Forty-eighth activity report

to data protection

and

Second activity report

to freedom of information

of

Hessian Commissioner for Data Protection

and freedom of information

professor dr Michael Ronellenfitsch

submitted as of December 31, 2019

according to Art. 59 of Regulation (EU) No. 2016/679 i. in conjunction with Section 15

of the Hessian Data Protection and Freedom of Information Act

and Section 89 of the Hessian Data Protection and Freedom of Information Act

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection / 2nd activity report on freedom of information

Contributions to data protection and freedom of information

Published by the Hessian Commissioner for Data Protection and Freedom of Information

Prof. Dr. Michael Ronellenfitsch

Gustav-Stresemann-Ring 1, 65189 Wiesbaden

PO Box 31 63, 65021 Wiesbaden

Phone:

Fax:

E-mail:

Internet:

(06 11) 14 08-0

(06 11) 14 08-9 00 or 14 08-9 01

poststelle@datenschutz.hessen.de

www.datenschutz.hessen.de

Design: Satzbüro Peters, www.satzbuero-peters.de

Production: AC medienhaus GmbH, Ostring 13, 65205 Wiesbaden-Nordenstadt

Table of contents

Table of contents

III

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection / 2nd activity report on freedom of information

X

List of Abbreviations

List of Abbreviations

List of Abbreviations

a. a. O.

a. f

Section.

Inc

AI

AK technique

kind

at the specified location

old version

Unit volume

public company

artificial intelligence

Technology working group

Article

BAR

BCR

BDSG

BDSG a. f

BfDI

Civil Code

Federal Law Gazette

BGH

BMG

BORA

BRAOO

BReg

BRPrints.

e.g.

BTprints.

BTHG

BVerfSchG

or.

approx.

CVC

Federal working group for rehabilitation

Binding Corporate Rules (binding internal

data protection regulations)

Federal Data Protection Act

Federal Data Protection Act old version

Federal Commissioner for Data Protection and

Freedom of Information

Civil Code

Federal Law Gazette

Federal Court of Justice

Federal Registration Act

professional regulations for lawyers

Federal Lawyers Act

federal government

Federal Council printed matter

for example

Bundestag printed matter

Federal Participation Act

Federal Constitutional Protection Act

respectively

approximately

Card Value Code

That means

i.e. H.

German Accreditation Body

DAkkS

German industry standard(s)

DIN

DPIA

Data Protection Impact Assessment

DS-GVO/DSGVO General Data Protection Regulation

XI

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection / 2nd activity report on freedom of information

Conference of the independent data protection supervisory

federal and state authorities; short: data

protection conference

registered association

European Data Protection Board

European Data Protection Supervisor

(European Data Protection Supervisor)

European Data Protection Board

recital

et cetera

European Union

Court of Justice of the European Union

constitution

in which case

Joint Control Authority

basically

Jurisdiction Act

census of buildings and dwellings

Hessian representative for data protection and

Freedom of Information

Hessian data protection officer

Hessian Data Protection Act

Hessian Data Protection and Freedom of Information

law

Hessian Teacher Education Act

Hessian Ministry of the Interior and Sport

Hessian law on public safety

and order

Hypertext Markup Language

Hypertext Transfer Protocol

Hessian Constitutional Protection Act

Hessian law on public survey

information and geographic information

Hessian administrative and procedural law

Hessian headquarters for data processing

usually

in terms of

DSK

e. V

EDPB

EDPS

EDSA

recital

Etc.

EU

ECJ

GG

possibly.

GKI

basically

GVG

GWZ

HBDI

HDSB

HDSG

HDSIG

HLBG

HMDIS

HSOG

HTML

HTTP

HVSG

HVGG

HVwVfG

HZD

i. i.e. R

i. s.d.

XII

i. S.v.

i. V. m.

ID

IFK

IMI

Incl.

esp.

IT

ITZ Association

AI

CIS

SMEs

LfV

lit.

LKA

LTDprints.

LUSD

m.e.

MDK

o. a.

above

OH

OwiG

PDF

List of Abbreviations

with the meaning of

combined with

ID

Conference of the Freedom of Information Officers

federal and state; in short: freedom of information

conference

Internal Market Information System

information system)

included

in particular

information technology

Federal Information Technology Center

Artificial intelligence

hospital information system

small or medium-sized company

State Office for the Protection of the Constitution

littera

State Criminal Police Office

State Parliament printed matter

Teacher and student database

in my opinion

medical service of the health insurance

specified/specified/specified/specified above

good

above/named/named/named

guidance

Administrative Offenses Act

Portable document format

No./Rn.

marginal number

S

s.

s.a.

see above

see below

page or sentence

please refer

see also

see above

see below

XIII

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection / 2nd activity report on freedom of information

Standard Privacy Model

social code

so-called/so-called/so-called

Secure Sockets Layer

Official State Publisher for the Federal State of Hessen

Code of Criminal Procedure

activity report

technical-organizational measure

among other things

and similar/more similar/similar

in certain circumstances

Sub-working group on data protection impact assessment

United States of America

and so forth

compare

Police and Criminal Prosecution Access Act

authorities and intelligence services on the visa

Information system (VIS Access Act)

Virtual Private Network

working paper

for example

digit

SDM

SGB

so-called.

SSL

StNumber

StPO

TB

TOM

etc.

etc.

u. u.

UAG DPFA

UNITED STATES)

etc.

see.

VISZG

VPN

WP

e.g. B.

item

XIV

Register of Legislation

Register of Legislation*

Register of Legislation

*The versions valid at the time of processing are quoted.

law/regulation

site(s)

BDSG

BDSG a. f

Civil Code

BMG

BORA

BRAOO

GDPR

Federal Data Protection Act of 06/30/2017 (Federal Law Gazette I p. 2097)

Federal Data Protection Act i. i.e. F. from 14.01.2003 (Federal Law Gazette I p. 66),

last amended by law from October 30th, 2017 (Federal Law Gazette I p. 3618)

m. W. v. 11/09/2017, expired on 05/25/2018 due to

Law of 06/30/2017 (Federal Law Gazette I p. 2097)

Civil Code i. i.e. F. from 02.01.2002 (Federal Law Gazette I p. 42)

Federal Registration Act of May 3, 2013 (Federal Law Gazette I p. 1084) last

modified by art. 1 law of 22.11.2019

Professional Code for Lawyers in the version of January 1st, 2020,

last amended by resolution of the Articles of Association of

06.05.2019, BRAK-Mitt. 2019, 245 f.

Federal Lawyers' Act in the Federal Law Gazette Part III,

Outline number 303-8, published revised version,

last modified by article 14 of the law of December 12th

2019 (BGBl. I p. 2602)

Regulation (EU) 2016/679 of the European Parliament and of

Council of 04/27/2016 for the protection of natural persons in the

Processing of personal data, free movement of data

and repealing Directive 95/46/EC (Privacy

Basic Regulation) (OJ EU L 119 p. 1)

G.GegG

Law of 18 April 2019 on the protection of commercial secrets

(BGBl. I p. 466)

HBO

HDSG

HDSIG

Hessian building regulations from 28.05.2018 (GVBl. p. 198)

Hessian Data Protection Act i. i.e. F. from 07.01.1999 (GVBl. I p. 98),

repealed on 05/25/2018 by law of 05/03/2018

(GVBl. p. 82)

Hessian Data Protection and Freedom of Information Act of

May 3, 2018 (GVBl. p. 82), came into force on May 25, 2018, changed

by Art. 5 of the law of September 12, 2018 (GVBl. p. 570)

HessStvollzG

Hessian prison law

Commercial Code in the BGBl Part III, structure number 4100-

1, published clean version, last modified by Article

3 of the law of December 12, 2019 (Federal Law Gazette I p. 2637)

Hessian Municipal Code in the version of March 7, 2005

(GVBl. I p. 142), last amended by Art. 2 of the Law on

Amendment of the LandtagwahlG and other regulations from

October 30, 2019 (GVBl. p. 310)

Act to Strengthen the Supply of Medicines and Aids (Healing and

Medical Aids Supply Act HHVG) of April 4, 2017; (Federal Law Gazette I

p. 778)

Hessian Teacher Education Act of September 28, 2011 (GVBl.

2011 p. 590)

Regulation for the implementation of the Hessian

Teacher Education Act of September 28, 2011 (GVBl. I p. 615),

last modified by article 6 of the law of March 24, 2015

(GVBl. p. 118)

Hessian law on public safety and order

i. i.e. F. from 14.01.2005 (GVBl. I p. 14, amended by law from

08/23/2018 (GVBl. p. 374)

Hessian surveying and geoinformation law of May 3rd

2018 (GVBl. p. 82)

Hessian forest law of 27 June 2013 (GVBl. p. 458)

Code of Administrative Offenses as amended

Notice of February 19, 1987 (Federal Law Gazette I p. 602), last amended

by law of December 9th, 2019 (Federal Law Gazette I p. 2146) m. W. v. 12/17/2019

Law on identity cards and the electronic

Proof of identity (Personal Identity Card Act) from 18.06. 2009 (BGBl.

I p. 1346)

Broadcasting Contribution State Agreement of 15 December

2010, last modified by the twenty-first

Broadcasting Amendment State Treaty, entered into force on May 25, 2018

The First Book of the Social Code - General Part - (Article I of the

Law of December 11, 1975, Federal Law Gazette I p. 3015), last amended

by Article 28 of the law of December 12, 2019 (Federal Law Gazette I

p. 2652)

The Fifth Book of the Social Code - Statutory

Medical insurance – (Article 1 of the law of December 20

1988, Federal Law Gazette I p. 2477, 2482), last amended by Article 1 of the

Law of December 21, 2019 (Federal Law Gazette I p. 2913)

HGB

HGO

HHVG

HLbG

HLbGDV

HSOG

HVGG

HWaldG

OWiG

PAuswG

RBStV

Social Code I

SGB V

XVI

Register of Legislation

The Tenth Book of the Social Code - Social Administration Procedures

and social data protection, in the version of the notice dated

January 18, 2001 (Federal Law Gazette I p. 130), last amended by Article 9 of the

Law of December 14, 2019 (Federal Law Gazette I p. 2789)

The Twelfth Book of the Social Code - Social Assistance - (Article 1 of the

Law of December 27, 2003, Federal Law Gazette I p. 3022, 3023), last

modified by article 11 of the law of December 14, 2019

(BGBl. I p. 2789)

signature law i. i.e. F. from 16.05.2001 (Federal Law Gazette I p. 876)

Road Traffic Act of 05.03.2003 (Federal Law Gazette I p. 310, corrected

p. 919)

Code of Criminal Procedure in the version published on 7

April 1987 (Federal Law Gazette I p. 1074, 1319), last amended by Article 15

of the law of December 12, 2019 (Federal Law Gazette I p. 2652)

Telecommunications Act

Law of 06/22/2004 (Federal Law Gazette I p. 1190), last amended by

Law of February 6th, 2020 (Federal Law Gazette I p. 146) with W. v. 02/14/2020

Telemedia Act of February 26, 2007 (Federal Law Gazette I p. 179), last amended

by Art. 11 of the law of July 11, 2019 (Federal Law Gazette I p. 1066)

Insurance Contract Act of November 23, 2007 (Federal Law Gazette I p. 2631)

SGB X

SGB XII

SigG

StVG

StPO

TKG

TMG

VVG

XVIII

core items

core items

core items

1. The GDPR requires a uniform approach by the supervisory authorities

all European levels and their close cooperation. Think

The European staff unit acts as a link for communication

at state, federal and international level. An insight into the

Section I 3.2 provides fields of activity. In the field of technology

HBDI on the development of a guideline on the subject of blockchain in a

Expert group of the European Data Protection Board involved

(Section I 14.5). A uniform inner-German concept for metering

of fines according to DS-GVO could from the data protection conference

be developed and published (Section I 15.2 and Appendix I 3.1).

2. Further results of the coordination work to standardize the implementation

This year's report on data protection contains the implementation of the DS-GVO

in Appendix I Materials. Because until reaching portable common

results in a considerable amount of work for my employees

and employees is to be addressed as a further new activity of the HBDI

be advised.

3. The annual review of the Privacy Shield by the European

Data Protection Board (EDPB) is gradually showing progress, e.g. B.

filling the office of ombudsperson. However, still are

leaves many questions unanswered in terms of practical implementation (Section I 3.1).

4. Since the GDPR came into force, the question of whether and to what extent a

Agreement on order processing requires the written form

uncertainties among users. The contribution No. I 4.2 continues with

the different legal views apart. With the adjustment

of the Hessian Data Processing Association Act (DV-VerbundG).

the DS-GVO, the Hessian legislator has a practicable way

found the new specifications regarding order processing

to be effectively implemented by the HZD (Section I 3.1).

5. Inappropriate use of personal data is more common

subject of the complaint. Whether in the application process (Section I 4.4), at

Cadastral information to" third parties (Section I 5.3), when disposing of official

Papers and documents (Section I 7.2) - there was always ignorance of the

Scope of legal basis or organizational reason

for the data breach. Such a one weighs considerably heavier

Violation if the data breach despite knowledge of the prohibition

improper use. This is the so-called employee

terexcess the case. In two cases, private curiosity led to the imposition

a fine (Section I 15.1).

XIX

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection / 2nd activity report on freedom of information

7.

6. In terms of data protection law, a lot is happening in the “school” area. The Hessen project box is closed (Section I 17.1). The Hessian school portal developed himself (Section I 7.3). The use of Office 365 in the educational field remains under review (Section I 7.4). The digitization of the process School transport must be checked in accordance with data protection law (Section I 7.5). The Teacher Education Act requires binding data processing standards (Item I 7.1). Apart from these bullet points, much remains to be done do.

In the health sector, there were very different and partial unusual case constellations that require my intervention ten. So threw the disposal of waste glass with patient data stuck on it problems in a clinic (Section I 9.2). In several cases it came through penetrating water to damage when storing patient documentation (Section I 9.3). In the freely accessible “service mailbox” a doctor's office were based on trust prescriptions and referrals deposited for collection by the affected patients (Section I 9.4). One Pharmacies dealt too freely with prescription pick-up slips (Section I 9.6).

8. The topic of video surveillance is now affecting many areas of life are sufficient. Cases from the nursing service, gastronomy, swimming Badbetrieb, the private property surveillance and also from the municipal area to combat "wild garbage" are listed under No. I 10 shown as an example.

Internet services and websites accessible via the Internet, it is immanent that they can be problematic in terms of data protection law. The use of integrated tools, small services, identification and authentication procedures, encryption of communication,

Chat applications and the integration of interfaces to order

processing and data management are frequent weaknesses (Section 8.3,

13, 14, 15.3). When examining so-called phishing attacks, it was noticed that

that both those in the run-up to defense and those to remedy after

Becoming aware of the measures taken do not meet the requirements of

DS-GVO (Section I 4.3). The new manual 2.0 for the standard

Data protection model supports those responsible, suitable technical

to include organizational measures for data protection (Section I 14.4).

10. The Freedom of Information Act is gradually being

munen, made use of. The law is being put to the test

still before.

9.

XX

Introduction

Introduction

Introduction

Was the 47th activity report on data protection by presenting the

Measures to deal with the upheaval in 2018,

the consolidation of the new

regulations. This resulted in an essentially constant workload

to a shift in the focus of task performance from the

Advice on the handling of complaints. Given the

immense internal organizational changes caused by the data protection reform

Additional expenses (tendering process, redistribution of offices

etc.) and because of the understaffing of the - which has since been remedied

office could not always meet the processing deadlines for complaints

be respected. This has already led to administrative complaints,
the processing of which also tied up capacities. It was further shown that
with the existing human and material resources, the Union law
Planned control activity, especially in the private sector, is not what is required
measure is feasible. Whether even when exhausting all savings
the requirements of Art. 52 Para. 4 DS-GVO can be met,
therefore seems questionable.
The new legal basis for the activity reports was already discussed in
47th activity report of the HBDI. There was also reasoned
which is why it is one of the tasks of the data protection supervisory authorities to
ultimately constitutionally enshrined special position as the supreme federal
or to outline state authorities. Serving since the 35th activity
report general preliminary remarks on the status of data protection and the
data protection law. The current discussion is characterized by the discussion
from positions that have been known for a long time and that already have catchphrase character
assumed, but are only now becoming virulent. To be mentioned here is the
Artificial intelligence (AI) and data sovereignty. This is not the place
for a detailed discussion of the above topics. But just this one
Topics provide an opportunity to deal with informational self-determination as
foundation of our data protection law.
In addition to this, my second activity report shows freedom of information
on that the extension of the right to informational self-determination
in the area of access to information, increasingly among the citizens
and citizens as well as by the public authorities.
This is also the case with the statutory reservation of municipal statutes for
the validity of the freedom of information (§ 81 Para. 1 No. 7 HDSIG) already after

almost a year since the law came into force in some municipalities

already been converted into a corresponding right of access to information.

XXI

The Hessian Commissioner for Data Protection and Freedom of Information

47th activity report on data protection / 1st report on freedom of information

I

First part

48th activity report on data protection

48th activity report on data protection

The Hessian Commissioner for Data Protection and Freedom of Information

introduction

1. Introduction

introduction

The derivation of a data

fundamental right to protection from informational self-determination (BVerfGE

65.1) has often been mentioned, also in my earlier activity reports,

shown. In the 1st activity report on freedom of information, p. 197 ff

once again the dogmatic foundations and the historical development

development of this construct of the Federal Constitutional Court. It can

therefore be assumed to be known that even before the enactment of the Volks-

census judgment the designation and construction of the informational

self-determination had been the subject of controversial discussion in the literature. Whom

is to be attributed to the formation of concepts (cf. Steinmüller, basic questions of the

data protection, report prepared on behalf of the Federal Minister of the

Interior, Bundestag printed paper VI/3826 [1971], p.5 ff.; Christoph Mallmann, data protection in

management and information systems: on the proportionality of

exchange of individual information in the norm-executing administration,
1976), ultimately no longer plays a role. Also the arguments of the time
minority opinions are outdated. The criticism of this opinion, however, is
still up to date. So Otto Mallmann saw the danger that an exaggerated
Paralyze data protection administration and economy (on the status of data
protection discussion, JZ 1973, 274). This is still claimed to this day.
The Federal Constitutional Court did not allow itself to be drawn into this controversy
but instead initiated informational self-determination independently
from its previous case law on the general right of personality.
By linking Art. 1 Para. 1 GG with Art. 2 Para. 1 GG that became
Prohibition of weighing in the sphere of influence of human dignity lifted.
In the core area of human dignity, however, it remained exclusive
Validity of Art. 1 Para.1 GG. In this respect, despite Bull's criticism, I remain
(Informational self-determination - vision or illusion?, p.1) at my
Qualification of informational self-determination as constitutional
fundamental norm. The understanding of data protection law as a balancing
right makes it immune to an application of artificial intelligence.
At the same time, data protection law opens up for the consideration of others
Fundamental rights as the general right of personality to strengthen the
Data protection in the context of considerations. The time for a restriction
of data protection on the protection of personal data has expired.
This has been recognized at EU level. The Hessian legislature
has also drawn the first conclusions from this. The events
on the occasion of the Hessian Data Protection Act coming into force before 50
Years provide an opportunity to see the latest developments in interaction

of data protection and freedom of information, data sovereignty, data economy

and analyze and appreciate data ownership.

4

Legal development and legislation

2. Legal development and legislation

Legal development and legislation

2.1

DS-GVO - An interim assessment

Initial experiences in dealing with the GDPR prompted some

to work out an evaluation right away, but after the only short one so far

period of validity of the DS-GVO could not serve to eliminate any implementation deficits

to uncover, but in truth the revival of claims

purposes that are not enforced in the legislative process

could. However, the task of the HBDI is merely to inform the legislature of new

Point out problems of data protection and advise him as far as possible. One

Correction of the compromises found in the legislative process

The HBSI is not entitled to solve traditional problems.

With the GDPR, an agreement was reached on fundamental issues

can no longer be shaken materially. A continuation of the reform

discussed problem areas would be inadmissible. An evaluation for the

As a result, no norms were enforced in the reporting period.

With regard to legal developments in the federal government, reference is made to the activity report

of the Federal Commissioner for Data Protection and Freedom of Information.

At the European level, the regulation of traffic with non-permanent

sun-related data ahead. In particular, the Regulation (EU)
2018/1807 of the European Parliament and of the Council of 14 November
2018 on a framework for the free movement of non-personal
Data in the European Union (OJ L303, 28.11.2018, pp. 59-68) im
Reporting period validity. Personal data, on the other hand, is treated
on Regulation (EU) 2018/1725 of the European Parliament and
of the Council of October 23, 2018 on the protection of natural persons in the
Processing of personal data by the institutions, bodies
and other bodies of the Union, on the free movement of data and on repeal
of Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC
(OJ 295 of 21.11.2018, pp. 39-98).

2.2 Amendment of the DP Association Act

The Hessian Center for Data Processing (HZD) also processes personal
Name-related data on behalf of Hessian departments. With the addition
of the Data Processing Association Act (DV-Verbundgesetz) is used as a replacement
for the respectively required, individually concluded order contracts

other legal instrument i. s.d. Art. 28 Para.3 DS-GVO created, the one
more effective procedure when placing orders.
The Hessian Center for Data Processing (HZD) is in accordance with Section 1 Paragraph 1
DV-Verbundgesetz the central service provider for the Hessian state association
administration. Legally, this service is classified as order processing i. s.d.
Art. 28 GDPR. This means that for every service that

the HZD as a processor for a department as the responsible party

provides, a contract according to Art. 28 Para. 1 DS-GVO would have to be concluded. This

would have required immense administrative effort. That's why after

looking for a way to meet the requirements of the Basic Regulation

fill, but to reduce the administrative effort.

I have therefore proposed to the state government that the DP Association Act

be expanded in such a way that individual contracts are no longer required.

The state government has taken up this suggestion and

proposal for success submitted to Parliament:

Section 1 (2) DV-VerbundG is worded as follows:

"The Hessian Center for Data Processing can be managed by the state government or

the competent state authority in the case of central or other joint

are commissioned to drive, binding for all agencies involved in the operation of the country

of the procedure for automated data processing as a contractor in the sense

of Art. 28 of Regulation (EU) No. 202016/679 of the European Parliament and of

Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal

personal data, the free movement of data and the repeal of Directive 95/46/

EG (General Data Protection Regulation) (OJ EU No. L 119 S.1, No. L 314 S. 72, 2018 No. L 127

S. 2) and § 57 of the Hessian Data Protection and Freedom of Information Act of 3

May 2018 (GVBl. p. 82), amended by law of September 12, 2018 (GVBl. p. 570),

to perform. To fulfill the tasks provided for in this law

and maintains an operating manual tailored to the respective process, from which

the guarantees, rights and

Obligations of a processor arise."

