

2019

840

1208

12

4

878

637

1186

1872

1188

2714

23

32

991

795

5

8th

1492

2948

972

2785

39

72

1289

2553

122

LfDI BW - 35th Activity Report 2019 - From the Tables for Article 1.6 "E-mail advertising according to § 7 Paragraph 3 UWG"

Examples regarding goods:

Purchased Goods

goods with corresponding

typical use and

possible uses

Classic accessories or

spare Parts

traffic usual

supplementary goods

men's shoe

children's bike

Other men's shoes

Tricycles, scooters, balance bikes

Insole, laces

kids bike helmets,

air pumps, bicycle baskets

Women's winter coat

laser printer

Ticket for one

Opera

Women's winter jackets

inkjet printer

Tickets for classic

music and ballet

---

color cartridges

---

shoe polish

bicycle insurance,

theft protection,

bike financing

gloves, scarf, hat

paper

Ticket, ticket vouchers

E-MAIL ADVERTISING ACCORDING TO SECTION 7 PAR. 3 UWG PERMITTED

Examples of services:

services with

rendered

corresponding, typical

service

performance goals

Classic accessories

traffic usual

additional or

supplementary services

Printing of business cards

(on-line)

online booking

Package tour to

Nice (flight, hotel)

Online Cell Phone Contract

online car rental

contract

Online photo development

(on paper)

Printing of stationery or

envelopes

Package tours to

France

business card case,

business card stand

cancellation insurance

Personalized printing

of objects

Rental cars, excursion packages

other telecom

contracts

Other rental car contracts

Other photo developments

mobile phone, charging cable, music

or Filmflat, mobile phone spare parts

Rent navigation device, rent

child seat

Photo album, photo glue

Cell Phone Insurance

Hotel accommodation

photo book printing,

posters, calendars

E-MAIL ADVERTISING ACCORDING TO SECTION 7 PAR. 3 UWG PERMITTED

The individual categories are defined according to DIN EN 62676-4 (https://www.din.de/de/service-fuer-anwender/din-term).

defined as follows:

Monitor

Allows you to view count, orientation

and speed of human movements

over a large area, provided their application

is known to the operator.

Allows the operator to be reliable and easy

determine whether any target, e.g. B. a person,

is present or not.

Allows characteristic details of in-

divide, such as g. conspicuous clothing, while

a view of activities in the environment of a

if granted.

Allows the operator to recognize an in-

individuals.

Enables the unequivocal identification of an individual

viduums.

Enables even with difficult contrast conditions

the unequivocal identification of an individual.

detect

Watch

Recognize

Identify

Check over

Results of the Hearing

the state representative for data protection and

Freedom of information Baden-Württemberg

from June 28, 2019 at the IHK Stuttgart

to the

Evaluation of the GDPR

-

"If it doesn't make sense, then it's not privacy."

- For practical data protection in Baden-Württemberg -

125

1

LfDI BW - 35th Activity Report 2019 - Appendix

contents

Foreword 3

1. Obligations to provide information, information and transparency 5

Solution approaches 6

2. Processing directory 7

Solution approaches 7

3. Obligation to appoint data protection officers..... ..... 8th

Solution approaches 9

5. Manufacturer's liability - "privacy by design" 10

Solution approaches 11

5. Ambiguities in the joint responsibility, especially in the "social media" area

.... 12

Solution approaches 12

Conclusion 14

126

2

LfDI BW - 35th Activity Report 2019 - Appendix

foreword

Since May 25, 2018, he has been the state commissioner for data protection and freedom of information

Baden-Württemberg (LfDI BW) legally obliged to comply with the regulation (EU)

2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons in the processing of personal data, on the free movement of data and on Repeal of Directive 95/46/EG, in short: the General Data Protection Regulation - DS-GVO in Baden-Württemberg and to advise those responsible in the state.

Art. 97 para. 1 DS-GVO provides that the EU Commission must inform the EU Parliament and the Council by 25 May 2020 submitting a report on the assessment and review of the GDPR. Article 97 paragraph 3 DS-GVO gives the Commission the right to obtain information from the request supervisory authorities. The LfDI Baden-Württemberg also wants to do this Assessments, which are based on the previous practical experience of its independent supreme State authority results, give notice and takes the opportunity to make suggestions to submit an evaluation of the GDPR.