The Hessian state parliament passed the law on December 11th, 2019 in the second reading

decided unchanged.

It will be my job to regularly check whether the HZD

the operating manual to be kept in accordance with this provision,

which would have to be placed on individual contracts is sufficient.

6

Europe, International

3. Europe, International

Europe, International

3.1

International Data Transfers - 3rd Annual Privacy Review

shield

In the year under review, one HBDI employee, as a member of the Dele-

gation of European supervisory authorities together with the European

Commission and the US Department of Commerce and other US agencies

the practical implementation of between the European Commission and

conditions negotiated by the US government for a transfer of personal

Son-related data from the EU to the USA under the EU-US privacy

Shield checked.

The two reviews of previous years have already been reported on (cf.

46. TB, clause 4.1 and 47. TB, clause 4.2.1). In the present reporting year, the

Checking back in Washington D.C. instead of. The roughly 40-strong delegation

tion from the US was led by Secretary of Commerce Wilbur Ross. The

European delegation was made up of eight representatives of the European

Data protection supervisory authorities and representatives of the European Commission

together.

As with the review last year (47th TB, Section 4.2.1, p. 94 f.)

the test included questions about the practical implementation

of the Privacy Shield. Here the focus was primarily on the process and content of the
(Re)certification process and the mechanisms with which
should be made that the certified company the conditions
also actually fulfill and ensure, for example, that those affected
the rights to which they are entitled under the Privacy Shield
can exercise.
Its report on the third annual Privacy Shield review was published by the
European Data Protection Board (EDPB) at https://edpb.europa.eu/
our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-
report-12112019_en published. Overall, it was found
that the US Department of Commerce and the Federal Trade Commission
We continue to strive to fulfill the commitments made in the EU-US Privacy Shield
implement.
However, this year's report also identifies areas in which
more work is needed: The biggest criticism remains the concern that oversight
about the certified organizations rather limited to formal aspects
could be and there are not enough substantial controls. Another
A point that still requires closer examination is the transfer

Communications from Privacy Shield-certified companies to third parties or in
other third countries. From the EDPB's point of view, it must be ensured here that
that the conditions set out in the Privacy Shield for this purpose are in reality
also be complied with so that the Privacy Shield does not become a loophole
for uncontrolled forwarding of data to non-certified organizations

organizations within the USA or recipients in another third country

can be used without an adequate level of data protection. Finally

should continue to be the area of employee data and recertification

fication process must be kept in mind.

In addition to the practical implementation questions, the question increased again

State access to data that is transferred to the USA under the Privacy Shield

a large room. Here, too, it can be stated

that some conclusions of the European Data Protection Board

from the past year were picked up by the US authorities.

In the meantime, the Office of the Ombudsperson, set up by the EU-US

Privacy Shield was created in the first place. Also is the

Privacy and Civil Liberties Oversight Board now fully staffed again.

The task of this body is to ensure that the US authorities

privacy in their counter-terrorism efforts

and give due consideration to civil liberties.

Overall, it continues to be the case that the field of international data transfers

is fraught with serious uncertainties. As before, there are procedures

pending before the ECJ, the outcome of which will have far-reaching implications for the

Admissibility of data transfers to countries outside the EU will have. In the

first quarter of 2020 is in the case C-311/18 Facebook Ireland and Schrems

(Schrems II) to expect a decision of the ECJ that will influence

international data transfers and the instruments available for this

ments according to Chapter V of the GDPR.

3.2

Europe-wide cooperation with the other European ones

Supervisory authorities under the General Data Protection Regulation

(see also 47th activity report, item 4.2.2)

With the entry into force of the General Data Protection Regulation (GDPR),

as already described in the 47th activity report, numerous innovations for

the cooperation of the supervisory authorities in Germany and Europe

result. Due to the new European legal requirements, in the reporting

period, a significant intensification of cooperation and an increase

to observe the examination effort. Those at the HBDI in the past

The European and International Office that was set up last year acts as a

8th

Europe, International

Link for communication between the HBDI and various

Jobs outside Hesse in Germany, Europe and the world.

Due to the GDPR, the supervisory authorities in cases of cross-border

progressive processing of personal data to a closer

committed to cooperation. Cross-border processing lies

according to Art. 4 No. 23 DS-GVO, if processing within the framework of

Activities of branches of the person responsible or order processing

ters takes place in more than one Member State or if the processing takes place in

Within the scope of the activity of a single branch of a controller

or processor in the EU takes place, but has a significant impact

has or may have on data subjects in more than one Member State.

The so-called one-stop shop

According to the newly introduced concept of the so-called one-stop shop, a

Supervisory authority (usually the supervisory authority of the so-called head office

of the person responsible or processor, Art. 56 Para. 1 DS-GVO)

as the so-called lead supervisory authority, the only contact person for the

Responsible or processor according to Art. 56 Para. 6 DS-GVO,

i.e. H. a company has to opt out because of one and the same data processing

only deal with one supervisory authority. But this means

not that the lead supervisory authority decides alone. Much more

In addition to the lead supervisory authority, all those affected also have an effect

supervisory authorities in the decision-making process. “Affected” are after

Art. 4 No. 22 DS-GVO all supervisory authorities of the member states in whose

Territory of the controller or processor established

is, data subjects have their place of residence or with whom a

complaint was filed. The lead supervisory authority and the

The supervisory authorities concerned work together in the cooperation process

and try to reach a consensus (Article 60 (1) GDPR). After

Examination of the case, the lead supervisory authority submits the data subject

supervisory authorities before a draft decision (Art. 60 para. 3 sentence 2 DS-

GMO), against which the supervisory authorities concerned can object if necessary

(Art. 60 Para. 4 DS-GVO). In case of disagreement

the matter will be referred to the European Data Protection Board (EDPB)

in the consistency procedure according to Art. 63 DS-GVO for a binding decision

submitted.

New forms of cooperation: mutual assistance and joint

Measures

In addition to the general idea of the one-stop shop, the GDPR

with mutual administrative assistance (Art. 61 GDPR) and so-called joint

Measures (Art. 62 DS-GVO) further possibilities of cooperation
before. First experiences have now shown that administrative assistance
request in the course of case processing and for the exchange of information
frequent use is made. For example, the HBDI has 28 in the reporting period
Processing requests for administrative assistance from other European supervisory authorities and
nine requests for administrative assistance to other supervisory authorities.
Overall, the new procedural regulations serve to
progressive data processing as uniform as possible throughout Europe
interpretation and application of the GDPR. In addition, should
communication with the supervisory authorities for both those responsible
and processors as well as for data subjects are simplified.

Example "Binding Corporate Rules"

A clear example of the increased cooperation between supervisory
authorities under the GDPR provides the modified approval procedure
of Binding Corporate Rules (German: binding internal data protection
regulations; in short: BCR). BCR are measures to protect personal
personal data that a group of companies agrees to comply with
or group of companies obliged to collect personal data
within the group of companies in so-called third countries (i.e. countries outside
half of the European Economic Area) to transmit the on and for
do not offer an adequate level of data protection. This way should
a group-wide uniform level of data protection can be established
reflects the high standards of the GDPR.
BCRs are developed in a Europe-wide cooperation process, i. H. from up
checked jointly by the supervisory authorities of several Member States. Here acts
a supervisory authority as lead or so-called BCR lead and coordinate

dines the procedure. One or two more regulators will be

supporting as a so-called co-examiner. In addition, all European

Supervisory authorities in accordance with the consensus set out in Art. 63 GDPR

be included and opportunity for examination and

Receive comment from the BCR.

While under the previous Data Protection Directive still a procedure of

mutual recognition (“Mutual Recognition”) took place, the

EDPB to issue an opinion on the BCR. Only if this is positive

fails, an approval can be given by the BCR Lead, which then for

all other regulators are binding. All European regulators

authorities are thus held more accountable and obliged.

The aim of the process innovation is greater standardization of the

BCR, which also means a new and increased examination effort for the

supervisory authorities.

Over 125 BCR approval applications are currently pending. For

Eight of these BCR procedures is the HBDI Europe-wide as the so-called BCR Lead

in charge. The HBDI took the lead in 17 BCR procedures

tion within Germany and in three procedures at the same time the co-examination

accepted. In addition, companies whose BCR from the HBDI

were still authorized under the previous Privacy Policy, these

update, adapt to the requirements of the DS-GVO and the HBDI

submit for examination.

Case processing in the "IMI system"

In addition to the BCR procedures, the Europe and International

nationales at the HBDI also processes all other procedures that require an
cooperation with other German and European supervisory authorities
make necessary. In order to provide the requested collaboration electronically
enable and facilitate, among other things, the IMI system (inter-
nal Market Information System, German: Internal Market Information System)
deployed. In the reporting period, the HBDI (as of November 29, 2019)
a total of 910 cases registered in IMI in the new form of the European
edit collaboration. In 244 of these cases, the HBDI proved to be
reported "affected" and is therefore involved in the processing. In further
The HBDI took the lead in seven cases. Almost all of these
Cases would either not be available to the HBDI before the GDPR came into force
became aware of or referred directly to the "competent" supervisory authority
been, in whose supervisory area the person responsible or order processing
worker against whom the complaint is directed has its registered office.

Additional novelty: the work is in English

An additional novelty for the work of the HBDI in cases after the
DS-GVO now processed with other supervisory authorities in Europe and
must be voted is the almost exclusive English language
work. This is how correspondence with the European bodies takes place
or other European supervisory authorities in English and the
official language of cooperation procedures and complaints handling
in the IMI system is English. Received at the HBDI in German

Complaints and all communication with the person responsible

or processors must therefore in cases of cross-border processing

works are translated. In addition, as part of the

relatively close legal cooperation with the European supervisory authorities

Deadlines that the authorities have to meet in the performance of their duties.

Conclusion

The DS-GVO therefore not only provides for data processing offices and

fene represents a challenge, but also means for the HBDI and

the other German and European data protection supervisory authorities

a considerable additional effort in terms of communication and organization,

that has to be overcome.

12

cross-section

4. Cross section

cross-section

4.1

Change in the obligation to designate a

Data Protection Officers and the Effects

The obligation to appoint a data protection officer was

by the Second Data Protection Amendment and Implementation Act EU

changed on November 26, 2019.

In addition to the conditions that continue to exist unchanged,

to appoint a data protection officer only when a responsible

usually at least 20 people at all times

engaged in the automated processing of personal data.

The new Section 38 Paragraph 1 Clause 1 BDSG now reads:

§ 38 BDSG

(1) In addition to Article 37(1)(b) and (c) of Regulation (EU) 2016/679

the controller and the processor appoint a data protection officer

or a data protection officer, insofar as they are usually at least 20 people

constantly engaged in the automated processing of personal data.

When determining the number of people are in addition to the (free) employees

full-time and part-time also the managing directors, board members, doctors,

Pharmacists, accountants, insurance intermediaries, etc. to be taken into account.

With the increase in the relevant number of persons in Section 38 (1) sentence 1

BDSG should above all relieve small and medium-sized companies

as well as voluntary associations and practices.

Even if the legislature wants to relieve this, there is no reason to

All clear in data protection law. Because the requirements for data protection and

on IT security also apply to these - regardless of whether a data

must be named or not. A responsible body

or a processor, however, the voluntary designation of a

Data protection officer according to Art. 37 Para. 4 Sentence 1, 1st Alternative DS-

GMO free to meet the data protection requirements to the extent required

implement.

The dismissal of internal data protection officers due to legal

I consider the change (omission of the obligation to name) to be permissible. However

labor or civil law follow-up questions may arise here. How himself

the competent courts position remains to be seen.

Written form requirement for agreements on

order processing

Since the General Data Protection Regulation (GDPR) came into force, I have often been

asked whether, according to the new legal situation, the agreement on

processing requires a written form.

Until May 25, 2018 came as an electronic replacement for the § 11 paragraph 2

sentence 2 BDSG a. F. Mandatory for order data processing contracts

Written form only an electronic document in question, which the name of

Declaring contained and with a qualified electronic signature after

§ 2 No. 3 Act on Framework Conditions for Electronic Signatures (SigG)

was provided (§ 126 a BGB).

Whether the GDPR, which has been in force since May 25, 2018, also includes other electronic

Permits forms for agreements on commissioned data processing

cannot be clearly inferred from the wording of Art. 28 (9). the up

data processing agreement or other legal instrument (e.g. a

legally binding declaration of commitment by the processor).

according to this regulation in writing, which can also be done in an electronic

cal format can be done.

The written form requirement of Art. 28 Para. 9 GDPR is not identical to

the written form according to § 126 BGB. Accordingly, it does not have to be as per Section 126 (1).

BGB mandatory a document signed by the exhibitor

to be created. From the functions of the BGB formal requirement, warning function,

Proof function with identity, authenticity and verification function, information

tion function (Palandt/Ellenberger § 125 No. 2 ff) it only pursues the

latter purpose. That the contracting parties are not protected from ill-considered or

must be protected from hasty commitments is obvious, for on-

Contract processing relationships are not entered into spontaneously, but
are the result of negotiation and selection processes. There are too
hardly expected situations in which the content of the order, the identity
of the contracting parties or the authenticity of the agreements can be proven
would have to. This is likely to apply all the more if the Commission and the
supervisory authorities should have developed standard contractual clauses in the future
(Art. 28 Para. 7 and 8 DS-GVO) and the contracting parties as expected in
usually use these. With the one set out in the GDPR
Written form should ensure that those involved have the opportunity
have permanent and reliable information about the content of the order processing
agreement or a unilateral declaration of commitment.
14
cross-section
The text form also fulfills this permanent information function, as
§ 126b BGB (Palandt, loc. cit.).
The exchange of computer faxes or emails with or without PDF attachments
therefore satisfies the written form requirement of Art. 28 Para. 9 GDPR. The
Processors could also place a contract text on their website
set and the person responsible the declaration of acceptance by clicking
of a box (cf. correspondingly for the submission of a
Declaration of consent EC. 32 GDPR). In this case,
shall be that the person responsible saves and prints out the contract
can. The GDPR does not require that a download actually takes place.
On the other hand, the text form according to § 126 b BGB is different, it is for declarations
only preserved on websites if the recipient prints out the declaration
or stored on a data medium. In the opinion of the

BGH (NJW 2010, 3566, 3567 No. 19) in the case of cancellation instructions on a

Website in the necessary text form if the recipient does not see the page

download or print out.

The systematic consideration of the GDPR also supports the view that

that “electronic format” in Art. 28 Para. 9 does not mean a

BGB electronically signed document can be meant. In Art. 30 Para. 3

DS-GVO there is one for keeping the processing directory

verbatim written form regulation. However, there is no reason why

half a list of processing activities with a qualified

electronic signature should be provided. But there aren't any

Evidence that the Union legislature uses the term "electronic for-

mat” in the two regulations with different content.

In the literature, too, the prevailing view is that

electronic format permitted as written form by Art. 28 Para. 9 DS-GVO

does not require a qualified electronic signature under German law,

but in relation to § 126 b BGB even a somewhat larger

faster text form is meant. (J. Hoffmann in A. Roßnagel, Europäische

General Data Protection Regulation, p. 180 (text form), J. Albrecht / F. Jotzo, Das

new data protection law of the EU, p. 98 (text form), P. Laue et al., The new

Data protection law in operational practice, p. 167, K-U. Plath, BDSG/DS-

BER, Art. 29, para. 17, C. Piltz, The General Data Protection Regulation, K&R,

2016, pp. 709, 713, op.cit. A. Martini in Paal/Pauly, General Data Protection Regulation,

Art. 28, para. 75).

The lower requirements for the written form may

which have a detrimental effect. If the order processing contract z. B.

only justified by corresponding e-mails, it can be at later

Differences about the agreement come to risks of evidence. The GDPR

nevertheless leaves it up to the parties to decide how reliable they are

Document the conclusion and content of the order processing contract

would like.

4.3 Privacy when dealing with phishing incidents

Since the introduction of the obligation to report violations of personal

ment-related data to the supervisory authority are reaching me more and more

Infringement reports that indicate the successful implementation of so-called

target phishing attacks. When examining these incidents

it is often noticeable that both the pre-defense and the remedial

The measures taken after they became known do not meet the requirements

comply with the GDPR.

The aim of so-called phishing attacks is to spy out access

data (e.g. username and password). To achieve this, simulate

the perpetrators create a situation by using technical aids, the users

prompted to reveal their access data. One is initiated

attack z. B. by sending an email message to the user. In

of the e-mail message, the user is informed of a hyperlink with the

request to open it. If the user clicks on the hyperlink, he is

usually led to a website that is known to the user,

pretends to be a trustworthy website operator and the

Possibility to register by entering access data. The

The user is thereby prompted to give his confidential login data at

give. A practical example is the following case: In the reporting

period, I received an infringement report in accordance with Art. 33 GDPR

a person responsible based in Hesse. The subject of the report was

that an employee was persuaded to do so by a phishing attack

was, their access data (user name and password) in a supposed

chen web access to the operationally used Microsoft Office 365 platform

to enter Using this access data, the attackers were able to log into the

Connection access to the stored in the Microsoft Office 365 platform

Provide employees with e-mail accounts. This access was then

used to launch further phishing attacks against the person responsible

to start: The attackers sent phishing emails from the email account

of those affected to other employees of the person responsible.

Some employees followed the phishing message

contained hyperlink and gave in the alleged web access to the

Microsoft Office 365 platform used for driving purposes also their access data

cross-section

a. This made it possible for the attackers to access further operational

Access email accounts and resubmit phishing messages

to ship.

Although the person responsible has been known since the first wave of phishing by the

the attackers knew how to proceed, the described

n phishing attacks several times. The attackers could thus - under

Use of an almost identical attack pattern and despite knowledge of the

those responsible - within a few weeks several parallel ones

Successfully carry out phishing attacks.

Legal Considerations

According to Art. 5 Para. 2 DS-GVO, the person responsible for compliance with the

accountable to the principles contained in Art. 5 Para. 1 DS-GVO. The

Accountability of Art. 5 Para. 2 DS-GVO is through the regulation

of Art. 24 GDPR specified in more detail.

Art. 5 GDPR

(1) Personal data must

a) lawfully, fairly and in a manner that is fair to the data subject

be processed in a comprehensible manner ("lawfulness, processing according to

good faith, transparency");

collected for specified, explicit and legitimate purposes and must not be

further processed in a way that is incompatible with those purposes;

further processing for archiving purposes in the public interest, for

scientific or historical research purposes or for statistical purposes

shall not be considered incompatible with the original purposes in accordance with Article 89(1).

("earmarking");

b)

c) adequate and relevant to the purpose and necessary for the purposes of the processing

be limited to what is necessary ("data minimization");

e)

d) accurate and, where necessary, up to date; they are all on

to take measured measures to ensure that personal data in view

are inaccurate in relation to the purposes of their processing, will be deleted or corrected immediately

become ("accuracy");

be stored in a form that allows the identification of data subjects

only permitted for as long as is necessary for the purposes for which they are processed

is Personal data may be stored longer if the

personal data subject to the implementation of appropriate technical and

organizational measures required by this regulation to protect rights

and freedoms of the data subject are required, exclusively for public

archival purposes of common interest or for scientific and historical purposes

processed for research purposes or for statistical purposes pursuant to Article 89(1).

(“Storage Limitation”);

f)

processed in a manner that ensures appropriate security of personal

related data, including protection against unauthorized or unlawful

moderate processing and against accidental loss, accidental destruction

or accidental damage by appropriate technical and organizational measures

Measures (“Integrity and Confidentiality”);

(2) The person responsible is responsible for compliance with paragraph 1 and must

be able to demonstrate compliance with it (“accountability”).

Art. 24 GDPR

(1) The person responsible shall take into account the type, scope and circumstances

and the purposes of the processing as well as the different probability of occurrence

and severity of the risks to the rights and freedoms of individuals

technical and organizational measures to ensure and provide evidence

to ensure that the processing takes place in accordance with this regulation. 2these

Measures are reviewed and updated as necessary.

(2) Insofar as this is proportionate to the processing activities,

the measures pursuant to paragraph 1 must include the application of suitable data protection

ments by the person responsible.

(...)

Art. 24 DS-GVO contains several undefined legal terms that

are in need of laying. Art. 24 GDPR can support this

the following regulations as well as the associated considerations of the

GDPR.

So for the assessment of the “appropriate technical and organizational

Measures” in advance to ward off phishing attacks and to

Correction after becoming known e.g. B. Art. 32 Para. 1 DS-GVO.

Art. 32 GDPR

(1) Taking into account the state of the art, the implementation costs and the way

the scope, circumstances and purposes of the processing, as well as the different

Likelihood and severity of the risk to the rights and freedoms of natural

Persons responsible, the person responsible and the processor make appropriate technical

and organizational measures to ensure a level of protection appropriate to the risk

guarantee; such measures may include, but are not limited to:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and resilience of the systems

to ensure permanent equipment and services related to the processing;

c) the ability to determine the availability of personal data and access to

recover them quickly in the event of a physical or technical incident;

cross-section

d) a process for regular review, assessment and evaluation of the effectiveness

quality of the technical and organizational measures to ensure the

security of processing.

(2) When assessing the appropriate level of protection, the risks are particularly important

to be taken into account with the processing – in particular through destruction, loss

or alteration, whether accidental or unlawful, or unauthorized disclosure

of or unauthorized access to personal data transmitted,

stored or processed in any other way.

(...)

Art. 32 para. 1 DS-GVO makes it clear that the technical

and organizational measures of the data processing

associated risk (risk-based approach of the GDPR).

will: Require risky processing of personal data

stricter measures than is the case for low-risk processing.

The objective assessment of the risk is therefore imperative in order to determine

to be able to effectively protect the rights and freedoms of individuals

are protect. The person responsible must therefore evaluate the risk and

Depending on the identified risk, appropriate technical and organizational ones

design measures.

The concept of “risk to the rights and freedoms of individuals”

is set out in recitals 75, 76 and 94 sentence 2 of the GDPR

cretized. In addition, the short paper number 18 “Risk for the

Rights and Freedoms of Individuals” by the Conference of Independents

Federal and state data protection supervisory authorities for risk assessment

division can be used (see also 47. TB, materials section 4.7 or

available at https://datenschutz.hessen.de/infothek/kurzpapiere-der-dsk).