- DSK) has teamed up with The conference of the independent data protection supervisory authorities of the federal and state governments (Privacy Conference their “Experience report of the independent Data protection supervisory authorities" from November 06, 2019, which was issued by the LfDI Baden-Württemberg was supported, already with the one from their experience with the application of the GDPR resulting proposed changes to the European Data Protection Board. The The LfDI Baden-Württemberg inside.

The perspective of the supervisory authorities is certainly important and helpful for the EU Commission - not little important, however, are the experiences that those responsible and those applying the DS-have collected GMOs in Baden-Württemberg – literally on their own bodies. About this one To take experiences into account, the LfDI Baden-Württemberg held a hearing on June 28, 2019 under the banner "#DSGVO works (?) - 1 year GDPR - practical experience and evaluation" in cooperation with the

Chamber of Industry and Commerce in the Stuttgart region. to

Invited keynote speeches were representatives from supervisory authorities, authorities, business, science,

Lawyers, associations and data processors. In a specially set up e-mail

Letters from all parts of the country were also received in the mailbox throughout the year

collected and evaluated - also from this "low-threshold" possibility, criticism and

Numerous institutions such as associations and clubs have suggestions for the GDPR to submit, but

many private individuals also made use of it.

The circle of those responsible in Baden-Württemberg is only partially in line with the national average

comparable. According to the Baden-Württemberg Ministry of Economics and Finance

small and medium-sized companies, for example, every second euro in sales

in the country and

employ two thirds of the employees subject to social security contributions. The middle class is with it

the backbone of the economy in Baden-Württemberg - and makes a decisive contribution

economic development. Also committed to a report by the Ministry of

Social affairs and integration in Baden-Württemberg According to almost every second Baden-Württemberger in

volunteer in clubs and associations in their free time: over 48 percent of citizens

citizens do this. This makes Baden-Württemberg the number one nationwide. This also results

very own, specific challenges and concerns for practical data protection.

These country-specific findings should - in addition to the experience report of the DSK - make a contribution

for the evaluation of the GDPR by the European legislator.

Overall, it has been shown that those responsible in Baden-Württemberg are in many areas

want solutions that are more suitable for everyday use and some regulations only deal heavily with data processing

Small business activities or volunteer work are applicable. In the foreground

there are above all questions about a possible relief in the information, transparency and
Obligations to provide information, but also in questions of joint responsibility and
Order data processing. Despite numerous samples and practical guides from my department and
There still seems to be a certain degree of legal uncertainty among the other supervisory authorities
to be responsible. Contrary to expectations, there were concerns about sanctions – at least
under the practice in Baden-Württemberg - not highlighted as a priority. This may not last
due to the fact that in Baden-Württemberg it was repeatedly made clear that advice
Punishment goes - and that many responsible persons are on the way to a data protection compliant
have done processing. According to a DIHK survey, around 75% of the companies in the state stated that
to have (at least partially) implemented the GDPR. My experiences with it are in
Overall congruent.
Data protection supervision in Baden-Württemberg is based on the principle "If it doesn't make sense
then it is not data protection". The present report is also intended to meet this objective
be understood. It reflects the voices from the country, which my department contributes
in their day-to-day work and throughout the evaluation process. This
The report is a compilation of the experiences and suggestions of those responsible and
affected in the country. As a supervisory authority, we see it as our duty, as does the European level
to make those voices heard

dr Stefan Brink

The state commissioner for data protection and freedom of information in Baden-Württemberg

1. Information, disclosure and transparency obligations

The DS-GVO brings obligations that affect small clubs as well as corporations like Apple,
Amazon, Google, Microsoft or Facebook. Including numerous obligations, which the

previously unknown to federal legislation. The LfDI Baden-Württemberg receives numerous concerned
Inquiries and complaints from clubs that feel overwhelmed or threats of sanctions
fear of misconduct. Advice alone is not enough for the clubs in the country, it will be
actual relief required. Clubs and small businesses can be in contrast to
larger companies often cannot afford external experts.
Many small and medium-sized businesses and volunteers have in practice significant
Difficulties in comprehensively fulfilling the statutory information requirements. It applies to
avoid that volunteering in particular becomes a liability risk for those responsible
becomes. At the same time, compliance with the level of data protection must be in the interests of all citizens
citizens are guaranteed. Here must be used in the course of the application of the GDPR
knowledge gained can be found in a practicable and meaningful way in the long term.
in the context of
Especially for small companies, whose data processing is mainly
Customer relations takes place, seems to fulfill the
Information obligations often with
associated with a disproportionate amount of effort or simply not realizable. in the
Within the framework of company-customer relationships, the commissioning customer is often faced with many of the
data subject to information is already known. For this purpose
however rarely for example the
legal basis for data processing. It seems questionable, however, whether this applies to everyone
placing the order is actually of interest. At this point, those affected often complain about a
unwanted flood of information. It would be worth considering whether taking into account the risk-based
Approach the assignment, for example
less risky
Data processing should only be subject to lighter regulations.
of a craft business