The paper first explains the concept of rights and freedoms more natural

Persons. Subsequently, the risk becomes – as the existence of the possibility
the occurrence of an event which itself causes damage (including
unjustified interference with the rights and freedoms of natural people
persons) or to further damage to one or more
natural persons can lead – defined. As part of the risk assessment
it is then recommended to first identify the existing risks,
an assessment of the probability of occurrence and severity of possible
To carry out damage and finally, using the terms “minor
risk, risk and high risk”.
After evaluating the risk associated with the processing activity
sikos is assigned the appropriate technical and organizational
technical measures taking into account the state of the art
implementation costs, the circumstances and purposes of the processing,

therefore the assessment of the question of the appropriate level of protection. For this
Art. 32 Para. 2 DS-GVO explains in more detail that the risks in particular
are taken into account that are associated with the processing, d. H. in particular
special by destruction, loss or alteration, whether accidental
or unlawful or unauthorized disclosure of or access to
to personal data that is transmitted, stored or referred to others
way were processed.
Article 32 (1) lit. a to d GDPR provides for the guarantee of the determined
Protection levels various measures, but not exhaustive
are.

Ability, confidentiality, integrity, availability and resilience

of systems and services in connection with data processing

Ensure duration (see Art. 32 Para. 1 lit. b DS-GVO), includes both in

to be taken in advance to avert dangers as well as after they become known

technical and organizational measures required to remedy the situation.

The provision therefore also comes in connection with the assessment

of phishing attacks.

It follows from Article 32 (1) (d) GDPR that taking technical and

organizational measures is subject to constant further development. The

Regulation is u. a. the idea underlying that framework conditions

of processing activities and thus risks and attack scenarios

change and evolve over time. Also the use of

The term "state of the art" makes it clear that it is merely a matter of

“current” provision, which is regularly evaluated and further developed

needs to be wrapped.

Finally, Art. 32 Para. 4 GDPR makes it clear that the person responsible

also within his own organization all necessary steps and

must undertake to ensure that persons reporting to him who

Have access to personal data, only on the instructions of the

process those responsible. This includes about that in the sovereign area

persons responsible for compliance with data protection law

be obliged to comply with regulations and in a data protection-compliant manner

Be trained in handling personal data. Over and beyond

are to take measures that prevent misuse of personal

prevent data from subordinate persons or the clarification

possible incidents.

cross-section

Detected Defaults

Against the background of these legal considerations, I have in technical

and from an organizational point of view, which became known during my examination

Phishing attacks repeated the following omissions on the part of the responsible

literal stated:

1. Actions to be taken in advance

– Insufficient protection of the authentication process:

In many cases, there is a lack of adequate organizational and technical support

Measures to secure the authentication process. So missing

For example, binding password guidelines or the required password

word complexity is in relation to the personal data processed

data inadequate. In addition, authentication using user

identification and password are usually just one of several alternatives

is. For the Microsoft Office 365 platform, for example, there is also the possibility

to use a 2-factor authentication (i.e. in addition to entering the

User name and password is another "factor" for authentication

authentication of the user).

– Lack of regulations on internet and e-mail use at the workplace:

Those responsible often failed to provide clear and conclusive

to make general regulations for the use of the Internet and e-mail at the workplace.

For example, a tolerated, unregulated private use of the operational

e-mail accounts mean that the clarification of IT security incidents

len - for example by examining a compromised e-mail account

avoidable legal uncertainties. For the evaluation of

risks to the rights and freedoms of data subjects, it is

wise usually required a review of email content and

- Carry out metadata.

– Inadequate technical and organizational preventive measures:

In addition to the core functionality of e-mail communication, common

E-mail platforms supplementary interfaces and functionalities. For this

include in particular those from the field of IT security, e.g. B.

the possibility of integrating virus scanners and spam detection

tion. These should be set up, used and maintained accordingly.

At the same time, functions and services that are not required should be deactivated

become. They may contain vulnerabilities exploited by attackers

could become. In many cases, however, there are no purely technical solutions

sufficient. For example, in a test procedure I found that

that even flagged as potential SPAM emails by the platform

E-mail messages were opened by employees. technical dimensions

measures must therefore be supplemented by organizational measures

in order to develop their full effect. For example, specifications for

Handling of e-mails identified as spam by the system.

– Non-existent emergency plans:

Should third parties succeed in phishing one or more e-mail accounts

to take over, the time factor can have a significant impact on

the further spread, scope and containment of phishing

have attacks. Accordingly, those responsible should have contingency plans

provide them with rapid, comprehensive and effective containment

enable the phishing attack. In doing so, value should not only be placed on the

provision of corresponding documentation, but the

Practicality of control and coordination should also be carried out

emergency drills are reviewed.

– Missing structures and processes for the treatment of injury

reports:

It is often found that within the organizational structure of the

Those responsible have no established processes for reporting and handling

with personal data breaches. So recognize

Employees often do not realize that their behavior violates data protection

may have violated the rights of other people. Also is the act-

People often don't realize that because of the 72-hour period

of Art. 33 Para. 1 Sentence 1 DS-GVO immediately after becoming known

Personal data breach notification to the

supervisory authority has to take place. It is often unclear which people

are to be informed by the person responsible (e.g. data protection and

IT security officer). Processes should therefore be established in advance

the structured and efficient processing of the breach of protection

allow personal data.

– Lack of effectiveness of the training measures taken:

It is true that those responsible are making an effort to

Communicate content relevant to data protection law to employees. Also

can regularly oblige employees to regulations of the

Data protection can be proven (see also brief paper no.

19 of the Conference of the Federal and State Data Protection Commissioners

cross-section

for the “Instruction and obligation of employees to observe the

data protection requirements according to the DS-GVO" (available via

https://datenschutz.hessen.de/infothek/kurzpapiere-der-dsk). With mine

Incidents that have become known to the authority show, however, that an actually

Sustained awareness of data protection issues is often not

is available. This is shown, for example, by the fact that – even if structures and

Processes are in place to handle breach reports – these

are not sufficiently internalized by the employees and therefore not

lead to effective action in terms of data protection.

2. Post-Disclosure Actions

– underestimating the scope:

There is often a strong focus in phishing incidents

to review email communications. At the same time, any

far-reaching effects not considered or only insufficiently considered. In the

The context of the Microsoft Office 365 platform is not taken into account, for example,

that the user ID used for authentication in the e-mail

account usually also for authentication to other services

Platform can be used (e.g. Teams, Sharepoint, OneDrive). It

should therefore be ensured that individual users

Services not required by users are blocked for their user accounts.

Only blocked services do not have to when analyzing phishing incidents

be taken into account. Depending on the design of the authentication pro-

zesses should also be checked as to whether it might be temporary

all user accounts must be blocked in order to be able to

prevent the attack from spreading. Before reactivation must be in the

Usually all passwords are reset.

– Insufficient follow-up:

In addition to the emergency plans, measures should also be taken that

a complete analysis and processing following a phishing

allow attack. These include e.g. B. a data protection-compliant protocol

collation, event-related training measures and the review

the effectiveness of the measures taken as part of the incident. Only

on the basis of an appropriate follow-up and a corresponding

A person responsible can fulfill his obligations arising from the documentation

fully comply with the GDPR.

– Insufficient and late information of data subjects:

According to Art. 34 Para. 1 DS-GVO, data subjects are informed of an infringement

to inform immediately about the protection of personal data,

if these are likely to pose a high risk to the rights and freedoms of the

data subjects and none of the conditions of Art. 34

Para. 3 DS-GVO is fulfilled. This initially sets the identification of those affected

person ahead. Then, for these people, the expected

risk to rights and freedoms and the existence of the conditions

Art. 34 Para. 3 DS-GVO can be determined. When assessing the risks

for the rights and freedoms of the data subjects, I note that

Those responsible for both the number of people affected by a data breach

tend to underestimate both people and the potential risks. Also

many responsible persons fear possible damage to their image, which

development of the information obligation. It is also important to ensure

that those affected are transparent about suitable means of communication and

-ways about the breach of the protection of their personal data

be taught.

Legal consequences of identified omissions in the context of a report

according to Art. 33 GDPR

Basically, it should be noted that omissions that occur within the framework of a

examination according to Art. 33 DS-GVO, further supervisory

official administrative procedures and fines.

4.4

Use of old application documents

Data from a completed application process may be

approval of the applicants concerned for a new selection process

be used. This also applies to applications for the position of 1.

councilor in a municipality.

In a Hessian municipality, the position of the first city councilor was

wrote. The election preparation committee of the municipality could

not agree on a candidate among the applicants. One decided

then to re-advertise the position and a private company

entrusted with handling the application process. This sub

asked for the application documents for the second selection process

the applicant from the first procedure and also received it.

cross-section

This fact was brought to my attention by a member of the city council

meeting that in this procedure a violation of

data protection regulations suspected.

Applicant data is employee data in accordance with Section 23 (8) sentence 2 HDSIG and

may be used by the recruiting body for the duration of the selection

be worked. After completion of the selection process, the data of the

return applicants who have not been considered or destroy them.

Something else can only apply if the applicants expressly

have consented to their use for another application process. In

the case presented was based on the consent of the applicants from the first

Application procedure clearly does not exist.

Section 23 (8) sentence 2 HDSIG

Applicants for employment and persons whose

Employment relationship has ended are considered employees.

These principles also apply to filling the position of the 1st City Council

or 1st deputy, even if the selection decisions are made by a

other body to be met.

The municipality in question, which used the applicant data for the second

drive to the private company had got obvious

also doubts about the legality of this use of data; because she

reported the transfer as shortly after notification by the city councillor

Case according to Art. 33 DS-GVO (data breach) at my authority.

I have asked the municipality to instruct the company commissioned to

to delete the data sent immediately and a deletion certificate

request and send them to me. This has happened.

25

General administration, municipalities

5. General administration, municipalities

General administration, municipalities

5.1

Transmission of anniversary data according to the Federal Registration Act

Municipal newsletters are not included in the press term, therefore

Section 50 (2) of the Federal Registration Act cannot apply here.

Data transmissions of anniversary data to the press according to § 50 paragraph 2

Federal Registration Act (BMG) are always the subject of inquiries

and complaints.

Family name,

first names,

doctoral degree,

§ 50 BMG

(2) Mandate holders, the press or radio demand information from the population register about

Age or marriage anniversaries of residents, the registration authority may provide information about

1.

2.

3.

4. Address as well

5. Date and type of anniversary.

Age anniversaries within the meaning of sentence 1 are the 70th birthday, every fifth additional birth

day and from the 100th birthday every following birthday; Marriage anniversaries are the 50th and

each subsequent marriage anniversary.

The regulation sets out the prerequisites, the framework, clearly and unequivocally

and the addressees of the data transfers, among which the reporting

authority may transmit data. From the wording it follows that

it is not a bid, d. that is, it exists on the part of the addressees

under no circumstances a legal claim to the data transmission. This can

be rejected by the municipality or reduced in scope.

For example, it can be waived that the address of

anniversaries is transmitted.

However, there are misjudgments in connection with the press

expression. This is basically quite broad, so that church

newspapers and advertising papers here addressee of the data from the population register

may be. Communal handouts are exempt from the press term, however

not included. It is therefore not allowed within a municipality

Data for publication i. s.d. § 50 paragraph 2 BMG transmitted

or be passed on.

The possibilities of objection according to § 50 Abs. 5 BMG as well as the related

lich information requirements seem to me against the background of the current

data protection regulations of the DS-GVO are no longer up to date.

§ 50 BMG

(5) The data subject has the right to object to the transmission of their data in accordance with paragraphs 1

to object to 3; then she is at the registration according to § 17 paragraph 1 and once

annually through a customary local announcement.

An active consent to data transmission would be the previous regulation

preferable to active opposition.

5.2

Signature of support for a nomination

To prove that a voter has supported an election proposal, may

only this can be documented at the municipality and not which electoral

suggestion he supported.

A citizen contacted my authority and described the following to me

Facts: He has an election proposal for the upcoming European elections

supported in his home community and therefore applied to the Citizens' Office

give in order to have his right to vote certified. Have in the Citizens' Office

the employee then fills out the entire form for documentation purposes

copied and filed for a supporting signature.

This also resulted in which election proposal the citizen with his

signature had supported.

The electoral regulations provide clear guidelines as to what is to be

legal certification of supporting signatures is to be documented.

§ 32 paragraph 5 sentence 2 EuWO

(5) ²The municipal authority may issue the certificate of electoral

grant right only once; it may not state for which election proposal the

issued certificate is determined.

For the support signatures for the European elections, the form

Annex 14 to the European Elections Regulations is used. This points in a footnote

once again clearly point out that it must not be stated which

election proposal is supported by the signature.

The municipality had clearly with the copy of the entire form

violate the provisions of the European Elections Regulations. I have therefore

demands that she complete the part concerning the party to be supported

removed from their records. This has been confirmed to me.

Since the petitioner had also contacted the Federal Returning Officer,

also from this the removal of the information about the supported party

required, as the community informed me.

5.3

Provision of information on property owners by the

communities

Inquirers at local authorities information about owners of there

occupied plots must be sent to the state office/offices for

soil management.

In the counseling and complaint practice of the last few years,

raises the question of whether a municipality can provide third parties with information about the

may be granted to owners of property located in the municipality.

Property developers, infrastructure development associations, private initiatives or also

Neighbors contact the municipalities of the properties located there

and want information about the property owners. For hedging

The municipalities send me inquiries about the data transmission

the admissibility of this information under data protection law.

All property-related information in Hessen is

property cadastre kept. These at the State Administration for Soil

management-run cadastres are public registers belonging to each person

open for inspection and information. The insight into the names, the

Dates of birth and the addresses of the owners are, however, according to § 16

Paragraph 2 of the Hessian law on public surveying and

Geoinformationswesen (HVGG) only to those persons who have an authorized

have an interest in knowing this data.

Section 16 (1) and (2) HVGG

(1) Any person or body can use the databases of public surveying as

view generally accessible sources and receive information or editions from them.

(2) Deviating from paragraph 1, the inspection of the names, the dates of birth and the

Addresses of the owners as well as relevant information and

Spending only to those persons or entities that have a legitimate interest in knowing

have this data. The same applies to the data of the authorized representatives. The legitimate

interest must be shown. The recipients may only use this data for the purpose

which justifies the legitimate interest and for the fulfillment of which the relevant data

were transmitted. Sentence 3 does not apply to

1. beneficiaries in rem,

2. State authorities and local authorities in fulfillment of their

Tasks,

3. publicly appointed surveyors as well as

Notaries, as far as the personal data in individual cases for the fulfillment

of their tasks are required.

Municipalities usually have within the framework of participation in a

automated retrieval process the possibility of accessing the data from the

Access real estate cadastre. However, this access authorization exists

only for cases where the data to perform municipal tasks

are required (§ 16 Para. 2 Sentence 5 No. 2 HVGG). This will also be in the

corresponding usage contracts between the state administration for

land management and the municipalities.

Answering inquiries from third parties who need the data on the basic

property owners need for their own purposes is not found

within the framework of the fulfillment of municipal tasks. Use the

Municipalities their access authorization for issuing the corresponding

Information to third parties, they transmit personal data without a

data protection basis. On Art. 6 Para.1 Sentence 1 lit. c GDPR in

In connection with § 16 Para. 2 Sentence 1 HVGG, you can use this data transmission

ment because of the obligation to provide information

§ 16 para. 2 sentence 1 HVGG only the state administration obligated to provide information

for soil management is concerned.

As originally responsible for third-party inquiries about the property owners

The state administration for soil management is authorized to do this

requesting the disclosure of information charges to cover the expense of her

for the maintenance of the real estate cadastre arises to compensate.

If the information is provided by the municipality, the Land

desverwaltung für Bodenmanagement unduly charged these fees.

It should also be noted that the necessary competence and experience

the determination of the legitimate interest within the meaning of Section 16 (2) sentence

1 HVGG is only available at the state administration for soil management.

The municipalities must therefore refer the inquirers to the state administration

refer for soil management. The persons entitled to information may

only use the data received from the property owners for a specific purpose

(Section 16 (2) sentence 4 HVGG).

Design of citizen surveys by public authorities

In the past year, the HBDI has repeatedly contacted public bodies

Advice on the design and implementation of surveys. Here acted

These are diverse topics, ranging from a simple citizen survey to

sense of security in one's own region, a midwife survey

went to a survey on the experience of violence in public administration.

The following is intended to provide information on the main contents of the consultation.

Description of the surveys as anonymous - midwife survey

In a large number of surveys, the collecting body

said that the survey was "completely anonymous". here

was unfortunately often disregarded, that precisely the interaction

of the collected data very well leads to a personal reference. At-

A planned survey of midwives should be mentioned playfully.

Based on the present questionnaire, it was no longer possible to say that an "ano-

nymen questioning" can be assumed. That's how it was for me based on

four questions possible to identify a specific person. The mentioned

Questions were as follows:

– Are you a member of a professional association or a specialist society?

(Answer: No or Yes, namely the association to be named)

– In which district or in which urban district are you mainly

actually active?

- In which year were you born?

– Which services that are not remunerated according to § 134a SGB V offer

you at?

The questions were checked using an example and given as an example

answered. The selection was made by a member of the association of freelance midwives

Germany's e. V. (BfHD), which is active in the Schwalm-Eder district and

haft was born in 1960. The association's website gave

ultimately only one person who also offers acupuncture as an additional service

offers. As a result, it was clear that only one person completed the questionnaire

could have filled out accordingly.

Further examples of this kind were conceivable, so that in the entire do-

cuments the concept of anonymity should have been emphasized.

Likewise, the assurance that no conclusions could be drawn was to be withdrawn

individuals are possible. The same applied to the assurance that

the data collection and the measuring instruments used are not suitable

are, individual persons - also not about the indication of characteristics or

Combinations of features – to be able to identify. Rather should after

My House believes that the raised

Data may be personally identifiable under certain circumstances, but that by means of

technical/organizational measures remove the personal reference and

no attempt is made to achieve re-identification. The corresponding

Risk must therefore be clearly and transparently identified.

In addition, it should always be considered in such surveys whether individual

Questions with a high re-identification factor can be deleted

or whether these are actually required for later evaluation. The

Necessity must be justified accordingly.

Alternatively, the possibility should always be considered of larger category

to form rias in which the participating respondent can enter. So are

to form birth cohorts and to indicate roughly rastered time periods

instead of an exact year. This reduces the risk of further disclosures

to achieve a re-identification of the participant.

As a result, the responsible body expressed the wish

to continue to call the survey anonymous.

For this purpose, the specific professional association or the specialist society was no longer

shank queried. The question of obtaining the midwifery exam was also raised

roughly gridded. Likewise, the age was now only in categories

queried. The gender question was also removed. Just at

midwives was to be assumed that there was only a very small

number of male midwives.

Also the question about the average distance of the workplace

from place of residence omitted. In the case of another study concerning the safety

sense of well-being among the population, it was also pointed out that it

makes sense to only include districts that also have a certain population

reach number. In this way, the risk of re-identification

also be minimized.

Special constellation in the survey on violence against employees

in public service in the state of Hesse

I finally had a special constellation during a survey, which

dealt with the experience of violence by public servants. At

the original design of the survey, it was mandatory

ensure that the interviewee also names the authority in which he works

is. This was particularly the case with smaller authorities, such as

my own department, poses a risk of re-identification. If here

also a combination of professional function (e.g. head of department)

General administration, municipalities

and profession (e.g. fully qualified lawyer) is queried is almost 100%

assume identifiability. So I tried again with the

responsible body to clarify whether the specification of the specific authority

is actually required.

The addition that your own authority can only be used by a certain employee

is to be named, in my opinion the remaining residual

risk cannot be completely ruled out. Especially the term "very small authority"

is too vague for this. For the participants is ultimately not apparent from

when to speak of very small units, or whether their own place of it

is affected. In addition, re-identification is also used by authorities with more

than 100 employees, provided that they are named.

The responsible body then informed me again that it was for

the evaluations are fundamentally important that the sectors or

able to classify departments as "professional". But that was it in my opinion

the specification of the office is not decisive, but the occupational field. The

The query should therefore generally be: "Please enter the occupational field (roughly)

in which they work." A corresponding change was finally

taken, so that no longer the specific employer, but merely

the occupational field was queried (education, health and care, justice,

administration or other).

Consulting in the context of online surveys

I also often receive requests for advice on surveys in which the data

should be collected online. In this regard, I was also asked whether

appropriate online surveys with the Survey Monkey program

can carry out and whether this program is seen as a means per se

can be used to conduct anonymous surveys

can be.

For this I shared that Survey Monkey is a widely used tool

for relevant surveys. However, surveys with Survey Monkey are

not automatically anonymous. Here you need at least special settings

be made (see also How-do-I-make-surveys-anonymous

at help.surveymonkey.com). There are also server logs (see data

declaration). The statement that Survey Monkey is used and

the fact that no personal data is requested is not sufficient.

Additional measures are required here.

Incidentally, I agree with the corresponding online survey

encountered that the questionnaire was advertised as anonymous, the

At the same time, participants are informed on the last page that

that the questionnaire can be sent. Here, among other things, one

email address provided. In this context, there was no indication that the

Sending the e-mail means that the submission is no longer anonymous.

The same applies in the event that a postal dispatch stating the

sender takes place.

As a result, I have decided to refrain from future surveys here as well

the incorrect designation as anonymous recommended because the participant

otherwise incorrect and uninformed. Rather it should

it can be said that the answers are personal upon receipt

can be drawn, but by means of technical and organizational measures

the personal reference is removed and anonymization is worked towards.

Final note

My office will be happy to provide advice in the future as well

conduct surveys. In this respect, assistance can always be provided in particular

be given when there are questions of sufficient anonymity

mation, transparency and being informed of the consent. this concerns

in particular the mandatory information to be provided in relevant surveys

Seeing information according to Art. 13 DS-GVO.

6. Police, judiciary, social affairs

Police, judiciary, social affairs

6.1

Controlling my written communication with prisoners

Written communication by my agency with prisoners is subject

not the mail control in Hessian correctional facilities.

I received written communications from prisoners in the Hessian judiciary

zuganstalten, which, among other things, complained that too

the mail I addressed to her only reached her open. the underlying

lying legal regulations in § 33 paragraph 4 Hessian penal system

law state that communication between prisoners and

the bodies mentioned in Section 119 (4) sentence 2 of the Code of Criminal Procedure (StPO).

is not monitored. In Section 119 Paragraph 4 Clause 2 No. 7 StPO, the

Check compliance with data protection regulations in countries

responsible authorities of the federal states are explicitly mentioned.