The principle of "one size fits all" works particularly well with the information and transparency obligations
not in practice. One consideration would therefore be whether for controllers whose core activity is not the
Data processing is, exceptions could be created. Differences are in everyday life too
clearly recognizable where there is already a lot of information in the context of business relationships
are available and there is a certain level of equality between those involved. With many contractual or
contractual relationships, data protection requirements are often seen as a bureaucratic burden
seen added value.
Information obligations must be "easily accessible". This should
however, just none
Excess information arise, which tempts to no longer use the information at all
perceive as the distinction between essential information and those that are not
are primarily of interest is difficult. In individual cases, this can lead to a lack of rather than to
promoting transparency. This development must be counteracted.
However, general exceptions to the duties of those responsible always harbor the danger of the goal
contrary to the rule itself. Any facilitating change would therefore have to be on it
Care should be taken to draw the boundaries so clearly that the actual target audience is the larger
data-processing companies or companies with data-processing core activities
may fall under the exemptions.

5

The obligation to provide information according to Art. 15 DS-GVO often puts those responsible before the big ones
Challenges. In part, a perversion of the right to information as an instrument of
"Vigilante" reports. Actually are - especially in exchange with public authorities, but also
in our own work as a reporting body - again and again questions of interpretation, above all
met on the right to copy. Here it is unclear how far this goes and whether the concept of

"Copy" is accompanied by a right to be handed over in paper form. The distinction between

the "information about this personal data" according to paragraph 1 sentence 1, the information about "the

Categories of personal data that are processed" according to paragraph 1 sentence 1 lit. b and the "Copy

of personal data "according to paragraph 3 sentence 1 falls responsible both in the public and

equally difficult in the non-public area.

solutions

 Equivalence of the exemptions of Art. 13 and 14 GDPR

 Raising or differentiating the risk level in Art. 13 and 14 GDPR

 Exceptions to information obligations, for example for data processing

privileged purposes, in favor of companies whose data processing is not purpose

of the business activity or in favor of the secrecy interests of the

responsible

 Introduction of a 250-person limit (similar to Art. 30 Para. 5 GDPR) for

information requirements

 Introduction of definitions and differentiation of the obligations of micro-enterprises and

small and medium-sized enterprises (SMEs),

for example following the recommendation of the Commission of 6 May 2003 regarding the definition

micro, small and medium-sized enterprises (Ref. K(2003) 1422)

 Deletion of the information requirements arising “at the time of collection” for

certain case scenarios

 Admission of the so-called media discontinuity for low-risk case constellations and legal ones

Standardization of the necessary information in a two-stage process

 Modification of deadlines for providing information in day-to-day operations under

Taking into account the purpose of the regulations on information obligations

 Standardization of privacy statements on websites

 The "necessity" in the information requirements of the "specific circumstances"

dependent in order to be able to deal with everyday situations

 Clarification that specifying a category of recipients is also sufficient if

the person responsible knows the recipient specifically

 Clarification of the relationship between transparency obligations and operational and

trade secrets

 Limitation of the right to information, for example via an objection of proportionality,

further sharpening of the objection to abuse Art. 12 Para. 5 S. 2 "in the case of obvious

unfounded requests", conceptual clarification or deletion Right to "copy"

130

2. Processing record

The creation of the register of processing activities provides for small and medium-sized

companies often present a difficult challenge to overcome.

With Art. 30 Para. 5 DS-GVO, the GDPR holds an exception to the obligation

Companies or institutions that employ fewer than 250 people, provided that the

processing carried out by them does not pose a risk to the rights and freedoms of the

data subjects, the processing is not occasional or not

Processing of special data categories according to Article 9 DS-GVO or the processing of

personal data on criminal convictions and offenses within the meaning of Art. 10

GDPR includes.