§ 33 HessStvollzG

(4) Contacts with persons listed in Section 119 (4) sentence 2 of the Criminal Proceedings

Regulation named persons and bodies, as far as

1. in the case of verbal communication, the identity of the contact person is certain,

2. Outgoing letters are addressed to the respective office and the sender

specify as applicable or

3. doubts as to the identity of the sender of incoming letters are not justified

exist or can be resolved by other means than surveillance.

§ 119 StPO

(4) §§ 148, 148a remain unaffected. They apply accordingly to the traffic of the

accused with

7. the Federal Commissioner for Data Protection and Freedom of Information,

the one responsible for monitoring compliance with the regulations on data protection in the

States competent authorities of the states and the supervisory authorities according to § 40 of the

Federal Data Protection Act,

(...)

So unless there is any doubt that I am the sender or also

am the addressee of communication with prisoners, no con-

trolls of written communication take place.

In order to obtain a relevant assessment on the part of the prison staff

easier, I will use the "letter in letter" procedure, i. H. the enveloped

Letter to the convicts or the convict is located

in an envelope addressed to the relevant JVA with a cover letter,

in which again on the sender and a telephone possibility of

contact for verification purposes.

6.2

Deletion of incomplete data records in POLAS-Hessen

Insofar as personal data records on criminal offenses in the police

formation system POLAS-Hessen must also be stored there

information about the outcome of the procedure.

The Hessian police operates on the legal basis of § 20 paragraph 6 of the

Hessian Law on Public Safety and Order (HSOG)

a police information system. With this system, data that

were obtained in connection with the prosecution of criminal offences, for

used to prevent crime.

Section 20 (6) HSOG

(6) The police authorities may, insofar as provisions of the Code of Criminal Procedure or

other legal provisions do not prevent personal data that you

have won within the framework of the prosecution of criminal offences, to avert a danger or

further processing for the preventive fight against criminal offenses. As far as data goes

is about persons who are suspected of having committed a criminal offense are the data

to be deleted as soon as the suspicion ceases.

Specifically, it is the database that is regularly

wise for identity checks, but also for background checks

is queried. If personal data on criminal offenses are stored there

are always related to suspects, accused or convicted

Persons. If data about persons are available there, this is

fundamentally disadvantageous for the person concerned, in particular

especially in connection with background checks. These are

required by law in various areas, for example in connection

menhang with firearms permits, when taking up work in

sensitive areas of public authorities or even with privileged access

to high-risk events.

A special feature of this database is that the data that was

Criminal offenses are recorded at a time and available to the police for retrieval

be made available on which neither the competent State

prosecution nor by a court conclusively on the criminal proceedings

was decided. Only after such a decision by a state

administration or a court, the outcome of the proceedings is determined in accordance with section 482

StPO transmitted to the police and deposited in POLAS-Hessen, as far as they

does not immediately lead to the deletion of the relevant data record.

§ 482 StPO

(1) The public prosecutor informs the police authority that was involved in the matter

your case number with you.

(2) In the cases referred to in subsection 1, it shall inform the police authority of the outcome

of the procedure by notifying the decision formula, the decisive body

and the date and nature of the decision. The sending of the notification to

Federal central register is permissible, if required also the judgment or one with

Reasoned hiring decision.

(3) In proceedings against persons unknown and in traffic offense cases, insofar as they are not under

Sections 142, 315 to Section 315c of the Criminal Code fall, the outcome of the proceedings will be determined

according to paragraph 2 not communicated ex officio.

(4) If a judgment is sent that has been contested, it must be stated who the legal

put in medium.

Therefore, these records as long as there is no notification of the

outcome of the proceedings is deposited, an exit still subject to reservations

significant. This period of time between the time the data was recorded by the police and

a notification of the outcome of the procedure is therefore data protection law

not unproblematic.

After notification of the outcome of the proceedings by the public prosecutor's office

to the police, another problem can arise. prosecutor

scientific proceedings on the basis of § 170 paragraph 2 StPO

Code of Criminal Procedure mean that the investigation does not give enough cause

offer to bring public charges.

§ 170 StPO

(1) If the investigations offer sufficient grounds for bringing a public complaint,

the public prosecutor's office raises them by filing a bill of indictment with the competent

final court.

(2) 1Otherwise the public prosecutor's office discontinues the proceedings. From this she sets the

accused if he has been questioned as such or if an arrest warrant has been issued

was issued against him; the same applies if he has asked for a decision or if

a special interest in the disclosure is evident.

This can be done by the public prosecutor's finding that the suspicion

cleared up or the offense did not take place, be triggered and

then leads in principle to a deletion of the relevant police

database in POLAS-Hessen on this criminal offence. So much for an attitude

according to § 170 paragraph 2 StPO due to lack of suspicion

the police make their own professional decision on the need for further

Storage in POLAS-Hessen, in which regularly a meaningful

Justification for the public prosecutor's office must be included.

My reviews based on complaints in individual cases revealed that

that in the case of individual data sets in POLAS-Hessen on criminal offenses, years

re did not store any data on the outcome of the proceedings after the commission of the crime

were. At the Hessian State Criminal Police Office (HLKA) initiated by me

Individual checks have found that even with the

permanent prosecutors no information on the concerned

process outcomes could be obtained more. In these cases it can

therefore it cannot be ruled out that the

permanent public prosecutor considered the suspicion cleared or

determined that the act did not take place or that it was not a criminal offence.

In my opinion, such a data set should therefore be deleted.

With regard to data storage in POLAS-Hessen, the police have in § 20

Para. 6 HSOG has its own and independent legal basis and may

whose framework in its own technicality about the requirement of the data for

purposes of preventive crime fighting. Because final

Notifications from public prosecutors and courts on the outcome of proceedings

However, these can lead to deletions of the databases

always to be evaluated by the police for data protection reasons

and must therefore always be present.

6.3

How to deal with (anonymous) whistleblowers to the

social administration

Dealing with information from the population to the social administration

opens up a field of tension that does not exist for the official whistleblower

always easy to deal with. It also applies in these case constellations

the data protection principle of direct collection from data subjects

as well as the priority of the requirements of social data protection over those of the

social administration procedure.

I received a complaint from an SGB beneficiary who

As a result of early retirement for a number of years, both benefits

of the statutory pension insurance as well as supplementary benefits

Basic security according to SGB XII obtained through the social welfare office. early May

In 2019 he received a letter from the social welfare office, in which the hiring of the

Benefits according to SGB XII have been announced for the first of the next month.

At the same time, he was asked to provide evidence of a possible

to submit the receipt of social benefits. The reason given was,

that information was available according to which there was a further right to benefits

would drop out. In this letter, the person concerned was given a

behavior shown that the social welfare office had apparently received as a tip and

recognized as fact. The attempts of the affected person from the social welfare office

find out who gave the information failed. The social welfare office

referred to the person concerned on informant protection and a higher

res interest of the whistleblower worthy of protection compared to the interests

of the person concerned to a provision of information. He complained about this

concerned contacted me and asked me for a data protection assessment

or intervention at the social welfare office.

Clarification of the facts

At my request, the social welfare office first took a position on the case.

Thereafter, the person concerned received benefits under the third chapter of the

SGB XII, as indicated by an anonymous letter on April 22, 2019

received by the authority, after which the person concerned on the same day to a

had left for a stay abroad of several months. Because a grant

of benefits after a stay abroad of more than 28 days

§ 41a SGB XII is not permissible, he was then informed by notification

from 02.05.2019 informed that the service from 01.06.2019 to

Evidence of his return would be discontinued.

§ 41a SGB XII

Beneficiaries who stay abroad for more than four weeks without interruption,

received after the end of the fourth week until their proven return to Germany

no benefits.

Since the author of the letter expressly

asked for anonymity, the person concerned was given this information upon request

refused. The anonymous tip was noted by the social welfare office

and, at discretion, reason for writing

been to those affected. The informing person has no information

information about the agency's response.

Since the social administration is required to fulfill its statutory

like support from the population is dependent, would inputs

generally treated confidentially. Exceptions could be, for example

reasonable assumption of malicious slander or allegation

untrue facts exist. In individual cases, there would always be a weighing up

in accordance with § 22 Para. 2 No. 2 HDSIG.

Section 22 (2) HDSIG

(1) 1The transmission of personal data by public bodies to public

Bodies is permitted if they are to fulfill the responsibility of the transmitting body

or the third party to whom the data is transmitted

and the conditions are met that would allow processing in accordance with Section 21.

2The third party to whom the data is transmitted may only process it for the purpose

for the fulfillment of which they are transmitted to him. 3A processing for other purposes is

permitted under the conditions of § 21.

(2) 1The transmission of personal data by public bodies to non-public

Liable positions is permitted if

1.

them to fulfill the tasks for which the transmitting body is responsible

is necessary and the prerequisites for processing according to Section 21

would allow

2. the third party to whom the data is transmitted has a legitimate interest in the

knowledge of the data to be transmitted credibly and the data subject

has no interest worthy of protection in the exclusion of the transmission or

3. it is necessary to assert, exercise or defend legal claims

is

and the third party has committed to the transmitting public body that

To process data only for the purpose for which they were transmitted.

2Processing for other purposes is permitted if a transmission pursuant to sentence 1

would be permissible and the transmitting body has agreed.

The proper weighing of the interests of the parties involved has

present case at the expense of the person concerned.

The representation of the social welfare office raised further questions for me:

– Why did the social welfare office immediately respond to an anonymous tip?

cash caused the suspension of the SGB XII benefits of the person concerned?

– Why, according to the principle of direct survey, was the person concerned

not contacted and confronted with the notice?

– Why was the anonymous tip immediately considered credible and dubious?

freely rated, so that the issuance of a notice of cessation of

performance seemed imperative?

In its second opinion, the social welfare office acknowledged that the

the author of the information letter is personally known to the authority and

considered trustworthy.

The reference was correct, since it could be established that

the person concerned is actually no longer in Germany. the

Knowing the informing person at the social welfare office does not change anything

Result of the balancing of interests, the information about the person is not included

pass on to those affected. The data protection interests of the data subject

nen were not injured. There is no financial disadvantage either

arose because the services had been instructed again in good time.

Legal Assessment

In fact, some parts of the public administration do too

are dependent on information from the population in order to avoid possible grievances,

to be able to investigate legal violations or the like. This will not

promoted or encouraged wanton denunciation, any

Submit defamation and the like to the authorities.

If such an unsolicited notice is received by an authority, this has

at its best discretion and within the scope of its official investigative or

investigative principle to check whether the information has a credible

attaches truth value to liability and, if so, to pursue it.

There are no data protection objections to this.

In principle, however, social service providers always have the data protection

legal principle of direct collection, § 37 S. 3 SGB I and § 67a Para. 2 S. 1

SGB X, must be observed.

§ 37 sentence 3 SGB I

The second chapter of the tenth book takes precedence over the first chapter as far as the

Determination of the facts extends to social data.

§ 67a paragraph 2 sentence 1 SGB X

(2) 1 Social data must be collected from the data subject.

In the present case, the social authorities were able to

However, do not contact tenen directly, as the person concerned is after

local conviction already stayed abroad. To an overpayment of

benefits or improper payment of social benefits

which actually no longer exists to avoid in good time saw

the social welfare office is forced to issue the decision on the cessation of social

to waive benefits from the following month. About the rights of the person concerned

nevertheless as far as possible, he has been given the opportunity

to prove his (timely) return to Germany or in this

his further, continuous entitlement to benefits

according to SGB XII. Accordingly, the performance

resumed without financial disadvantage.

Due to this special constellation, I was able in the present case -

especially because of the overlapping processes – one

clear violation of social data protection regulations

not find the social welfare office.

However, I pointed out to the social welfare office that non-compliance

of the direct collection requirement can and may only be an exceptional case.

Those affected must be given the opportunity to (also officially as

credibly classified) allegations and indications against her person

better. The issuance of a notice solely with reference to a "credible"

As a rule, the truthfulness of a tip cannot be accepted.

6.4

New Federal Participation Act: Social data protection in the

cross-institutional rehabilitation process

As part of the project "Data protection in cross-carrier rehabilitation

Process" at the Federal Working Group for Rehabilitation (BAR) in

Frankfurt am Main, as a representative of the federal states, I was a member of a

Project group to develop a work aid for the above Theme. Legal

The background to the endeavor for such a work aid was the new

structuring of SGB IX as part of the Federal Participation Act (BTHG). The

The project was completed in summer 2019 with good results.

In the summer of 2018, the BAR chaired the data protection conference

renz to the data protection supervisory authorities with the wish for a

project planned there to create a work aid with the project title

"Data protection in the cross-carrier rehabilitation process" at least one

Participant from the group of state data protection supervisory authorities

to recruit and win permanent and active members. This

the BAR, for understandable reasons, made sense to add to that

Representative of the Federal Data Protection Commissioner (BfDI) as the responsible data

safety supervisory authority also a participant from the circle of

To be able to win state data protection supervisory authorities, since the BTHG

/ SGB IX-new will have a broad effect. I like this job

taken over and subsequently acted as a mutually authorized representative

the state data protection officer as a member of the above project group

attended the meetings in 2019.

In addition to the BfDI, HBDI and representatives of the BAR, other participants/

Members of this project group representatives of:

- Federal Ministry of Labour and Social Affairs
– Federal Ministry of Health
- German Federal Pension Insurance
– German statutory accident insurance (DGUV)
- Federal Employment Agency
– National Association of Statutory Health Insurance Funds
– Social insurance for agriculture, forestry and horticulture
– for the federal states: Ministry of Labour, Health and Social Affairs NRW
- for the integration offices: Center for Family and Social Affairs Bavaria

On a total of six appointments at the BAR in Frankfurt am Main

the project topic is worked up and worked out in all-day working sessions.

In the last meeting of the project group, the working aid

"Data protection in the cross-carrier rehabilitation process" to be adopted.

This work aid is of course a compromise of the most diverse

Concerns and (technical) requirements of the participating institutions. So

BfDI and HBDI were also able to exert an influence in a positive sense

and get an appropriate result.

The work aid is available for download on the BAR website

and can also be obtained from there as a bound brochure.

From winter 2019, the BAR is planning a follow-on or

this in-depth follow-up project "Data protection in rehabilitation" is planned.

The same group of institutions and participants will probably gather here

bring it back and develop a document that will be useful in practice.

7. Schools, colleges, statistics

Schools, universities, statistics

7.1

The teacher training law requires binding

data processing standards

The Hessian Teacher Training Act regulates the training of teachers

graduates in preparatory service or traineeship. So far are in

this law norms regarding the processing of personal data

Insufficient student data available. Almost two years after

entry into force of the General Data Protection Regulation, it is time for clear

to create lungs.

The Hessian Teacher Training Act (HLbG, GVBl. I 2011 p. 590) regulates the

Training and examination of trainee teachers

tern. The law contains a wide range of norms regarding study and

of internships, the first and second state examination or the teaching qualification

and the authority to teach. More information on this and regulations

with regard to pedagogical training, the Ordinance on the Implementation

implementation of the Hessian Teacher Training Act (HLbGDV of 09/28/2011)

contain. The pedagogical training takes place in the subjects studied

at ten study seminars at 17 locations and at training schools,

which are regionally assigned to the study seminars.

Unfortunately, both legal norms contain hardly any regulations on handling and

the processing of personal data of the trainee teachers

and student teachers. However this is precisely with regard to that

General Data Protection Regulation has been in force for almost two years,

a situation that urgently needs to be changed. Finally, currently

personal data from well over 1,000 prospective teachers

collected and processed.

As part of the development of standards, I think it is urgently

ten to observe the so-called principle of homogeneity. Data processing only

Wanting rules in a regulation does not meet these requirements.

Rather, the content, purpose and extent must be determined in the law.

Is provided by law that an authorization further delegated

can be transferred, the authorization of a legal

basis. This is usually a legal regulation.

Just as in the Hessian school law, basic provisions for

processing of personal data of students,

Teachers and parents are included and the specific design in the

Regulation on the processing of personal data in schools takes place,

are basic data processing standards in the Teacher Education Act

record. The concrete design is then in the already existing

to implement the Ordinance on the Implementation of the Teacher Education Act.

7.2

Human error and insufficient organizational

administrative actions carried out at the institute for

Vocational Training (IBB) at the University of Kassel to a serious extent

breach of data protection law.

The IBB of the University of Kassel uses for the disposal of papers and

are stored in lockable containers containing personal data

external service provider provides. The containers will be inside

agreed periods and the personal documents

destroyed by the disposal company in accordance with data protection regulations. To prevent accidental

to be able to get thrown documents out again, were in the institute

kept several keys for the containers. A new employee

in the secretariat took advantage of this opportunity. What was fatal, however, was that she

did not close the opened container again. Rather, the container

placed in a different place, namely on a corridor within the

Institute area in which regular public traffic prevailed. No

It is therefore surprising that within a short time someone lost interest in it

effective container and found that it was not locked.

The container contained personal data, e.g. from teaching

aspiring teachers. My office became anonymous

informed about the data breach. Attached to the email were a large number

of image files showing the quality of the unprotected and actually used

Documents intended for destruction showed. It was u. a. around

– Lists with names, school, matriculation number and private e-mail addresses

s and telephone numbers,

- Confirmation of receipt of a leaflet on the implementation of the

– Infection Protection Act with name and date of birth,

– List of participants in a course in the winter semester 2016/17,

– Certificate of internship of a teacher candidate,

– Table of contents for the report with personal notes on a

Pupils,

– Written statement on a term paper, etc.

Measures taken by the University of Kassel

After I pointed out the data breach to the university management, they reacted

quickly and also contacted the university's data protection officer

a. The container was immediately closed again and sent to his

original location.

When processing the breakdown, it soon became clear that the contract

for order processing (Art. 28 DS-GVO) as well as the internal organization

the key authorization and key custody of a repair

needed. As it turned out, it wasn't clear how many keys, anyway

were in circulation, where they are kept and who has access to them-

te. Consequently, there was also a lack of assignment of responsibility for the

single key. In the future there will only be one key, the

kept and managed in a safe place. The employees

and employees have been sensitized accordingly. Such regulations

belong to the technical and organizational security measures

ment that every person responsible for data processing must meet in order to

an adequate level of protection for the data it processes

guarantee (Article 32 GDPR).

In this case it's actually a pretty simple thing to sort out.

Nevertheless, it took this data breach to establish a procedure

that should have been there from the start. A report

according to Art. 33 DS-GVO was not required because of the university administration

the data protection violation only became known through my information and

she then immediately implemented all necessary measures.

7.3

The Hessian school portal is developing

Already in 2016, the education ministers of the federal states with their

common strategy "education in the digital world" on clear goals and

Time horizons regarding the use of so-called learning management

systems (LMS) or learning platforms. In Hesse there will be one

Uniform learning platform within the framework of the so-called school portal

implemented.

The advantages of digital platforms

The advantages are apparent. School is no longer just the place where

by teachers e.g. B. Assignments for students or

Teaching and learning materials are made available. The physical

Presence of all actors is partly dispensable because the data is in a cloud

transported to which those affected have access. Also

such systems can be used for communication and thus

extend the functionality of such platforms. Finally is also

School organization possible in this way because room plans or hourly

Plan changes are communicated via the medium. A row of

federal states has opted for state-wide digital platforms.

In North Rhine-Westphalia z. B. this was "logineo", in Baden-Württemberg one

Platform called "ella". Lower Saxony and Bavaria also use central

solutions or working on them. Development is also happening in Hesse

progress towards a central portal solution.

The Hessian school portal is being built step by step

For years, employees of the Hessian Teachers' Academy have been working with

support and according to the specifications of the responsible digitization department

in the Hessian Ministry of Education on the development of a portal that

characterized in particular by the fact that only "freeware" software

goods are used. Binding to specific products of certain

manufacturer is eliminated. Seconded teachers with practical knowledge from the

Everyday school life develop both applications for the pedagogical area

as well as school organization. For example, the functional

quality of an electronic grade book for teachers in the so-called LANiS

Disposal. The name is an acronym and stands for Easy Administration

of networks in schools”). This means access and applications

organized for students and teachers.

In the meantime, a whole range of applications have been added

is available to all participants in a closed platform. Approximately

A quarter of all Hessian schools are currently registered on the school portal

det, about 250 of these schools use the applications extensively.

Other modules such as B. storage options for teaching material

in planning or partially already implemented.

Aspects of data protection law when used by schools

As a rule, within the scope of the use of digital (learning) platforms

personal data of teachers and students

processed. That starts with setting up an account and continues

e.g. B. continue with the communication. Also the assignment of housework and

their evaluation is part of their functionality.

Schools are not prohibited from using digital learning materials. You need to

However, guarantee participation and ensure the security of data processing

care. Finally, the school or the school management as

Responsible within the meaning of Art. 24 DS-GVO for the data protection compliant

Processing of the personal data of teachers and students

students have a duty. Data protection requirements for

the use of e.g. B. Learning platforms have the data protection officers

from the federal and state governments in an "orientation guide for learning platforms" (https://

datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Orientationshil-

fe%20online learning platform%20in%20school lessons%20-%20stand%20

04-2018.pdf). Providers are responsible for implementing these requirements

of platforms sometimes face major challenges. This applies equally

Measures for schools using the privacy and data protection tools

Data security provided by the provider should be adequately circumvented. je

a process is more complex and the large number of functionalities

becomes apparent, the greater the risk that in the context of the application

fundamental data protection issues are ignored.

Data protection requirements for the Hessian school portal

A comprehensive data protection assessment of the Hessian school

I haven't been able to do this so far, even if it was in the year under review

a series of contacts and exchanges with the responsible representatives

the teachers' academy. Nevertheless, I have compared to the Hessian

Ministers of Education believe that data protection regulations are fundamentally positive

pressure communicated by the platform. At the same time I announced that

only on the basis of comprehensive documentation a qualified

assessment can be made by me.

The core element of the portal is the central identity management. This

must be in line with the favored “single sign-on” solution

of access meet high standards. Single sign-on makes sense to

not to make access to the portal disproportionately complex.

But also access permissions, logging or authentication

procedures are the focus of data protection considerations. Not

last are lists of processing activities according to Art. 30 DS-GVO

required, which are currently being prepared by the teacher academy.

If those involved succeed in overcoming these challenges,

a general use of the portal as a Hessen-wide offer

the schools nothing in the way.