In practice, however, this exemption is as good as it gets for small and medium-sized companies

never relevant. The counter-exceptions to this are so far-reaching that hardly any company from

benefited from this exception. Employing a little less than 250 people is one

only occasional processing of personal data is hardly possible. Any business that

employees, inevitably processes at least their data to carry out the

employment relationship - also health data within the framework of absence management or the

Religious affiliation in the context of tax administration. The exception fails at the latest

"occasional" processing in the sense of "frequency". This should not be the legislative objective

have been. The only way to counteract this undesirable consequence is this

Restriction of the counter-exception of Art. 30 Para. 5 DS-GVO. In this “unsuccessful

Return exemption regulation" is seen as an urgent need for adjustment.

The risk-based approach actually intended does not apply here. "One size fits all" seems

not working here either. It would be understandable for those responsible if, for example

would be geared more towards a data-processing core activity and for other controllers

lower requirements would apply, e.g. in business relationships. Here would be one

Differentiation on the basis of the core activity take more account of the actual aim of the regulation.

In return, the threshold for the number of employees could be lowered.

solutions

 Replacement of the frequency requirement of Art. 30 Para. 5 DS-GVO by switching to

Data processing as a core activity of the company (e.g. similar to Art. 37 Para. 1

lit. b GDPR)

 Creation of privileged processing categories, for example for business relationships

 Sensitive categories of personal data according to Art. 9 GDPR as the only exception

 Increasing the risk level

3. Obligation to appoint data protection officers

The call for the abolition of the obligation to designate data protection officers is probably nationwide

heard most often. The overall benefit of the obligation to designate and the obligation to report to the

Data protection regulators are often questioned, especially when it comes to smaller clubs

or company goes.

The goal of harmonization of law at European level is often not achieved here

viewed. Wide opening clauses are criticized, different application of the law can up to

lead to competitive disadvantages. Here, too, the risk-based approach is often strengthened

approach, facilitating low-risk data processing and focusing on quality

and quantity of data processing required.

Since the national legislature raised the personal limit in the Federal Data Protection Act of

turned ten into twenty, the topic became quieter at first. However, will

those responsible soon realize that a lack of a designation or reporting obligation does not apply to them

relieved of their duties as data protection officer.

In this discussion, it should be borne in mind that the data protection officers are responsible for a competent

provide advice on data protection law in order to avoid data protection violations in advance and

last but not least, to keep the risk of sanctions low. It is often forgotten that even if the

obligation to designate, the obligations under data protection law remain in place, internal advice and

however, the acquired expertise is lost. A cessation would be perceived as a relief in the short term

be, however, when the next data protection question arises, a

There is no internal possibility of recourse and the LfDI could take care of all individual cases

Clubs in Baden-Württemberg cannot guarantee this even with massive increases in staff.

is also not an end in itself. The basic

The obligation to report to the supervisory authority

Abolition of the reporting obligation of the data protection officer would control the

regulators

difficult in this area. The obligation to report also comes a

self-control function - also with regard to the development of a data protection organization. A

Data protection officer ensures the protection of the rights of employees and citizens, their

data are processed. Data protection officers offer the opportunity to spread know-how without

to be dependent on service providers who work more on a flat-rate basis.

According to the risk-based approach, which is also the basis of the provisions of Art. 37 et seq. GDPR

a data protection officer only has to be appointed if this is due to the risk

is required. The determination of the risk, however, is based on rather rigid assumptions

made dependent. The risk-based approach could certainly be given greater weight here

will.

Above all, Bavaria has passed the registration obligation for amateur sports clubs, music bands and others

voluntary commitment supported clubs abolished. Should this prove to be compatible with

German and European data protection law should be considered here

legal clarification of such possibilities

to be included in the legal text in order to

bring about Europe-wide relief. However, ways would have to be found to

advice on compliance with the existing obligations could still be guaranteed,

for example by setting up a central advice center with the appropriate equipment.

8th

solutions

 Exceptional rules for non-commercial associations that work exclusively on a voluntary basis

 Derogations for micro-enterprises, combined with an appropriate one

legal definition

 Alignment of the obligation to order in the public and non-public area,

instead, differentiation of obligations based on company size or industry

 Establishment of a central advice center for those who are exempt from the obligation to order

responsible

9

5. Manufacturer liability - "privacy by design"

With privacy by design / privacy by default, the GDPR sets out principles that are aimed at manufacturers

but does not oblige manufacturers as such. Manufacturers, suppliers,

Importers, sellers, etc. are held accountable, as is the case in product liability law

(ProdHaftG or RL 85/374/EWG) is already the case.