7.4

Technical investigations into data protection-compliant use

of Office 365 in the pedagogical area of Hessian schools

For years I have been dealing with the topic of a data protection compliant

Use of the Office 365 application in schools. Also in

Since the beginning of the 20th century, I have purchased certain Office 365 product lines at great expense

checked. The provisional result of these examinations were two opinions

with the aim, based on sustainable knowledge, to a final

to be able to come to the evaluation. The technical inspections carried out so far,

especially at local schools, will be continued.

With the nationwide digital pact for mo-

modernization of the Hessian schools is the use of the application

Microsoft Office 365 in the Microsoft Education license model is stronger for me

been requested. This product line became progressive within the year

- also technically - for use at Hessian schools in the pedagogical

area checked. Two statements from my House led to direct

Discussions with the manufacturer Microsoft.

An increased need for testing on the one hand and discussions directly with

Microsoft, on the other hand, needed it because in the year under review, individual

School authorities (regardless of open data protection issues)

services connected to Microsoft Office 365 massively into school

rolled out landscape. For those responsible, such as school administrations, it was almost

impossible to assess which license model will cover their needs and

at the same time represents a data protection compliant solution. In particular, will

making such decision-making difficult for several reasons, because

not just applications and services from the Microsoft Education product line

Tobe offered.

From a technical point of view, the following apply to the use of Microsoft Office 365

data protection requirements for data protection-compliant

processing of personal data resulting from art. 5, 25, 28, 32 and

46 DS-GVO derive or result from decisions of the European

Data Protection Board, Investigations by the European Data Protection

Commissioners, the IT Planning Council or the Conference of Independents

federal and state data protection officers.

Regarding the use of Office 365 based on Microsoft Education in the

pedagogical area of Hessian schools, the role of the

provider Microsoft in relation to other data centers or IT service

achieve discussed.

Schools, universities, statistics

7.5

Digitization of the process of student transport

The school board of the Groß-Gerau district is planning the redesign and

Digitization of the process of student transport. According to § 161 of the

According to the Hessian school law, the school authorities are under certain conditions

obligated to reimburse parents for costs. The circle

Groß-Gerau is one of the first facilities nationwide, in the sense

of the Online Access Act to create a digital process that

from the application to the reimbursement of money the use of

to make paper obsolete.

The Online Access Act (OZG) obliges the federal and state governments to

2022 their administrative services also electronically via administrative portals

to offer. The Groß-Gerau district is now one of the first in Germany

School authorities (the city of Munich has offered such a service since mid-2018),

of all services related to school transport to the parents in one

to provide online procedures.

In this context, data protection issues arise

genes regarding the security of data transmission, access protection

or data storage. In particular, it must be assessed whether the

required access to the teacher and student database (LUSD) to

to be able to check the information about the students,

legally possible. In the LUSD, a common procedure

of the schools and the Hessian Ministry of Education are among others

the master data of the students are stored, e.g. B. name,

address or date of birth. With an automated comparison with the

Data from the LUSD raises the question of whether an inequality is found

of the requested data with those of the LUSD, e.g. B. if there another

Address is given, these deviating data to the school board

may be transmitted.

The procedure, which is currently being modeled by those responsible, requires

yet a closer look on the basis of comprehensible

Information.

The approach seems interesting at the moment and under data

to be realizable from the point of view of protection law. I will therefore

continue to support the process.

7.6

The 2021 census is approaching

In 2021 there will again be a register-based system in Germany and throughout the EU

Census - a population, building and housing census - take place. With

the census in Germany should include the official number of inhabitants and a

Series of data on population, employment and housing situation

be collected. The last census will then be ten years ago.

Legal basis and intended course of action

The implementation of the 2021 census and in particular which registers

or data sources are used for this purpose is regulated by federal law

for carrying out the census in 2021 (2021 census law) of 26.

Nov 2019

At the same time, the Hessian legislature passed a "Hessian implementation law

to the 2021 census law", which will set up the local

common collection points in the districts, the urban districts and

the special status cities and the requirements for their establishment and

management and the individual tasks to be performed.

As of May 9, 2011, a register-based

census carried out. The 2021 census will again be register-based

be elevation.

One of the results obtained from the official statistics in the 2011 census

knowledge was the fact that the registers used were partly not

meet the required quality standards. The consequence of this

was the construction of an address-related control register in which
all addresses with living space and information on the building and living
are deposited with the owners. The statisticians received the data from
Official Real Estate Cadastre Information System (ALKIS) from the
deregisters from the registration authorities and survey data from the Federal Office
for Cartography and Geodesy (BKG).
On the basis of this data, a total survey of the building and
sion owner (GWZ) carried out. A household survey is also carried out
based on a random sample of around ten percent. In addition, in
A repeat survey is planned as part of quality assurance.
Data processing takes place in various IT systems and specialist departments
turns. As part of the "Online First" strategy of official statistics
should the answers from the census of buildings and apartments by the
Those required to provide information are primarily submitted online. For this purpose, as in
In 2011, an online portal was set up. The data will be within a

Schools, universities, statistics
Specialist application processed. This also applies to the household sample
be. This takes place via a reference database (the control register).
Comparison and plausibility check of the databases.
In the technical processes of data processing, the
tistic Federal Office or its processor, the information
Federal Technology Center (ITZBund) is of central importance. different
than in the 2011 census, the countries process the data of their respective countries
area of responsibility themselves, but are involved in the procedures
ITZBund affiliated through an administrative agreement. The central

Data storage on federal information systems and the reduction

the powers of the countries to "their" data in the form of "accesses" or

"Retrieval" represents a special feature - also in terms of data protection law - for

for which there is no example so far.

Data protection issues

From the computer-assisted construction described, which is in this form for the first time

is used, questions arise as to who is responsible

honesty. For the central IT infrastructure and the security of the data

According to Art. 24 DS-GVO, the statistical department is responsible for processing

federal office. This also applies to the implementation of the necessary measures

for data security i. S.v. Art. 32 GDPR. For access or retrieval

are the statistical offices of the federal states or the survey offices

responsible.

The need for protection of the personal registration data is classified as "very high".

evaluate. On the one hand, this is due to the fact that in the population registers

also contains data of persons for whom a so-called "blocking of information"

is applicable. This is e.g. B. to vulnerable people such. B. people,

who could make the threat of danger to life and limb credible,

or persons in a witness protection program. For the

others would be able to identify people by name and date of birth

to identify and determine their address. From the according to § 5 of the

Census Act to transmit personal data to official statistics

This results in the very high need for protection. Correspondingly understandable

and the data processing processes must be designed securely. the to

information required for the evaluation under data protection law should be given

supervisory authorities for data protection, including my authority, promptly

to provide.

53

Order processing by the statistical offices of the federal states

Except for the states of North Rhine-Westphalia, Lower Saxony, Baden-Württemberg

berg and Bavaria, the statistical offices of the federal states have formed a network

merged. Within the network, central processes are

tendered and implemented together. Finally, the award of the

Services Printing of the survey papers of the building and housing

counting and the telephone hotline. Unlike 2011, this is intended

Hessian Statistical Office, no own call center for the census

2021, but to commission an external company to do so.

This also raises data protection issues. So it requires z. B.

the clarification of whether and to what extent the external forces with a

Discuss content-related questions of the sheet that are subject to future requirements and for this

may fill out. What kind of access and write permissions would be

required for this? Should such sovereign measures be taken by a

external third parties are executed at all?

These and many other questions will be addressed in the coming reporting year

require further clarification. A trusting cooperation is

work with the Hessian Statistical Office on an important prerequisite

setting. The regular contacts that have taken place since the beginning of the year have been

so far a good basis for the process surrounding the 2021 census

to be able to provide appropriate support in accordance with data protection law. The supervisory

The federal and state governments are required to do this in the coming years

Large-scale data processing project census 2021 critical in terms of data protection

and constructively in the interest of the citizens.

54

traffic, services of general interest

8. Traffic, services of general interest

traffic, services of general interest

8.1

Copies of ID and driver's license for test drives

prospective buyers

The collection of ID and driving license data is for test drives by

prospective buyers required. Due to the principle of data mini-

However, you should refrain from making corresponding copies for this purpose

become.

During the reporting period, I received a complaint against a car dealership that

to carry out test drives, copies of identity cards and

prepared the prospective buyer's driver's license.

Presentation of driver's license and verification of identity

There is no doubt that presenting a valid driving license as well as

the specification of personal details by the car dealership when carrying out a

Test drive due to the due diligence incumbent on the dealer and

criminal law provisions may be required.

As the owner of the vehicle, the car dealership must ensure that

a vehicle is only driven by persons who have the necessary knowledge to do so

be able to show a driver's license. If the retailer fails to carry out this check,

this can not only result in criminal consequences for him according to § 21 paragraph 1

No. 2 Road Traffic Act (StVG), but also insurance law

have an impact. Are caused by the test drive, for example

Damage to the insured vehicle, the insurer can take over

refuse performance if the holder contravenes D 1.1.3 of the General

Conditions for motor vehicle insurance (AKP) has approved that

a driver without a license driving a vehicle on public roads

paths and squares.

But also the recording of the personal details on the basis of the identity card

serves to secure insured assets and thus the

Fulfillment of the insurance law due diligence obligations.

The transfer of the vehicle to a prospective buyer can namely

then a grossly negligent facilitation of theft according to § 81 des

Insurance Contract Act (VVG) if the dealer as

Policyholder Measures to establish the identity of the customer

and makes the vehicle available to him (see OLG Frankfurt am

Main, judgment of February 20, 2002 - 7 U 54/01). In these cases, the insurance

55

tion to take over the damage caused by the theft of the vehicle

Refuse or reduce the financial loss because the insured event is gross

was caused negligently.

The insurance industry requires the template for identity verification

an identity card or passport. The identity card and the

Passport represent official documents, with which in Germany the identity

of the holder can be established without a doubt. It contains a multitude

of security features with which the authenticity can be checked.

Preparation of a copy of an identity card

According to Section 20, Paragraph 2 of the Personal Identity Card Act (PAuswG), a personal

card by another person only with the consent of the card holder

be photographed if personal data is collected with the copy

or be processed. The copy must be permanently recognizable as such

be. Otherwise, the provisions of general data protection law apply

apply.

Section 20 (2) PauswG

(2) The card may only be used by the card holder or by other persons with their consent

of the ID card holder are photographed in such a way that the photograph is clear and

is permanently recognizable as a copy. Persons other than the ID card holder may use the

Do not pass copy on to third parties. Personal data are obtained through photocopying

collected or processed on the identity card, the data-collecting or -processing

authorized body can only do this with the consent of the ID card holder. The regulations of

general data protection law on the collection and use of personal data

Data remains untouched.

With the decree of March 29, 2011, the Federal Ministry of the Interior has

further specifications relevant to data protection law, on which

I establish the permissibility of copying an identity card. Thereafter

the card holder must access the possibility of blacking out the for the

Identification not required data are pointed out. Furthermore, the

Destroy the copy immediately by the recipient as soon as the pursued

purpose has been achieved.

In view of this regulation, I made the relevant dealership on it

aware that an effective consent under data protection law, a

to make a copy, can only exist if those affected give their consent

willingly and are sufficiently informed about the data processing.

Voluntariness is to be assumed if those affected have a serious choice,

traffic, services of general interest

such as B. between the copy of the ID or the written acceptance

of the necessary identification data in a form.

At this point, the dealership used one from its association to

Form provided that offered neither the option, instead of the

Paste a copy of the data in writing, add data protection information

Art. 13 DS-GVO contained. As an alternative to consenting to the copying of the

ID was so only the waiver of the test drive. Because this form

as a sample from a larger one responsible for the motor vehicle trade

association was created, I contacted them and obtained one

appropriate revision.

In the meantime, the association has published a new form in which between

the copy of the driver's license and the written acceptance of the driver's license

Scheindaten can be selected. Furthermore, only

the ID card number, the date of issue and the issuing authority

from the identity card or passport for identification in writing

queried. The form also contains a sample data protection information

mation according to Art. 13 DS-GVO, which is carried out by the respective user (car dealership)

is to be adjusted accordingly.

In terms of data minimization and data economy, the

Association also generally recommended in an accompanying letter that the date

to carry out the survey by means of written acceptance and from the

refrain from making copies. If a car dealership nevertheless decides to

to make copies of ID cards available to prospective buyers,

this is only possible with a voluntary data protection consent and

compliance with legal regulations.

The affected dealership assured that the new form would be included in the future

Carrying out a test drive by prospective buyers to use and

just enter the required data in the form.

8.2

Data processing of wireless smoke alarm devices

For the use of wireless smoke alarm devices, see data protection law

Regulations apply because the false alarms of the smoke alarm device

a certain behavior of the residents can be inferred and thus included

Personal reference can be established.

Due to a large number of complaints, I contacted myself during the reporting period

engaged in the data processing of wireless smoke alarm devices.

Since June 2005, inhabited real estate in Hesse has had to be

No. 1 Hessian Building Code (HBO) with smoke alarms in all sleeping

clear, escape and rescue routes must be equipped.

Section 14 Fire Protection

(1) Facilities are to be arranged, erected, modified and maintained in such a way that

Development of a fire and the spread of fire and smoke (fire spread)

is prevented and, in the event of a fire, the rescue of people and animals as well as effective

same extinguishing work is possible.

(2) Need to protect sleeping people

1.

in apartments the bedrooms and children's rooms as well as corridors, via the escape routes

lead from lounges,

in other usage units, the common rooms in which

people sleep,

2.

each have at least one smoke alarm. The smoke alarms have to be like this

installed or attached and operated so that fire smoke is detected early and

is reported. Ensuring operational readiness is the responsibility

1.

2.

unless the owners have passed this obligation

taken. Existing usage units according to sentence 1 no. 2 are until January 1, 2020

equip accordingly.

in apartments according to sentence 1 no. 1 the direct owners,

in usage units according to sentence 1 no. 2 the operators,

In the planning, installation, operation and repair of

Smoke detectors are also the requirements of the DIN application standard

14676 to be observed. For example, DIN 14676 stipulates that the

Smoke alarm in the middle of the room with a minimum distance of 50 cm

attached to a wall or to furnishings on the ceiling

are. The wireless smoke alarm device must set off an alarm if it

dismantled or the 50 cm distance is not observed. The recommended one

inspection cycle is independent of the type of smoke

alarm 12 months.

The unrestricted insurance protection of the building usually depends

of the proof of the proper maintenance of the smoke alarm device

according to the relevant DIN regulations.

The owners of rented accommodation may be subject to the obligation to

Ensure operational readiness according to § 14 HBO. Of the

Possibility of takeover often make the owners for protection

use of their rented property. To fulfill this obligation

they are increasingly opting for smoke alarm devices with radio modules.

These offer the possibility of complete remote inspection while in action

traffic, services of general interest

of radio technology. Entering the apartment is not necessary. The

Entering the stairwell is sufficient to collect the data.

So those who were not informed about the use of radio technology were surprised

tenants, if they have received a letter from the landlord with the

demand that the chimney dismantled during the renovation work

to reinstall the alarm. That's why many complained

affected tenants with me.

I took these complaints as an opportunity to explain how it works

of wireless smoke alarm devices from a service provider based in Hesse

to look at more closely. This service provider is used by the landlords / house

administrations with installation, inspection, repair and documentation

the smoke alarm activated. The type of smoke alarm determines

always the landlord. He can also opt for the radio-based

technology (according to the Federal Court of Justice in its judgment of 06/17/2015

(VIII ZR 216/14)).

During my data protection check, I found that the radio

smoke detector a serial number (series) and ID (device number)

own. These are assigned to the respective residential unit and room

arranges. Through the remote inspections, in addition to the technical values

(Battery charge status, technical malfunctions of the smoke sensors or the

warning signal, etc.) also the behavior of the residents - the dismantling or

adjusting the smoke alarm device – detected using radio technology

become. It is therefore personal data of the residents

within the meaning of Art. 4 No. 1 DS-GVO.

In the automated processing of personal data, the

Provisions of the General Data Protection Regulation and the Federal Data Protection

to observe the law. The data protection basis for the collection

of personal data is Art. 6 Para. 1 S. 1 lit. c GDPR, § 14

HBO in connection with the requirements of DIN 14676. By the

The state of the art is defined in accordance with the requirements of DIN 14676.

Neither the tested service provider nor the affected property managers

when using the wireless smoke alarm device, there was a processing

sun-related data. Based on my exam results,

Service provider assured that the requirements of the DS-GVO and the BDSG

to observe the data processing and thus, for example, order processing

to conclude rental contracts with the landlords and to ensure that they are complied with

of the information requirements according to Art. 13 ff DS-GVO.

8.3

Sending of automatically generated confirmations of receipt

with personal data when using an encrypted

contact form

If a service provider provides an encrypted contact form to its customers

available, should the automatically generated confirmation of receipt be sent by

E-mail without communication of personal data, as not secure

can be asked that the provider of the customer's e-mail service

enables transport encryption.

A citizen made me this year on a privacy law

Problem when using the contact form on the homepage of the

Deutsche Bahn attentive. When using the contact form

the customer his personal data in particular in the form of

Contact details such as name, address, telephone number etc. This information

Transmissions were encrypted via the contact form to Deutsche Bahn

transfer. However, the customer then received an automatically generated

ated acknowledgment of receipt by e-mail, all specified in the form

included personal data.

Sending e-mails with personal data carries the risk

that in the absence of encryption third parties intercept the communication

and thus gain access to the data. True, the leading

e-mail service provider in Germany, a transport

use encryption throughout when communicating with one another

("E-mail made in Germany"), however, full implementation may occur

especially when using foreign (particularly non-European)

bidders are not guaranteed. Users of an e-mail service

are therefore dependent on providers using transport encryption

use in email communication.

After I changed the group data protection of Deutsche Bahn to this

Problem pointed out was a change in the technical process

performed. Since then, in the automatically generated return mail to the

When using the contact form, customers do not receive any data from the contact form

mular contain more. The customer only receives an acknowledgment of receipt

sent by e-mail with the transaction number.

Since this adjustment means that the customer specified in the form

no more contact details (name, telephone number etc.) in the e-mail

are transmitted, I have the procedure for data protection

deemed permissible.

9. Healthcare

healthcare

9.1

Medical record requirements by law

Health insurance companies to support the insured

medical errors

Due to the legally defined division of tasks between the medical

zinische Dienst der Krankenversicherung (MDK) and the health insurance companies

there is the principle of social data protection law that the health insurance companies

are generally not allowed to take note of any medical data.

However, this does not apply when documents are required by law

Health insurance companies to support the insured in the event of treatment errors.

Many statutory health insurance companies offer their members the option of

Contact the health insurance company if you suspect a treatment error

can turn. Help and a professional treatment

error management offered. The health insurance company checks the suspicion

Treatment or care errors as well as damage caused by medical devices

or pharmaceuticals could have arisen and supports those affected

in enforcing claims.

During the reporting period, I received a number of inquiries from doctors about this. At-

Specifically, the question was whether a statutory health insurance fund itself provided medical

Documents to support insured persons in the event of treatment errors

may demand without turning on the MDK. Ultimately, the health insurance company

basically do not take note of any medical data.

Legal Assessment

In the fifth and tenth social code (SGB V and SGB X) are the

data protection powers of the health insurance companies comprehensively and

finally settled. Accordingly, there is also a legal

basis for the described activities of the health insurance company. Already in 1989

§ 66 was added to SGB V, which allowed health insurance companies to

their insured persons in pursuing claims for damages

to support treatment errors.

Even according to the current version of the law, it is part of § 66 SGB V

the tasks of the statutory health insurance companies, insured persons with the insurance

to help follow up claims for damages from medical errors,

if the alleged treatment error in connection with the

claiming an insurance benefit from the health insurance company. The relative

indefinite provision was made by the Act to Strengthen Medicinal and

Supply of aids (Healing and Aids Supply Act - HHVG) from

04.04.2017 the following sentences 2 and 3 were added:

"The support of the health insurance companies according to sentence 1 can, in particular, check the

documents submitted to the insured for completeness and plausibility, with the consent

the request for further documents from the service providers,

the initiation of a socio-medical assessment by the medical service

according to § 275 paragraph 3 number 4 as well as a final overall assessment of all available

relevant documents. The on the basis of the consent of the insured at the

Data collected from care providers may only be used for the purpose of support

of the insured person in the event of medical errors."

This extension of § 66 SGB V represents a specification of the sentence

1 of § 66 SGB V specified support service of the health insurance

sen dar. On this basis, therefore, the direct publication of

Treatment documents are sent by the doctor to the health insurance company. The

associated regulation that allows the health insurance company to do this

to collect and store data accordingly can be found in § 284 paragraph

1 number 5 SGB V.

The health insurance company is allowed to release patient documents according to § 66

SGB V to call them themselves however only if they rely on the support

according to § 66 SGB V, namely to a more precisely defined treatment case

relates. In addition, it is a prerequisite for publication that a current,

declaration signed by the patient on the release from the medical

Confidentiality with consent to release to the health insurance company

se is available. This declaration must relate to the specific treatment case

relate.

According to § 66 sentence 2 SGB V, the health insurance company can also use the MDK with a commission assessment. Accordingly, the health insurance company can Also request the MDK to hand over the treatment documents. Is this the case are the copies of the treatment documents according to § 276 para. 2 Sentence 2 SGB V directly to the MDK, not to the health insurance company. According to § 276 paragraph 2 sentence 1 SGB V, the MDK can also Test order by the health insurance company itself Treatment documents dated request doctor.

As a result, it can be stated that within the framework of the support of the Insured persons in the event of treatment errors according to § 66 V SGB with the consent of Insured persons are permitted for the health insurance company to insure corresponding data

healthcare is working. For this purpose, medical documents from the service providers can also be sent directly to the health insurance company.

9.2 Glass container with patient data in the hospital

In addition to the classic patient file, hospitals also have other areas in which attention is paid to the protection of patient data must become. Disposal of "used glass" can also lead to data protection break down.

Before May 25, 2018, Hesse was required to report data protection cases for hospitals that are subject to the HDSIG. With the entry into force of the GDPR, the Hessian hospitals according to Art. 33 DS-GVO independently report data protection incidents. The following case has turned into

happened in a Hessian hospital:

The data protection officer of the clinic was pointed out by a person

made you aware that there was an overflowing used glass con-

tainer noticed. The container was a normal one

Standard containers, such as those usually provided by waste disposal companies

Waste glass collection is set up. Disposed of in the relevant container

the clinic waste glass, as is the case with infusion solution bottles or

other liquid medication is used. Problematic here

was that a not inconsiderable proportion of these glass containers with an

additional label was provided. This label contained at the time of

Incident, a detailed record of the affected patient with:

– Patient Identification Number (PID)

- Name first Name

- Birth date

- Address

– health insurance number

- Name of Health insurance

– affected hospital ward

– Name of the doctor treating you (in part)

The open structure of the container made it easy to

Data from some hospital patients and hospital staff

to see and steal individual bottles.