With the term "data protection through technology design" (Privacy by Design), which is defined in Article 25 Para. 1 DS-

GMO is prescribed for the person responsible, in practice the group of addressees turns out to be

not out far enough. Since those responsible do not usually develop software themselves

and in large parts standard and application software from manufacturers or suppliers, in part

even by those with global, national or regional monopoly or at least

market-dominant position, have to obtain and use, this requirement often comes to nothing.

You should therefore also encourage software manufacturers to comply with this privacy policy

Commit to the design principle. In practice, this applies in particular to manufacturers of complex software such as e.g.

B. operating systems, database management systems, standard office packages or

very

special specialist applications.

Operating systems around are on the market only

available in limited numbers, so

Those responsible for servers, desktop computers, notebooks, tablets, smartphones or similar

Operate devices, have to resort to one of those. Usually these are at the time of purchase

already pre-installed by the user. According to the current legal situation, it is the duty of

those responsible, any weak points relevant to data protection law, incorrect configurations

to find and turn off functions, etc., that you consider undesirable. None applies to the manufacturer

obligation to deliver its products without these defects. The situation is similar in everyday situations,

For example, with front door locking systems via smartphone app or other "smart home" applications.

Possibly between the responsible app and the m

in a third country without

appropriate level of data protection) manufacturer data traffic takes place. Uses

If such systems are used, it is itself responsible and must process data

responsible, which it cannot see through. The manufacturer is not effectively available. sets one

A private person who uses such systems in the context of private family activities is a responsible party

i.S.d. DS-GVO already not available. The obligations of the DS-GVO do not affect anyone, so go into

Empty.

The previous legal situation contradicts the approach of "data protection by design" or "by default".

Contrary to recital 78 sentence 4 DS-GVO, manufacturers are in no way encouraged to “the right

to data protection in the development and design of the products, services and applications

take into account and ensure, with due regard to the state of the art,

that controllers and processors are able to meet their data protection obligations

to comply". This not only leaves significant gaps

in the field of protection

personal data, but there is a potentiation of technical and

bureaucratic effort in the attempt to eliminate deficiencies in a decentralized manner that are caused centrally

will. This burdens all controllers and processors, with SMEs disproportionately

be charged.

134

The legal situation also contradicts that which has been harmonized via Directive 85/374/EEC

product liability law. According to this, manufacturers, importers, suppliers, etc. are liable for damage caused by

their products are created. This legal situation, which has already been harmonised, should be placed in the area of protection

personal data to be transferred. For products relevant to data protection law

therefore the manufacturer should also be held responsible.

Going beyond the position of the DSK, the LfDI Baden-Württemberg takes the view that

the enforcement of a legal situation adapted as described would only be possible if the

Data protection supervisory authorities also to monitor compliance with data protection at manufacturers,

Importers, suppliers, etc. would be authorized.

solutions

 Insertion of a manufacturer definition based on the product liability guideline in the

general definitions and inclusion in all responsible person duties

in the obligations to cooperate with the supervisory authorities and in the

Competence, task and authority standards of the supervisory authorities as well as in the

Possibilities of sanctions for the purpose of effective legal enforcement

such as

5. Ambiguities in the joint responsibility,

especially in the "social media" area

The entry into force of the DS-GVO has in particular the operation of websites and the use

caused massive uncertainty by social media.

Questions about joint responsibility according to Art. 26 DS-GVO and the delimitation to

Order data processing according to Art. 28 DS-GVO is the result. Frequently, in case of rejection

processing on behalf of a joint responsibility, but this regularly

not available.

A survey by my authority in the municipalities in Baden-Württemberg has the subject

“Online Usage Data Sharing” revealed that almost every municipality has a website and

more than half of them incorporate content or elements from third parties (e.g. Google/Facebook) into the site

involves. This often has the consequence that the entire usage behavior of website visitors

passed on to third parties without any apparent legal basis.

In other constellations, consent is used as the legal basis. the actual

In practice, the aim of user protection does not seem to be achieved by consent buttons and banners

but, on the contrary, tends to lead to defensive reactions. With so-called "tracking" or

"Targeting" on websites by third-party tools or web analysis tools often poses the

Question about the legal basis and the fulfillment of the information obligations.

Especially when operating pages on social media, according to the latest decisions of the

ECJ to categorize as joint responsibility for the site operators the question of how

they are to realize the resulting obligations. In practice, there is often

Owner does not have the opportunity to influence the joint data processing and purpose

and resources, let alone make this transparent. Even if the possibility

exists, the jointly responsible persons within the framework of Art. 26 without further assistance

Supervisory authority - such as through our "Contract model for an agreement according to Art.

26 DS-GVO" - it is not clear which essential contents are to be defined, so that a large number

of insufficient agreements and those affected have clarity about the correct one

Contact person is missing. The regulation of Art. 26 GDPR is often described as deficient. It will

There is also a need for clarification with regard to the transparency requirements and the legal relationship

of those responsible seen each other.

solutions

 Clearer demarcation criteria between joint responsibility according to Art. 26 DS-

GVO and order data processing according to Art. 28 DS-GVO

 Clarification to the effect that the fulfilled facts of a common

Responsibility no legal basis for the data exchange between the parties involved

responsible

 Orientation of the right of the data subject based on the organizational obligation and limitation of

range of joint liability to an adequate extent

136

12

LfDI BW - 35th Activity Report 2019 - Appendix

 Clarification that a shared responsibility for an entire application or

also exist for an entire project, but also only a part of it

entire processing system

 Clarification of when joint responsibility can exist, for example

o if two or more responsible persons decide which persons are involved in the

are involved in data processing and have access to the data,

o which categories of personal data should be collected,

o how the personal data should be collected,

o on what legal basis the data processing is carried out

target,

o which technical and organizational measures should be taken,

o when personal data will be deleted;

o give rise to data collection, or

o in the case of joint processing of personal data, your own individual

follow goals

 Clarification that Joint Controllers will regularly review their

agree on mutual obligations

 Standardization of a regulation similar to order processing to the essential ones

contents of an agreement on joint responsibility

 Promotion of further guidelines at European level

Conclusion

Despite all the criticism, one must not forget the advantages that the new data protection law offers. One has now, especially in relation to other economic areas, a uniform European one Instrument. Civil rights have clearly been strengthened as a result. So the GDPR is a Successful model - with potential for improvement.

For its task, the European Commission needs the further development of data protection law all experiences from the application of the GDPR; not just from a regulatory perspective, but full. We make a contribution to this.

The LfDI is aware of the fact that the chances of actual changes in the law EU level after the long negotiations when the GDPR came about and the current ones Experiences from the negotiations on the ePrivacy Regulation are rather limited. Nevertheless we see it as our task to continue to monitor the application of the GDPR on site and an open ear for the concerns and problems of those responsible in Baden-Württemberg - and the knowledge gained in this way to the legislators in the state, in the federal government and in Europe to carry on.

A

Accreditation 8

Destruction of files/data carriers 32

Document shredding 98

Outpatient nursing service 78

doctor's offices 20

Processor 97

Order processing 95

Request for information 28

Right to information 25

B

Powers of the supervisory authorities and sanction practice 8

Employee data protection 95

Data subject rights 26, 28, 64, 68, 81, 91, 120

Body cams 17

Credit check 102

Fine 70, 115

fines 33

BvD 16

D

Data protection by design 8

Breaches 8, 20

Privacy notice 106

Service agreement on the use of information technology 88

direct mail 8

E

self-promotion 24

Consent 106

email 77

Email promotion 23

Emotet 29

Eurodac 48

European Data Protection Board (EDPB) 37

European Data Protection Board 36

f

Telecommunications secrecy 87

remote maintenance 30

Cells 47

G

Money Laundering Act 102

health 108

Sweepstakes 107

Home nursing 77

House manager 101

property management 99

Home supervisors 80

I

Information obligations 81

Information and transparency obligations 7

J

Job Center 77

Youth Welfare Office 77

K

Day care centers 89

control visit 17

Ministry of Culture 90

Customer rating 24

artificial intelligence 8

M

malware 28

messenger services 15

N

Rules of Use 87

P

Parking surveillance 96

ID card copy 101

Phishing 28

police 17

Pre recording 18

Private internet or e-mail use 87

R

Right to information and a copy 28

tour operator 108

S

school 90

School information technology 87

School law 87

social media 37

Social worker 77

T

Technical and organizational data protection 20, 28, 124

poll 10

Unfair competition (UWG) 23

V

accountability 97

Connected vehicles 37

Insurance company 103

Administrative regulation on data protection in public schools 90

video surveillance 35

W

Advertising contradiction 25

Advertisement 23, 123

Condominium association 99, 101

Wound manager 77

Z

earmarking 8