Measures taken

After the clinic found out about the facts, she has the incident

reported to me immediately according to Art. 33 DS-GVO.

In order to reduce the risk of unauthorized access by third parties,

As an immediate measure, the containers were placed in a lockable room

accommodated. There they should be

be kept closed, so that only employees of the clinic and

authorized personnel have access.

In a further step, the clinic worked with the responsible disposal company

agreed that the containers will also be picked up at the scheduled pick-up time

are no longer publicly accessible.

It was then checked which data was used in terms of which

Adhesive labels for which purpose are absolutely necessary. In addition

at the same time controls the extent to which processes make sense and are proportionate

can be restructured, so that in some places there may be no corresponding

corresponding data or adhesive labels are no longer needed.

It turned out that in compliance with Art. 5 Para. 1 c DS-GVO

at a significant number of points of use on a majority of the

data can be omitted. The clinic then has the templates for the

The adhesive labels to be used have been fundamentally revised and adapted to the

adhesive labels specifically tailored for different areas of application

developed with appropriately adapted data sets.

As a further safety measure, the disposal processes were

fits, so that unintentional knowledge by third parties does not continue

is possible. Documents or forms on which labels are used

den, will, as before, comply with data protection after the expiry of the statutory

Retention periods in the document destruction of a certified service

given. As it is for appropriate drug packaging

(especially glass and plastic) no certified disposal company in the sense

data protection-compliant document destruction and the removal of the

Labels of any medication packaging hardly or only with

proportionate effort is possible, the disposal processes were

changed for such packaging. These are now sent to the processing

collected at the posts (clinic wards) and daily in locked ones

Containers placed in an electromechanical compactor. the

The closed garbage compactor is located on the premises of the clinics

and cannot be opened or otherwise viewed by third parties.

After collection by the disposal company, these compactor containers are

straight into the closed antechamber of the waste incineration plant (so-called

healthcare

Bunker) emptied, which is restricted access for security reasons. Through

the emptying into the bunker takes place in the first step, a thorough mixing

with other waste. In the second step, the contents of the bunker

continuously by an automatic transport device in the combustion

chamber forwarded in due to the prevailing there enormous

Temperatures in particular the labels and thus the personal

data will be irretrievably destroyed.

Conclusion

In the present case, the clinic has, in my opinion, been exemplary

behavior and reacted immediately after learning of the incident. As a result,

created a disposal process for the clinic's glass waste, which is under

Compliance with Art. 5 Para. 1 f DS-GVO the risk of becoming aware of the

Excludes patient data from third parties as far as possible.

9.3

Loss of treatment documentation due to water damage

Doctors have suitable technical and organizational measures

to take measures to protect the patient documentation from natural hazards

to protect. The accidental loss of the treatment documentation

a reportable personal data breach

i. s.d. Art. 33 i. V. m. Art. 4 No. 12 DS-GVO.

In the spring and early summer of 2018, there were several strong ones

Storms in Hesse. Independently of each other, medical practices reported to me that

that a storm had caused water to enter the basement of the practices,

where patient records are kept. Here the water

destroyed a large part of the medical documentation.

In a first case in mid-May and thus before the GDPR came into force

the water from the sewer through toilet and shower practice in

the cellar. The ones stored in the bottom drawer of a filing cabinet

Medical records were sodden by sewer water.

In a second case at the beginning of June, i.e. after the GDPR came into force

the water opened a window and flowed through the metal

cabinet in which the documentation was kept. All stored in it

Index cards were badly soaked. The paper documents are in both

cases become illegible.

Finally, a third case took place in the fall of 2018 in a doctor's office

through a pipe blockage in the ceiling of the basement, a massive

escaping (mixed with faeces) instead. This resulted in patient records

soaked and partly very dirty. However, the files could open

my reference to be dried and have been practiced according to

Years divided, packed and sealed in tight bags. According to

In practice, if necessary, the heavily soiled files could also be cleaned

be made available at any time.

Legal Assessment

Case 1 – ingress of sewage water into the basement room

When the documentation was destroyed by sewage water in mid-May

2018 in the first case, according to the old BDSG, there was still no obligation for the

Practice of reporting the loss of patient documentation. § 42a BDSG

old provided for a notification obligation to the supervisory authorities only if the in

§ 42a sentence 1 BDSG old listed data unlawfully transmitted or

otherwise unlawfully made known to third parties.

The incident could not have been punished with a fine. Because of

the insufficient backup of the documents may have been here

a violation of § 9 BDSG-old, since the necessary technical and

organizational measures had not been taken by practice.

However, this required repressive sanctions through the mechanisms

of the law on administrative offenses in the BDSG a. F. not provided.

At my suggestion, the practice carried out a sewer renovation and built

a backflow preventer to prevent such damage. This pointed

follow me up with a craftsman's invoice for the work carried out.

Case 2 - Water ingress through a basement window

In the case of early June 2018, where flowing through a basement window

Water made the patient documentation illegible, however

new legal situation, a violation of Art. 5 Para. 1 lit. f DS-GVO to assume

men. According to this, personal data must be “processed in a manner

will ensure adequate security of personal data

guaranteed, including protection against unauthorized or unlawful

processing and against accidental loss, accidental destruction

or unintentional damage by suitable technical and organizational

satorial measures ('integrity and confidentiality')".

Loss of patient documentation constitutes a breach of protection

personal data according to Art. 4 No. 12 DS-GVO and is therefore

according to Art. 33 DS-GVO usually to be reported to the supervisory authority, since here

almost always from a risk to the freedoms and rights of individuals

66

healthcare

to go out. Finally, the legal documentation obligation also serves

Purposes that are primarily in the interest of the patient

(See for example Wagner in: MüKo BGB, § 630f Rdnr. 2f., 7th edition 2016:

"A well-managed patient file makes it easier to switch doctors because it

makes it easier for the physicians who take over to build on what has already been achieved

and thereby the repeated implementation of diagnostic or therapeutic measures

Avoiding measures helps. Furthermore, the documentation ensures that in

Interest to be recognized within the framework of the general right of personality

of the patient to learn from their own history of illness and treatment

to be able to take note of it."). Also the function of preserving evidence

Documentation or its function as evidence in a medical liability

process is defined by the legislature as one of the regulatory purposes of § 630f

BGB recognized (Bundestag publication 17/10488 p. 25). For these law purposes

The patient documents, which have been damaged to the point of being illegible, cannot

be processed more.

Violations of the principles of Art. 5 DS-GVO can, according to Art. 83

Para. 5 DS-GVO can be punished with an increased fine. present

However, the facts were due to the timely notification according to Art. 33

DS-GVO not relevant to fines, § 43 Para. 4 BDSG.

In the future, the files will be moved to another basement room without windows.

brought, in which they are kept far above the ground. The exchange

the windows through which the masses of water could penetrate into the cellar,

was prompted.

Case 3 – Heavy contamination of documents due to burst pipe

In the last case from autumn 2018, the documentation was due to a

Damaged due to a burst pipe, but not lost. A risk for them

Rights and freedoms of natural persons according to Art. 33 Para. 1 DS-GVO

could therefore be denied here. However, there was one here as well

Notification according to Art. 33 DS-GVO makes sense, since only on notice from my authority

the practice promised to dry all (even heavily soiled) documents

and to store it until the end of the statutory retention period.

General information on storing patient records

The storage of patient documents is according to Art. 5 lit. f DS-GVO

established principles. There is also a special one for this

Protection against elementary damage and tap water damage.

Since basements are particularly at risk of flooding, the storage of files

to take precautionary measures in cellars, e.g. e.g.:

– adequate drainage

– Check valves (against pressing water from the drain)

– tight windows (against the pressing water from outside)

– Secure location of the files (not under a window, storage from a

certain height, no water pipe in the room)

In addition, the paper documents and other data carriers should be

protection against damage in the basement, e.g. by:

– Regulation of humidity (this must not be too high)

– Temperature regulation (must be constant)

9.4

Offer of a "service mailbox" by a doctor's office

Doctors have suitable technical and organizational measures

take measures to prevent unauthorized third parties from accessing patient data

to refuse. This is true even when they have prescriptions and referrals

outside of their practice rooms for their patients

would like. For documents that contain health data, there is a

special need for protection.

Through an entry I became aware that a doctor had a prescription

te and referrals for their patients to collect in a public

accessible mailbox. The key to the mailbox was in it

thereby permanently in the mailbox, so that authorized and non-authorized

People could take the documents stored there with them at any time. On

When I asked, the doctor said that the patients

mostly by telephone asking to be left in the mailbox, asking for the

to be able to take items with you outside of the opening times. The recipes

or bank transfers would, in a sealed envelope and with

labeled with the names of the respective patients, in the

put mailbox. The postal route is an unsafe alternative for this.

The mailbox was in front of the entrance to the practice, the one from the street

secluded and not visible to bystanders. According to the

Doctor has not received any negative or abusive feedback so far

uses of content by third parties have occurred. Nevertheless struck

In the future, they will only accept orders for depositing them in the mailbox in writing

and attach a combination lock to the mailbox.

68

healthcare

Legal Assessment

The practiced procedure was - even with the proposed changes

Demands – not permitted under data protection law.

The storage or deposit of patient documents is according to the

in accordance with the principles laid down in Art. 5 (1) (f) GDPR.

Despite any express written order from patients

and patients to deposit in the mailbox, the doctor remains the owner

and operator of the mailbox and as the "sender" of the data responsible

Liable body for the processing of the data within the meaning of Art. 4 No. 7 DS-GVO.

She continues to bear the obligations from Art. 5 DS-GVO and has in particular through

appropriate technical and organizational measures

To ensure the security of personal data (Art. 5 Para. 1 lit. f DS-

GMO). According to Recital 39 of the GDPR, this includes unauthorized

Individuals should not have access to the data. What measures

must be taken to protect the data depends in particular on
the risk of unauthorized access, the type of processing and the
Importance of the data for the rights and interests of the data subject
away. When assessing the appropriate level of protection, in particular
separate the risks of destruction, loss, alteration or unauthorized
Disclosure of or unauthorized access to personal information
into account (Article 32 (1) and (2) GDPR).
Since the doctor, by forwarding the prescriptions and referrals,
processed health data within the meaning of Art. 4 No. 15 DS-GVO is Art. 9 Para. 1
GDPR to be observed. As a special category of personal data
Health data is particularly worthy of protection. Because of that it is
in my view inadmissible, the patient entirely on the protection
to have their health data waived. Effective Consent
is eliminated here because neither for the doctor nor for her
Patients can see who has access to the data
might and for what purposes they might be used
could. The patients can therefore not be fully informed
consent to such transmission or disclosure, which ultimately
unforeseeable dangers, such as e.g. B. a publication on the Internet, in itself
can salvage.
Requirements for the technical and organizational measures
With regard to the sensitivity of the data, the through the permanent
existing keys that can always be opened by anyone
acceptable. The solution of a numerical

castle with daily changing access codes would have to be designed like this

be that the access number used daily neither for bystanders

Third parties for patients who currently did not have anything to collect,

is predictable. So separates z. B. the use of the current day number or

a fixed two-digit number with a running number of the current one

day of the week as too easy to overcome. Rather, it would have to be random

Sequence numbers are generated.

A standard mailbox is also available for depositing recipes or

other medical documents with patient data are completely unsuitable.

Neither the material nor the locking system pose any serious resistance

against burglary or vandalism. A suitable container for the

the service offered by the doctor would have to ensure, be that

- the unauthorized opening of the collection container only with considerable expenditure of time

and use of tools is possible,

- a theft of the locked container by appropriate

anchoring is largely prevented or made more difficult and

– an unauthorized removal by third parties via the possibly existing one

throw-in is not possible (locking flap or blocking of the throw-in).

With regard to the location, too, there were increased demands on the

to provide protection. The entrance area that cannot be seen from the street

outside the practice opening hours was in this respect with a high degree of probability

largely unobserved.

In addition, the individual sealed envelopes with the prepared

clearly marked the documents in the container with the respective recipients

be labeled in writing so that they can immediately recognize that

the document

– clearly comes from practice,

– has not been opened by third parties,

– the content is complete and unchanged.

Finally, the question arose whether several documents – and

if so, how many - per day could be made available for collection, there

it could not be ruled out that authorized users accidentally

remove or manipulate third-party documents maliciously or willfully.

Above all, it is problematic that an abusive removal

me would only notice afterwards: Recipients who have sent their document/s

miss, could contact the practice on the following opening day at the earliest.

animals. It could only be determined in retrospect whether the announced

Document was forgotten or possibly stolen by a third party.

Result

In order to meet the data protection requirements regarding health

to meet the requirements, the doctor would have a locker or packing station-like

must provide a system that is compatible with the measures described above

a suitable number of pick-up boxes for each patient (with

random change of the access number after each pick-up).

The technical and organizational requirements I have set for the

The nature and operation of a data protection-compliant "service letter

kastens” the doctor did not want to fulfill and therefore stopped the operation of the

mailbox.

9.5

Advanced training certificates from the State Medical Association of Hesse

Continuing education certificates that are posted publicly in the doctor's office or in the

Hospital should be used, no date of birth information

and/or place of birth of the doctor. This information is

to prove to the patient that the doctor is

has trained in accordance with professional regulations is not required.

A doctor complained that the state medical association

Hesse (LÄKH) issued advanced training certificates apart from the preliminary and

Surnames and the salutation also the date and place of birth

will be printed. The advanced training certificate is a voluntary offer

LÄKH to its members and can be printed out in the LÄKH member portal

become. Although the certificate is also intended for public display in

the doctor's office or in the hospital is determined, was the indication and the

Printout of date and place of birth mandatory by the system

been given and could not be restricted.

When I asked the LÄKH about the need to state

Place of birth and date of birth on the certificate stated that her

Information according to physicians the advanced training certificate as well

to prove the fulfillment of the further training obligation to the cash register

medical association Hessen would use. In order for this to be possible

the certificate must be unique. The certificate is a certain one

better assignable to a person. In coordination with the recognition body of the

LÄKH became the formulation of the advanced training certificate by the LÄKH

nevertheless changed in such a way that this is now without the indication of the

Place of birth and date of birth can be generated.

From my point of view, doctors must

ten not disclose date and place of birth when providing proof

result in them continuing their education in accordance with professional regulations

- Finally, the posting of the further training certificate in the practice or

not compulsory in the hospital. The risk of abuse, for example

if the names are the same, I see a certificate intended for posting

fikat rather as low. A necessity of this information is therefore not

given and against the background of the principle of data economy

pursuant to Art. 5 (1) c) GDPR dispensable.

9.6

Examination of a pharmacy

In my past activity reports, the examination of medical

practices and hospitals. This year was too

a pharmacy the subject of an on-site visit.

The anonymous submission reached me in February of the reporting period

of a citizen: As the submitter described, he was from a public

accessible paper bin documents "flown against", which personal

related data contained. These could be found at a nearby pharmacy

be assigned. The documents found were the input

attached. As could be inferred from these documents, it was

primarily about application documents and thus about personal data

Employee data i. S. of § 26 Para. 8 BDSG. These actually were

intended for destruction.

I went to the pharmacy at short notice to find out what was going on on site

to clear up.

The paper bins mentioned were in the backyard when I visited

the pharmacy. The entrance to the yard is provided with a door which, due to the

Frequency of use is mostly open, so that the yard with the paper bins

not only visible from the outside, but also accessible to everyone.

The backyard is also used by the residents and visitors of the

house used.

At my appointment, which was only announced shortly beforehand, I was able to go to the public

accessible paper waste bins further documents with personal

Discover data that could be assigned to the pharmacy (e.g. prescription pick-up

banknotes and various handwritten notes). The papers were

only roughly torn or crumpled before disposal.

72

healthcare

The "deletion and destruction" of personal data falls under

Art. 4 No. 2 DS-GVO under the processing concept of the DS-GVO. According to Article 5

DS-GVO must process personal data in accordance with paragraph 1

lit. a to lit. f are processed. But she has to

The personal data will be processed in a manner that

ensure adequate security of personal data,

finally, protection against unauthorized or unlawful processing and against

accidental loss, accidental destruction or accidental damage

Damage caused by appropriate technical and organizational measures

("Integrity and Confidentiality").

As the owner of the pharmacy admitted, the pharmacy did have one

document shredder, but did not use it regularly or did she think

that some documents are not so sensitive that they can be processed professionally

would have to be destroyed. In addition, the shredder was both from

in terms of its performance and its protection class

the sensitivity of the data to be processed is insufficient.

I therefore asked the owner that the pharmacy

purchases document shredders that meet the requirements, with which in the future

it is ensured that any resulting paper waste complies with data protection regulations

can be crushed.

According to the requirements of DIN 66399, it should be a device of the

Class 3, better act class 4. Alternatively, there is the possibility

a sealed paper

to have the bin set up, with the professional disposal of the contents

is contractually and organizationally ensured.

On the occasion of my site visit, I presented two more data protection

legally impermissible facts.

At the time of my visit, the pharmacy used a wall in the immediate

close proximity to the customer area as a pinboard for pick-up slips. With a

short "look around the corner" it was possible to single data, such as

name or medication.

I asked the owner of the pharmacy to find an alternative storage

to find a means of protection to ensure adequate data security and

to ensure confidentiality.

Furthermore, in the rear working area of the pharmacy, application

documents from rejected student interns in two standing folders

true. The rejected applicants would receive the documents

usually pick up directly at the pharmacy. Since the pharmacy management does not

day in her office, this location was chosen. The folders carried

the inscription "Applications Good" and "Applications Bad" and are

freely accessible to all employees. I have an organizational one here too

remedy required.

Result

As a result, it was noted that the pharmacy is still in some areas

had some catching up to do in terms of data protection compliant pharmacy operations

concerning.

In the meantime, the owner of the pharmacy has confirmed to me that a

paper shredder that meets my needs was procured. Also

the employees were sensitized to the fact that

all documents with personal data before disposal in the

to shred paper bins according to the specified DIN standard.

A new procedure has been introduced for the storage of collection

leads. They are now no longer visible to customers.

From now on, all application documents will also be stored in a lockable

kept in the office and destroyed within the specified period.

Since the principle of Article 5 (1) (f) GDPR applies to data destruction

was not observed, there is a violation within the meaning of Art. 83 Para. 5 lit.

GMO before. The improper disposal of personal data

can meet the criteria for a fine and will therefore be imposed after completion

the technical case study also from my fine office to that effect

be checked and evaluated.

video surveillance

10. Video Surveillance

video surveillance

10.1

Video surveillance in the nursing service

In the business premises of an outpatient care service, the

aisle area, the waiting area and registration using a dome

Camera constantly monitored. After examining the facts, the

Dismantle the camera effected.

The complainant was an employee in an outpatient nursing

service. She complained about the installation of a video camera in the

Business premises of the outpatient care service. She herself, as a

constantly exposed to surveillance. An information through

the employer had not given her consent and, to the extent that her

known that other colleagues had not been granted either.

I have asked the owner of the nursing service for information about the video

installation requested. After examining the documents received,

found that a dome camera was installed covering the front door,

monitored the reception area and the corridor in front of the entrance. As

Purpose for video surveillance was stated that the camera for

Prevention of theft as well as burglary has been installed. Over and beyond

this should be used to identify whether senior citizens are in danger

be. The data is not saved.

According to Article 6 Paragraph 1 Letter f of the General Data Protection Regulation, the monitoring

regulation (DS-GVO).

According to Art. 6 Paragraph 1 lit. f. GDPR, the processing is only lawful,
if they are to protect the legitimate interests of the person responsible or
of a third party is required, unless the interests or fundamental rights
and fundamental freedoms of the data subject that protect personal
general data require, especially when it comes to
the data subject is a child.
To avoid theft or burglary was the video installation
not suitable. Proof to law enforcement would be here
not been possible because no recording took place.
The mere installation of the over-
watch not helped. In the event of a health hazard, the
Monitoring device no warning or alerting of the rescue
service made. Since the counter area in the foyer is permanently occupied
was, the direct help by the employees of the

Nursing service of affected seniors more appropriate than monitoring the
health-endangering situation.
In addition, I have complained that the owner of the nursing service
his information obligations towards his employees
workers and visitors to the practice rooms not extensively
had complied. On the entrance door to the nursing service practice was hanging
an approx. 8 x 5 cm reference to the video surveillance. This one was
but not in the field of vision and extremely discreetly on the door leaf in the upper corner
appropriate. All information on video surveillance according to Art. 13 ff

DS-GVO (including name and contact details of the person responsible, contact details
of the data protection officer, purposes for which the personal data
are processed, legal basis for processing, legitimate interests
eat, which are pursued by the person responsible) were missing. Also others
Information, in writing – e.g. B. by circular – or orally – e.g. B.
in an internal service meeting - did not take place.
I have therefore carried out a hearing in accordance with § 28 HVwVfG because I
intended to issue a removal order in accordance with Art. 58 Paragraph 2 lit. f DS-
GVO to enact against the owner of the outpatient care service.
However, the instruction to remove the video surveillance could
remain, since the dismantling of the video camera without replacement before the end of the
Deadline for comments has been proven.

10.2

Use of video surveillance to avoid "wild garbage"

The installation of a video camera is usually not permitted in order to
To convict the polluters of so-called wild garbage.
Although a waste management system is operated in Hesse, which allows the citizens
allowed to dispose of their waste free of charge in most cases, the inappropriate
casual dumping of garbage on streets, glass containers, forest parking lots,
a big problem on dirt roads and many other places. The rubbish remains
lie too long, often other waste or even polluted waste
added by other citizens.
This type of waste disposal is classified as an administrative offense or as a criminal offence
treated and subject to a fine. However, this does not appear to be effective
scare.

video surveillance

a) Problems in public places

The polluter is responsible for the disposal of rubbish in public places

responsible. If this cannot be determined, the property owner is liable

mer for disposal. In most cases, these are the municipalities. The

Waste is not only a major environmental burden, it also ties up staff and

Costs that are subsequently passed on to the general public.

In order to master the wild garbage dumps and a formation of dirt

To prevent corners, several municipalities came up with the

Idea of video surveillance in certain intra-communal areas

to install, and asked me under what conditions this in the

action can be implemented.

The concerns of the municipalities may be understandable. However, it existed

no legal basis for the projects that would allow this procedure

would let.

In the context of averting danger, the regulatory authorities may video surveillance

carry out remedial measures in places where various

Crimes have been committed and there is a risk of further crimes

be committed. Such monitoring must also always be open

(§ 14 Para. 4 HSOG).

Neither condition was met in the cases presented.

These were not crime hotspots i. s.d. HSOG and the

Surveillance should always be covert. The planned measures

were disproportionate. In addition to video surveillance, there were others

suitable ways to prevent deposits. The supervision

of public places should always be ultima ratio, ie the last resort

be of choice, other solutions are generally to be preferred. So

For example, public space could be designed in such a way that

structural measures or through a regulated access the deposit

prevented from littering.

Another request concerned the intended surveillance

a forest parking lot. Here publicly accessible space was affected

can be entered by anyone (§ 15 Para. 1 HWaldG). was to be considered

therefore, whether there were indications that interests worthy of protection

outweighed the people affected by the video surveillance. In consideration

of interests, the personal rights of forest visitors had a severe

re. Also when checking whether it is a video surveillance after the

Aspects of criminal prosecution under the Administrative Offenses Act

was acting in connection with the Code of Criminal Procedure, I came to none

different result. The admissibility of video surveillance was also here

to deny. With video surveillance, not only people would

be filmed in which there would be misconduct, but incomplete

los all visitors of the public parking lot. This fact applies

far-reaching in the personal rights of forest visitors.

Basically it has to be taken into account that the effect of a video

monitoring to prevent litter in public places

quickly runs out. As soon as the camera is discovered - and it will be

inevitably very quickly due to the existing transparency obligations,

required by the General Data Protection Regulation - the waste is deposited

at the next available opportunity.

b) Problems in residential complexes

In particular by residents or housing

communities in densely populated urban areas and high-rise residential

ten me both complaints about existing video surveillance of the

Garbage dumps as well as inquiries about installing new surveillance systems.

In the case of a high-rise apartment building, I came to the conclusion that the housing

construction company as the operator of the camera may continue to use it.

It could be presented in detail and documented when and how often it should be

gross violations occurred, which resulted in high costs for the community of owners

led. The legitimate interest i. S.v. Art. 6 Para. 1, lit. f DS-GVO could

I affirm.

In another case, the camera had to be dismantled. The camera was from

House wall of an apartment building on the garbage dump on the opposite

lying side of the street. Type and frequency of contamination

were not presented. The interests and those with surveillance

associated personal injury of passers-by and tenants

considered to be more serious than the insufficiently declared interests

of the operator.

10.3

Private video surveillance of public space

Numerous complaints reached me again from passers-by and residents

ners, which are aligned from private property to the public area

video surveillance systems concerned. Likewise, regulatory authorities gave

a number of incidents reported to them on the same subject

kindly off to me.

video surveillance

A video surveillance of public roads, sidewalks and private

places is generally not permitted. I have already done that in previous jobs

quality reports (see e.g. 46th TB, item 11.4; 45th TB, item 5.2.1,

43. TB, Section 5.2.1.2). Under the General Data Protection Regulation

(GDPR) nothing has changed here. The following examples show this.

A camera operator had his camera on the sidewalk and the street

ß aligned in front of his property to his often parked there

to monitor the vehicle. He filed a criminal complaint to justify it

due to property damage to the vehicle. A justification for that

It wasn't video surveillance of public space. Besides that-

of that surveillance was also carried out when the vehicle

was not employed there, parking motor vehicles is not a form of parking

riparian use. The video surveillance was according to the standards of the

Art. 6 Para. 1, lit. f) GDPR.

The justification for a one-off damage to property of the motor vehicle

I have, in view of a permanent surveillance of public space

mes in front of the property 24 hours a day, deemed insufficient.

The camera had to be dismantled.

In another case, a self-employed craftsman had two cameras

directed from the wall of his house into the public area. incidents were

not described by the camera operator. The reason given was

brought that in front of the property line in public space the hand

work vehicle was parked that contained tools. The supervision

succeed purely as a precaution.

The purpose given was domiciliary rights and vandalism prevention. A

However, domiciliary rights in public space (e.g. domiciliary rights on cars) do exist

not. Monitoring of public space is also preventive

purposes not permitted. These cameras also had to be dismantled.

Since there are always questions and incorrect assessments in the

Setting up and operating a surveillance camera is coming here

To summarize what is allowed and what is not:

1. The camera may only film its own property. On pivoting

Cameras should be avoided.

2. Recordings of public areas, such as streets and sidewalks, are in

usually forbidden.

3. Anyone who is filmed unlawfully can injunctive relief and compensation

demand.

4. Visitors should be made aware of surveillance.

5. The neighboring property may not be filmed.

10.4

Video surveillance in gastronomy

Where people gather for leisure activities or to eat and drink

As a rule, no one is allowed to stop for drinks during opening hours

video surveillance take place.

In the year under review, I received more and more complaints about video surveillance

in catering establishments (both indoor and outdoor catering)

gone Kebab shops, ice cream parlors and swimming pool restaurants were affected

as well as a number of eateries. In several cases I have

Removal of cameras successfully ordered. The cameras were

reduced.

The Business Working Group of the Conference of Independent Data Protection

authorities of the federal and state governments (former name: Düsseldorfer

Kreis) already carried out “video surveillance” in its orientation guide

non-public bodies" from 19.02.2014 under item 3.2 the common

Position of the supervisory authorities on monitoring in gastronomy

expelled:

"The video surveillance of the guest room of a restaurant is according to § 6b BDSG

(a. F.) usually inadmissible under data protection law. At least the ones with tables and

Gastronomy areas equipped with seating are customer areas,

that invite you to linger, relax and communicate and with that

may not be monitored with video cameras.

The behavior attributable to the leisure sector as a guest in a restaurant

with a particularly high need for protection of the personality rights of the person concerned

come along. Video surveillance disrupts undisturbed communication

and the unobserved stay of the restaurant visitors and thus takes effect

particularly intensively in the personal rights of the guest. The protectable

The interest of the visitor normally outweighs the legitimate interest of the

Gastronomy owner in a surveillance, which is why his interest only

can prevail in rare exceptional cases."

This has not changed as a result of the new legal situation, which is decisive

now Article 6 Paragraph 1 Letter f) GDPR. Operators of catering establishments should

therefore measure corresponding projects strictly against the orientation guide.

As a rule, video surveillance is not permitted under data protection law.

signed Source of the orientation aid: https://datenschutz.hessen.de/sites/

datenschutz.hessen.de/files/content-downloads/OH_Videoueberwachung%20

non%20public%20jobs.pdf

80

video surveillance

10.5

Video surveillance in swimming pools

Video surveillance of people in sanitary rooms, changing rooms

or changing rooms and in the sauna is not permitted.

Also this year I received several complaints regarding

video surveillance in swimming pools. A complaint was made

against surveillance in the collective changing area of a central Hessian

swimming pools.

According to Art. 6 Para. 1, lit. f GDPR, the monitoring device was allowed

evaluate.

Pursuant to Art. 6 Paragraph 1 lit. f. General Data Protection Regulation (GDPR).

the processing is only lawful if it is to protect the legitimate

interests of the person responsible or of a third party, provided that

not the interests or fundamental rights and freedoms of the persons concerned

person requiring the protection of personal data prevail,

especially when the data subject is a child

acts.

I found that the operator had a total of twelve cameras and two camera

dummies installed in the swimming pool. After testing and evaluation

the video surveillance was established on site in compliance with data protection as follows:

– In the entrance area at the turnstiles to the swimming pool and to the

Sauna, as well as at the cash desk and at the pay machine (monitoring
of employees did not take place) the recording was made during the
opening hours and adjusted to the times outside the opening hours
times reduced. Staff was on site during opening hours, so that
monitoring was not necessary at these times.

– The cameras at the entrance and exit of the slides remained
installed to support the supervisory staff. The recording function
was deactivated.

– The storage time of the remaining recording cameras has been increased
72 hours reduced.

– Cameras in the changing area, at the turnstile to the gym as well
a dummy camera in the family locker room has been removed.

– The information signs were in accordance with the basic data protection
adjusted and expanded.

81

In addition, I refer to my comments on video surveillance in
swimming pools in the 44th Activity Report 2015, Section 8.2. The one presented there
Guide to video surveillance in swimming pools has been revised
and published as of January 8th, 2019 (see also Appendix I 3.2).

82

11. Economy, banks, self-employed

Economy, banks, self-employed

11.1

Transmission of data by banks to divorced spouses

The transmission of personal data by banks and savings banks

to spouses is only permissible if this is based on a power of attorney

or account ownership are authorized to receive the data. On the

Marriage alone, on the other hand, cannot support a transmission.

In the year under review, I received a number of complaints which

Transmission of personal data to divorced spouses

by banks and savings banks. In all me

The data transfer was not permitted for the processes that were brought to attention.

There were two scenarios:

a. the publication of an up-to-date account overview, which also lists the accounts

and account balances of the divorced spouse were listed and

b. the sending of duplicates of account statements for the current account

the divorced spouse.

In case constellation a), one individual applied for an overview

his/her accounts, due to the known and in data processing

also stored marriage was also handed over. Everyone was there too

Accounts of the divorced spouse for which neither a power of attorney nor a

co-account ownership existed. In case b) applied for

a person duplicates of bank statements for their own account, the

then mailed to the divorced spouse's mailing address.

Both case studies represented impermissible transmissions of personal

ner data because the spouse was not the account holder and neither

Account authorization was available.

In principle, data transmission is only permitted if it is based on

the regulations of Art. 6 Para. 1 DS-GVO can be supported.

Art. 6 GDPR

(1) 1The processing is only lawful if at least one of the following

conditions are met:

a) The data subject has given their consent to the processing of data relating to them

personal data given for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the party concerned

fene person is, or necessary to carry out pre-contractual measures, the

be made at the request of the data subject;

c) the processing is necessary for compliance with a legal obligation imposed by the

Controller is subject to;

d) the processing is necessary to protect the vital interests of the data subject

or to protect another natural person;

f)

e) the processing is necessary for the performance of a task carried out in the public domain

interest or in the exercise of official authority, which the person responsible

was transferred;

the processing is to protect the legitimate interests of the person responsible

or a third party, unless the interests or fundamental rights and

Fundamental freedoms of the data subject, the protection of personal data

require, especially when it comes to the data subject

is about a child.

2Subparagraph 1 letter f does not apply to public authorities in the performance of their duties

processing carried out.

In the present case, neither of the two scenarios met the requirements

of Art. 6 Para. 1 GDPR.

If both spouses are joint contractual partners at the bank, e.g. B. in

As part of a joint real estate financing, the data may

this contract according to Art. 6 Para. 1 lit. b) GDPR, of course

be sent to the divorced spouse. The same applies if

the recipient has a power of attorney that is effective even after the divorce

has an account to which data is transmitted. Marriage alone, on the other hand,

does not constitute a permit. Therefore, a divorce usually has an effect

nor on the admissibility of data transmission to the person concerned

contractual relationship.

The cause of the incorrect transmission in the me as a complaint

The facts presented lay in all cases in the storage and

insufficient correction of groups of persons and their faulty ones

assessment by the bank.

For spouses, banks create different ones in their bank application

Found so-called associations of persons (here, among others, married couples). This is e.g. B. in

within the framework of issuing exemption orders or also,

to have an overview of the total commitment of the spouses.

These groups of persons also contain the respective postal addresses of the

spouse. Within the groups of persons there are often mutual ones

Account powers of attorney or joint account ownership, which at present

authorize the receipt of personal data.

84

Economy, banks, self-employed

In case constellation b), the duplicates of account statements were due

of the postal addresses stored for the association of persons to the postal address of the already divorced spouse. However, this was for Not authorized to receive data.

Authorization to receive does not exist within groups of persons without exception. Therefore, even with existing associations of persons, the temporary authorization to receive personal data in individual cases check and observe.

In the cases discussed here, this was not done sufficiently. To- In addition, the data reached an already divorced spouse, what was perceived as particularly critical by the persons concerned. In ongoing divorce proceedings may result in the improper transmission of personal data also on the ongoing negotiations or that affect judicial proceedings.

In order to avoid such errors, credit institutions are therefore recommended to le of the stored groups of persons the respective authorization to receive to check and stored associations of persons in divorce proceedings correct or to delete the spouses association.

I have therefore asked the banks in all cases to de Deletion of the group of persons as well as the adjustment of the stored ones to make addresses.

11.2

Data breach in Mastercard and Mastercard Priceless Specials

The data breach at Mastercard Europe SA (Mastercard), from which after the Result of the previous investigations only the customer loyalty program Mastercard Priceless Specials Germany was affected, has shown how easily confidence in data protection and data security will be shaken

can and what expenses caused by such an incident at the responsible
lichen body and the supervisory authorities already through the processing of
Inquiries and complaints arise. For this reason alone, responsible
meticulously ensure that there are no security gaps.
Mastercard was made aware of this on August 19, 2019 by a third party
that a list of Mastercard customers that includes about 90,000 people
has been published on the Internet. In this list was next to the names
of the persons concerned also their date of birth, the postal address, the
Email address and full credit card number included. The

Credit card expiry date and security code (CVC) were from the date
data protection incident not affected.
The data protection incident quickly led to a large number of
Complaints to my authority. Common Complaints
were a lack of apology for the incident by Mastercard, Be-
think about receiving larger amounts of spam mail and a
general uncertainty due to the publication of personal data.
The content of the complaints has clearly shown that the publication
publication of data that is not usually accessible to everyone, such as this
date of birth, e-mail address and credit card number, for those concerned
people can be severely affected. Especially clearly
felt was a severe loss of confidence in the credit card company
Mastercard, as part of the credit industry in general
high level of trust in data protection and confidential

handling customer data. This uncertainty existed, although
affected persons could not represent material damage and
I am not aware of any cases of abuse.
Due to the incident, Mastercard was required to report this data protection
violations to the competent supervisory authority in accordance with Art. 33 DS-GVO
obliged as soon as Mastercard had determined this. Such a message
was submitted to me, although at that time it was still unclear which
che supervisory authority in Europe is responsible for the data protection violation.
Mastercard's global market presence initially required that for the
Data protection incident competent supervisory authority within the European
determine union.
The vast majority of people affected by the incident have
their place of residence in Germany. The customer loyalty program is also
gramm Mastercard Priceless Specials Germany only to customers with a
Residence in Germany. However, there were also people from the incident
concerned who have their place of residence outside of Germany. Mastercard
operates throughout the European Union and has offices in Germany
a representative office in Eschborn near Frankfurt am Main. At this re-
representative office is in accordance with recital 22 GDPR
a branch within the meaning of the GDPR. The Head Office
of Mastercard for the European Union is based in Belgium.
The data was also processed by a processor in Austria
processed. Consequently, there was cross-border data processing
within the meaning of Art. 4 No. 23 lit. b) GDPR.
For the treatment of cross-border data processing,
DS-GVO sufficient precautions taken. Even with a cross-border

Economy, banks, self-employed

data processing initially remains in accordance with each supervisory authority

Art. 56 Para. 2 DS-GVO responsible for receiving complaints.

However, does this recognize that cross-border data processing

may exist, informs them for the main office or only one

branch in the European Union responsible and thus in charge

competent authority immediately about the matter. The regulators

then coordinate the further processing among themselves. Decides the

lead authority to take over the procedure, this takes over

the lead management within the meaning of Art. 60 DS-GVO and coordinates the rest

Proceed. This was the case here.

Due to cross-border data processing, I have contact

registered with the data protection authority of the Member State of Belgium. The

After a short examination, the data protection authority of the Member State of Belgium

due to their responsibility for Mastercard's main office in

of the European Union in accordance with Art. 56 Para. 4 DS-GVO

to deal with the process as the lead supervisory authority. With it

took over the data protection authority of the member state Belgium according to

Art. 56 Para. 1 DS-GVO the coordination for the processing of the supervisory

legal duties.

In this case, the GDPR stipulates that the lead supervisory

authority according to Art. 60 DS-GVO with other supervisory authorities who are

process are also affected, cooperates. Here tries the

lead supervisory authority, between all supervisory authorities concerned

listen to reach consensus, and draft where necessary

is, a draft decision. Are all concerned supervisory authorities with
agree to the draft resolution, it will be approved by the responsible
supervisory authority and the head office or sole office
communicated to the person responsible.
In execution of these regulations, the data protection authority of
Member State Belgium, in consultation with me, to clarify the facts
and to investigate the reasons for the data breach.
In coordination with the data protection authority, based on my
permanent for the representative office of Mastercard all activities of
coordinated by supervisory authorities in Germany. This also includes the
Processing the complaints I receive and responding to them.
Due to the largely the same, with a few exceptions
complaint content of all complaints, these were uniformly
answers. If other supervisory authorities in Germany so wish
had, I also sent them a letter to answer the at
complaints submitted to them. to the current one

Information was also sent to all affected persons via a web
website at the address https://datenschutz.hessen.de/daten-
Panne-at-mastercard-priceless-specials-germany about the others
informed of the course of the matter. All concerned persons can
get up-to-date information there.
The clarification of the facts showed that Mastercard for
Has taken care that the personal data available on the Internet

data was deleted immediately. Nevertheless, the data could already
be copied by third parties before deletion. Through the made
deletions, it was therefore not possible to ensure that the published
cleared data can no longer be used or disseminated. Mastercard
therefore monitors the Internet for further publication of the data and
has arranged for their deletion or will arrange for their deletion.
The persons concerned were also informed by Mastercard about the incident
informed. Mastercard also has at https://www.mastercard.de/de-
de/faq-pricelessspecials.html an FAQ list with more details about the
Data breach published, with the help of which data subjects found out about
the measures recommended by Mastercard and the current status of the
investigations can inform. Affected persons can contact
the email address Germany@mastercard.com also directly to Mastercard
contact for more information. As one of the main risks
In the cooperation with Mastercard, the possibility of phishing
attacks on affected persons detected. The concerned
People have been informed and they have been asked to be more vigilant.
Further investigation of the process by one of Mastercard
commissioned and specialized in such processes showed that
that the data breach occurred as assumed at the beginning of the investigation
the Mastercard Priceless Specials Germany program and that
Mastercard's payment network was not affected.
Based on the facts known so far, there are none
Doubt. The one with the operation of Mastercard Priceless Specials Germany
commissioned service provider has no order for operation or implementation
other Mastercard programs. In particular, the service provider is not

involved in the operation of the Mastercard payment system.

Further investigation into details of the incident revealed that primarily

Security problems with the service provider commissioned by Mastercard

led to the data protection breach. There are many indications that

abuse of access rights contributed to the incident. The

Investigation took several weeks what mine

88

Economy, banks, self-employed

was not criticized. The measures taken by Mastercard hold

I for sufficient.

In principle, data subjects have Mastercard or

to a person commissioned by Mastercard to process the data

company according to Art. 82 DS-GVO a claim for damages. A

damage can e.g. B. by exchanging the credit card as a precautionary measure or

associated expenses arise. The parties

However, credit institutions have already been informed by Mastercard

tet that Mastercard expenses in connection with the exchange of

Credit cards replaced and the expenses of the credit institutes involved

cannot be asserted against affected credit card holders

should. Any damage from the exchange of credit cards should be concerned

Individuals therefore usually do not arise. Should damage nevertheless

claims for damages can be made directly to Mastercard

be quantified and claimed. The data protection supervisory authorities

however, cannot support this.

In addition to claims for damages, there are claims from those affected

Persons according to Art. 15 et seq. GDPR. In particular,

Claims for information according to Art. 15 DS-GVO and for deletion

Art. 17 GDPR.

Mastercard has a

Portal set up. I am not complaining about this. The portal is run by

Mastercard and only the data is used to provide information

queried, which is used to provide information and to identify the requesting party

people are required. Identification is necessary to avoid

a provision of information to unauthorized persons and is therefore primarily used

the protection of data subjects. Since from the publication also from

The e-mail addresses used by the data subjects were affected, please

Mastercard for security reasons to use the portal that has been set up.

I don't complain about that either. I still have Mastercard on it

pointed out that inquiries received without using the portal

are to be processed on self-disclosure in accordance with Art. 15 DS-GVO and the

information is to be given to the persons concerned.

However, there is a legal right to erasure according to Art. 17 DS-GVO

not. Mastercard is to document the previous participation of affected

commercial law obliges and entitles persons to participate in the program.

Existing access accounts do not have to be deleted either. Would like

data subjects no longer participate in the program, it is sufficient

when access is blocked. The risk of using existing

gangs, whereby claims for deletion asserted in complaints

were frequently justified does not exist. In addition, the entire customer

loyalty program has not been operated by Mastercard and is

currently unavailable.

Due to the processing, both Mastercard and I have significant

expenses incurred. This affects both editing

of information requests as well as the handling of complaints and

the clarification of the facts. The operation makes it clear that too

Security flaws of supposedly minor extent at the time of publication

of personal data to a considerable effort and re-

damage to the reputation of the person responsible. from the content

of the complaints that have been submitted to me, it is also clear that

that data subjects experience a significant loss of trust in the

Mastercard managed IT infrastructure. Responsible should

therefore your IT infrastructure and the security measures implemented in it

meticulously and meticulously in all critical areas

Make sure to implement two-factor authentication. this applies

especially for administrator access.

11.3

Uniform Postbank ID for private and business accounts

Postbank private and business accounts can be managed under a uniform

chen ID can be managed. By setting up profiles / sub-IDs

ensure adequate separation.

The connection of private and business accounts under a unified

chen Postbank ID made a number of data protection changes in the reporting period

complaints led. In particular, it was criticized that a sufficient

Separation between private and business accounts not guaranteed

may be. Both account types would be compulsorily linked to each other.

For example, if employees use online banking on their home PC

drive, is immediate access both to all private and to all

business accounts possible. Then other family members could too

View employer business accounts. Since the managerial right

Employer not entitled to requirements regarding safety measures

set up for private PCs is questionable whether from a risk perspective in

In such cases, access via a separate Postbank ID is required.

The complaints prompted me to take a closer look at the procedure.

Postbank was cooperative in this regard. The procedure was me in one

Personal on-site appointment at the Postbank sales center in Wiesbaden

presented and explained. I was able to determine that - contrary to fears

ments – a sufficient separation between private and business

Account access is ensured.

In detail, I was able to determine that each user has a uniform post

bank ID is obtained, with which both private and business accounts

can be managed. This Postbank ID has an extension

so-called "profiles" (sub-IDs). These are preset filters

to the granted access rights. Every user becomes everyone

Account owner whose accounts are being accessed assigned a profile. After

the user receives the login with Postbank ID and password for the created

business profile first a message with the name of the profile

and instructions for using the profile. The associated profiles

can be managed in profile management. There are all available

Profiles - divided into private and business profiles - are listed.

Postings can only be made with the associated accounts of the respective profile

be performed.

Switching between private and business accounts can be done in two ways

different ways happen, on the one hand through a so-called "indirect exchange

sel" and on the other hand by a so-called "direct change". The desired

Variant can be defined in profile management.

The default setting for access to a business account is on

“indirect change” provided. This means that when you log in next to

the Postbank ID, the profile name must also be specified in order to

view accounts. For a change to private or business con-

Users must first log out and then log out again

log in again. This default causes access to private

Accounts only via login with the Postbank ID and for business ones

Accounts only possible with the appropriate extension for each business account

is. Depending on the authorization, corresponding profiles are automatically created for the

affected customer created and this as a message in online banking

Introductory page communicated. In addition, the corresponding profiles are

line banking can be found in profile management. This variant guarantees

adequate separation between business and private accounts

and is therefore unproblematic in terms of data protection law.

Example: Mr. Smith's Postbank ID is "Smith1". the profile

company name is “Unt”. Then the login takes place in the private

account via "Smite1" and into the business account via "Smite-

man1#Under“. The business account password is the same as

for the private account. After logging in via "Smite1#Under", Mr

Mustermann exclusively the business account. In addition, the

Note "Logged in as #Unt".

It can also be set that a "direct switch" between

private and business profile takes place. This attitude must

actively select the users first. A separate login is included

Postbank ID and profile name no longer necessary. To profiles about the

To achieve a direct change, users must log in with the

Postbank ID (without profile name) on the profile icon and then on “Profile

switch". Then click on the corresponding profile.

It can therefore be switched directly between business and

be switched from a private account. Even then, a separate transfer

view of business and personal accounts. Although this variant

a lower level of protection under data protection law than the indirect change

offers, is nevertheless still a sufficient separation between private ones

and business accounts guaranteed.

Business customers are managed by Postbank via the Postbank procedure

Id advise. If both a personal and a business account have one

customers, it should remain with the indirect account switch.

I recommend employers to do this in a company rule

development for their employees. A request from the individual

employees, whether they also have a private account with the Postbank

dispose, however, is inadmissible under data protection law.

11.4

The right to cancellation of the client against the

Lawyer and the obligation to keep manual files

The right to erasure of the client's personal data

his lawyer according to Art. 17 Para. 1 DS-GVO often fails at the

legal retention obligation of six years for reference files

according to § 50 Federal Lawyers Act i. In conjunction with Article 17 (3) (b) GDPR.

I have received complaints in which clients want the deletion of the

requested personal data stored by their lawyers.

Art. 17 Para. 1 DS-GVO (right to erasure) gives the data subjects

and thus also the clients towards their lawyers

You also have the right to have your personal data deleted. However

does this right exist, e.g. then not to the extent that the processing is necessary for fulfilment

a legal obligation is required.

92

Economy, banks, self-employed

Article 17(3)(b) GDPR

(3) Paragraphs 1 and 2 do not apply if processing is necessary.

b) to fulfill a legal obligation that requires processing under the law of

Union or the Member States to which the person responsible is subject, or

to perform a task that is in the public interest or is being exercised

public authority delegated to the controller;

Section 50 of the Federal Lawyers' Act (BRAO) regulates such a legal

Obligation that the right to erasure of personal data of the

Clients limited to the lawyer.

§ 50 BRAO

(1) By keeping manual files, the lawyer must have an orderly and correct

of the picture about the processing of his orders. He has the reference files for them

to be retained for a period of six years. The period begins at the end of the calendar year

in which the order was completed.

(2) Documents that the lawyer obtains from the

Client or received for him, the lawyer has to his client

desire to release. If the client does not assert a demand for return,

the lawyer has the documents for the duration of the period according to paragraph 1 sentences 2 and 3

to keep. This retention obligation does not apply if the lawyer

contracting party has asked to receive the documents and the client

has not complied with this request within six months of receipt. The

Sentences 1 to 3 do not apply to the correspondence between the lawyer and his

Client as well as for the documents that the client already has in the original or

received a copy.

(3) The lawyer may request that the documents be handed over to his client

Paragraph 2 sentence 1 refuse until he because of the owed him by the client

fees and expenses are satisfied. This does not apply if the withholding according to the

circumstances would be inappropriate.

(4) Paragraphs 1 to 3 shall apply accordingly if the lawyer decides to conduct

Hand files or for storing electronic data processing documents

served.

(5) Regulations made in other regulations on storage and surrender

obligations remain unaffected.

Section 50 (1) sentence 2 provides for a six-year retention period for hand files

of the lawyer. With regard to electronically stored data, the following applies

this, insofar as the lawyer decides to keep the reference files or to

safekeeping of electronic data processing documents,

§ 50 paragraph 4 BRAO.

In the draft law for the implementation of the professional recognition directive and for

Amendment of other regulations in the field of legal consulting professions

(Bundestag printed paper 18/9521 of September 5th, 2016, p. 115) becomes the current version of the

§ 50 para. 1 BRAO with reference to the obligation to delete

DS-GVO explicitly stated that a data protection deletion request

claim of the client during the six-year retention period

is excluded.

Therefore, in these cases, I was only able to inform the petitioners that the

There is no entitlement to deletion in the case of reference files or documents

on the basis of § 50 BRAO at the lawyer within the deadline

be kept.

11.5

Unencrypted e-mail communication between lawyers

and client

Secure processing within the meaning of the GDPR also means in principle

the encryption of personal data; that may with regard to

electronic communication involves the encrypted sending of e-mails

mean. From January 1st, 2020, the legal professional law will be subject to certain

Prerequisites, however, that the unencrypted e-mail communication

between lawyer and client – without violating the professional duty

to secrecy – should be permissible.

Secure processing within the meaning of the GDPR includes, according to Art. 32

Paragraph 1 lit. a DS-GVO (security of processing) in principle also the

Encryption of personal data.

Article 32(1)(a) GDPR

(1) Taking into account the state of the art, the implementation costs and the way

the scope, circumstances and purposes of the processing, as well as the different

Likelihood and severity of the risk to the rights and freedoms of natural

Persons responsible, the person responsible and the processor make appropriate technical

and organizational measures to ensure a level of protection appropriate to the risk

guarantee; such measures may include, but are not limited to:

a) the pseudonymization and encryption of personal data (...)

With regard to electronic communication, this can be an encrypted

require ter email communication. From January 1st, 2020, the professional regulations will

for lawyers (BORA) in § 2 para. 2 BORA a relief for the

Economy, banks, self-employed

electronic communication between lawyer and client (Be-

Closing of the 6th Statutory Assembly at the Federal Bar Association

on May 6th, 2019 on the new version of § 2 BORA confidentiality).

Section 2 (2) BORA

(2) The duty of confidentiality requires the lawyer to protect the

Mandate confidentiality required organizational and technical measures

take measures that are risk-adequate and reasonable for the legal profession. Technical measures

Men are sufficient for this, insofar as they apply in the case of the applicability of the provisions of

Protection of personal data whose requirements meet. Other technical

Measures must also correspond to the state of the art. Paragraph 4 lit. c) remains

unaffected by this. The use of an electronic

public or other communication channel that involves risks for the confidentiality of these

Communication is connected, at least then permitted if the client agrees.

Approval can be assumed if the client uses this communication channel

proposes or starts and him after the lawyer at least lump sum and without

technical details pointed out the risks.

After that, the client can also send an unencrypted e-mail communication

tion expressly or impliedly under Section 2 (2) sentences 4 and 5 BORA

agree to the above conditions. The Client's Consent

however, cannot include the personal data of third parties.

In addition, the competent Federal Ministry of Justice and Consumer

pointed out that the future § 2 Para. 2 BORA will

lungs DS-GVO should not circumvent (Anwaltsblatt 2019, confidentiality:

§ 2 BORA new, p. 528). This means that the question of admissibility is unencrypted

E-mail communication between client and lawyer only in certain

from a legal point of view answered - the question of data protection law

Admissibility under the GDPR has not yet been clarified. However, can

the new professional regulation in the future in the data protection law

Evaluation of existing concrete facts are included.

Apart from that, according to § 29 paragraph 3 BDSG, my authority only has limited rights

investigative powers over lawyers, so that a general

my examination of the communication channels in general – especially with

Complaints from third parties – is not possible.

95

Debt collection, credit bureaus

12. Debt Collection, Credit Bureaus

Debt collection, credit bureaus

12.1

Implementation of the GDPR by SCHUFA Holding AG

The processing of creditworthiness information by SCHUFA Holding AG

(SCHUFA) usually has a significant impact on the persons concerned

gen. If creditworthiness information from SCHUFA contains an indication of a

limited creditworthiness, participation in economic life is more common

also limited. That's why I subject the SCHUFA to one

tightened control.

The creditworthiness reports reach particularly intensively into the economic ones

interests of those affected. The GDPR therefore contains strict

gifts. This meant that SCHUFA had a lasting impact on the validity

the DS-GVO had to prepare.

Already in 2016, the supervisory authorities dealt intensively with the effects

of the DS-GVO on the data processing of the credit agencies.

The most important questions were dealt with in several meetings and, as far as

if this was possible, a uniform national view was agreed. This concerned

especially the admissibility of the data processing including the scoring

Credit agencies according to the GDPR, which are used by all supervisory authorities

was deemed to continue. In addition, it affected the out

the information requirements resulting from the GDPR and the economic

information to be given to credit agencies. The information was due to the

Adapt and expand the regulations in Articles 13 and 14 GDPR.

In addition, the self-disclosures issued by SCHUFA had to be adjusted

become. The measures required under the GDPR were agreed with me

coordinated and fully implemented by SCHUFA.

The most essential effect of the SCHUFA through an elaborate

change in the process was to implement concerned the legal basis for

the transmission of data to SCHUFA and the issuance of information

ten. Before the GDPR came into effect, contractual partners

of SCHUFA by using what is known as a “SCHUFA Clause”.

Part of the contract is consent to the transmission of data to the

SCHUFA obtained. Since this consent in the vast majority of cases

also a prerequisite for entering into contract negotiations

was, this procedure would have violated the necessary voluntariness of consent

7 of the GDPR. The Effectiveness of Consent

would therefore have been more than doubtful.

97

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

As a result, the procedure had to be changed and a

to waive consent. According to all regulators forms

Art. 6 (1) lit. f) GDPR already provides a sufficient legal basis for

the processing of data by credit reporting agencies. A consent

tion is therefore not required. Will be based on obtaining consent

waived, it is also ensured that the data processing by

Credit agencies exclusively within the framework of the statutory regulations

lungs. The changeover is therefore advantageous for those affected.

SCHUFA then changed the procedure and waived the

Advantage of all data subjects since the GDPR came into effect

to obtain consent.

With the entry into force of the GDPR, the provision of the

Section 35 (2) sentence 2 no. 4 BDSG (old) no longer applies, according to which data is

credit bureaus usually after the end of the third year

storage were to be deleted. Due to the start of the period at the end of

year in which the storage took place, the storage lasted in all

Usually considerably longer than three years. Nevertheless, with § 35 para. 2

Sentence 2 No. 4 BDSG (old) a clear legal regulation on the storage

Duration of data stored by credit reporting agencies.

In the absence of legal regulations, one had to deal with the credit agencies

new retention period to be set. In accordance with Article 17 (1) (a) GDPR

data must be deleted if they are necessary for the purpose for which they were collected

are no longer necessary. Purpose of storage of data by host

credit bureaus is the examination of the creditworthiness of the persons concerned. Through

Credit rating information processed by credit agencies must therefore

be deleted at the latest when they have no reliable significance

have more for the credit rating. The credit bureaus were able to prove

that credit information for a period of at least three years

enable a reliable statement on the creditworthiness of the persons concerned.

Because of this, the credit bureaus through their association

“The credit agencies e. V.” Rules of conduct in accordance with Art. 40 GDPR

drafted, in which a storage period of three years was specified. The

The period contained therein begins with the storage of the data. data become

therefore already exactly three years after the completion of the event to which they

relate, deleted. The storage period was thus compared to the

previous storage period has been significantly reduced.

These are referred to as the "Code of Conduct" and on the website

http://www.handelsauskunfteien.de retrievable rules of conduct

not least because of the shortened storage period for the association

“The credit agencies e. V.” responsible state representative for data

data protection and freedom of information North Rhine-Westphalia in coordination with
approved by the other supervisory authorities. As a result, for those affected
created a shorter storage period and legal certainty.

12.2

The storage of data to carry out a
Insolvency proceedings after the residual debt has been discharged
credit bureaus

The meaningfulness of data for conducting insolvency proceedings
with regard to the creditworthiness of the persons concerned, the data storage
security by credit bureaus even after a residual debt
liberation.

The object of a large number of incoming complaints is that Aus-
future data for the implementation of insolvency proceedings
Save granting of an exemption from residual debt. The storage of
slow to completed personal bankruptcies restricts participation in
Economic life usually includes and implies problems that affect the
in many cases with the granting of the residual debt discharge
considered to have been overcome.

According to Art. 5 Para. 1 lit. e) GDPR, personal data may only be
be stored for a long time, as is necessary for the storage associated with it
purpose is required. If there is no need, the person responsible
according to Art. 17 Para. 1 lit. a) GDPR obliged to delete the data.

With regard to the storage period for data from insolvency proceedings
however, no concrete legal regulation.

The purpose pursued with the storage of data from insolvency proceedings
consists of assessing the creditworthiness of the persons concerned. consequently are
Delete data from insolvency proceedings at the latest when
can no longer be used to derive any reliable information about the creditworthiness.
Persons who have gone through personal insolvency proceedings are advised to
wisely more frequently in payment difficulties than other people.
This can also be attributed to the limited ability to build
Reduce reserves during the insolvency proceedings. resulting from it
resulting meaningfulness of data on insolvency proceedings for a not
insignificant period of time justifies the storage even after termination
of an insolvency proceeding.
As part of the voluntary code of conduct for credit bureaus, the
Storage period for data from insolvency proceedings standardized and

cretized. Based on the so-called "Code of Conduct" of the association "Die
credit bureaus e. V.", the credit bureaus have committed themselves to
Personal data from insolvency or residual debt exemption
run exactly three years after they end or after they have been issued
to delete the discharge of residual debt. The "Code of Conduct" was created by the
Checked by data protection authorities and assessed as compliant with the law.
Accordingly, there is no entitlement to an earlier deletion of corresponding data
Data.
It must be taken into account that data from insolvency proceedings
progressively less and less effect on the creditworthiness. The longer

a discharge of residual debt is behind, the better it develops

average creditworthiness of the persons concerned. Improved as a result

This is also associated with a calculated by a credit agency

Score value usually steadily with an increasing time interval

to the granting of a residual debt discharge.

100

Internet

13. Web

Internet

13.1

Data protection for new Internet services

In the development and design of new, innovative internet services

data protection law should also be observed from the outset. Change-

if there is a risk of difficult to resolve privacy issues

arise that require extensive changes or even the operation

of the service.

Through a press inquiry and reports in various media

I notice a service offered by a startup company

sam dedicated to the protection of children when communicating over the Internet

should serve. The startup company had, using artificial intelligence

(KI) developed a system that allows written communication over the Internet

(e.g. via instant messenger) and was able to recognize content therein,

which can be problematic for children.

Using this technology, the company offered an app-based service

communication that is potentially dangerous for children and young people or

communication partners (e.g. cybergrooming, sexting, etc.).

and informed the legal guardians of the specific danger. The parents
could register with the service for a fee and establish a connection
between the service and an app installed on the child's mobile phone
of a specific, widely used messenger. This became one
interface used by the provider of the messenger for its web
based usage provides. Once this connection was established,
de the child's entire communication conducted via this messenger
transferred to the server of the service provider and analyzed there by the AI.
If the algorithm found evidence that the communication for
the child's welfare could be dangerous, the legal guardians were
advised of this fact and to review the process and
requested support of the child.
Although the purpose of this service is of course welcome and
is worthy of support, its design also entailed considerable risks for
the personal rights of those affected.
The service was particularly problematic from a data protection point of view
by the fact that the entire communication conducted via messenger
automatically forwarded to the service provider and stored by them
and processed. This necessarily affected not only the municipalities
nication of the child supervised by his own parents, but also

those of its various chat partners. The electronically guided ones
Conversations fall under both telecommunications secrecy and
also under data protection law, as the chats regularly have a large number

contain personal data and also meta data (e.g. time

of communication etc.).

To make matters worse, the service is explicitly dedicated to monitoring min-

of age, whose chat partners are mostly other minors.

Children and young people enjoy special protection under data protection law,

since they are regularly not yet in a position to assess the possible consequences of

record data processing operations.

In the present constellation it is already difficult to process

the data or communication content of the child whose upbringing

entitled to use the service in accordance with data protection law

way to shape. Since other legal bases are not considered

come, the data can only with the consent of the child concerned

are processed. However, it depends on the age and the insight

ability of the child, whether they consent to the data processing themselves

can or whether the parents, as legal guardians, do this for the child

can or must. Questions also arise in this context

of transparency and the obligation to inform the child. Also are

various technical data protection requirements (e.g. encryption,

secure storage, timely deletion, etc.) must be observed.

Even more problematic, however, is the fact that the entire communication

communication of the chat partners of a monitored child to the service provider

forwarded and processed there. Without the child being monitored

or the parents who used the service to protect their child

However, the chat partners don't even realize that the service is there at all

was used and all communication with the monitored child

automatically sent to an unknown company and there

has been processed. Without this knowledge it was for the communication

partner also not possible to avoid the service, let alone in

sufficient form and after information has been given to the processing of your

validly consent to data. It would probably have significant changes

to the service in order to find a viable solution under data protection law

implement for this problem.

Answering or solving these data protection problems

Questions could ultimately be left open in the specific case, however, since the service

was discontinued by the provider for financial reasons. That was also

the data protection check that is still ongoing at this point in time is irrelevant.

102

Internet

The present example shows, however, that even the best and

welcome wish to protect children from certain dangers when using the Internet

protection, also unintentionally with a not inconsiderable risk

for the personal rights of the children and uninvolved third parties

can. Developers of new, innovative services are therefore well advised to

already during the development of the services their consequences under data protection law

to consider and to design the services in such a way that the privacy rights

the user will not be affected by this.

13.2

Cookies, plugins & tools: What applies to their use?

In almost every internet-based service today there are various small

Services and tools integrated that are not provided by the operator of the service itself,

but are offered and operated by other companies. Very

In particular, services for web analysis, advertising networks and

Plugins used to integrate external content. Many of these services are

however, it is problematic under data protection law.

There are a variety of different tools that the operators of inter-

net-based services (e.g. websites, mobile apps, smart devices etc.) in

Their offerings can embed various additional features

for themselves and/or their users. For example, often

Web analysis services are used, by means of which the service providers can obtain more precise information

Obtain information about the actual use of their offers in order to

to optimize and adapt them. Many operators also use

Advertising networks to advertise their own offer on other websites

or to be able to apply to portals. External content is also often used

(e.g. videos, maps, interactive elements), services (e.g. payment services)

or social plugins (e.g. like button) integrated. Such services and

As a rule, tools are not provided by the provider of an Internet service themselves,

but offered and operated by specialized companies and are

integrated into a large part of all internet-based services today.

responsibility

In principle, every provider of an Internet service is responsible for the

falling user data responsible. Most of the above services

from third-party providers, however, also collect and process personal

collected user data or enforce the transmission of this data

the service provider in advance. In particular, for the function of many of these

Third-party services the (often cross-service) recognisability

of a specific user (so-called tracking). For the provider
of a service that uses third-party tools, the extent of the data
data processing often only plays a subordinate role in these, since it
essentially on the achievement of the purpose of each used
Tools (e.g. embedding a video, better marketing, web analysis
etc.) arrives. Nevertheless, by integrating such
Third-party services are regularly jointly responsible for data protection law
the data processing carried out by them, since on his behalf
data of its users are automatically transmitted to the providers.

background

Even after the old legal situation before the GDPR came into force,
legal requirements for the integration of such services
way clearly. With the validity of the GDPR since May 2018, the legal situation is
however, has become even more unclear. Originally should coincide with the
DS-GVO the European ePrivacy Regulation come into force, with which the
European legislators have special rules for data processing in the
wanted to establish electronic communication. Because of political reasons
However, the legislative process has dragged on for years and
seems to have failed, at least for the time being. Through this
are currently many questions of data protection in electronic communi-
nification unregulated or unclear. The resulting uncertainty
among those responsible and those affected is also impressive
in the large number of complaints and requests for advice that I received in
have reached the reporting period in this regard.

Legal situation / orientation aid for providers of telemedia

To explain the applicable legal situation and the views of the

authorities on this subject, the Conference of Independent

pending federal and state data protection supervisory authorities

March 2019 the "Guideline of the supervisory authorities for providers of

Telemedia" (https://www.datenschutzkonferenz-online.de/

media/oh/20190405_oh_tmg.pdf). This contains detailed explanations

to which data protection rules in the opinion of the supervisory

authorities in the processing of usage data in the electronic

Communication currently applicable and what are the requirements for

the use of the above Services apply.

Since the previous rules for the processing of user data from the

Media Act (TMG) no longer applicable due to the priority of the DS-GVO

can be used and there are no other, more specific regulations,

Internet

is currently only the DS-GVO for the processing of user data

to use.

After that, the use of third-party tools can occur in certain cases

the legal basis of Article 6 (1) sentence 1 lit. f GDPR

and therefore also permissible without the consent of the user. However, this is

only possible if the processing of the user data by the respective

Service interferes with the rights of the user to a relatively small extent and

whose interests do not clearly outweigh those of the service provider. In the

Within the framework of the balancing of interests to be carried out, various

ne factors such. B. Transparency, possibility of objection by the user,

Scope of data processing, number of participants, etc. must be taken into account.

Thus, with appropriate data protection-friendly settings

This legal basis, for example, services for web analysis, which without

Cross-offer tracking get by, used or external content

Third parties are involved if this is done without tracking user activities

by the third party.

For Internet services offered by public bodies (e.g.

websites of authorities), the processing of user data is only possible

permissible if they are required for the administration in accordance with Article 6 Paragraph 1 Sentence 1 Letter e GDPR

the public task of the position is necessary. During websites

for public relations and certain content-related online offers

(e.g. e-government) are regularly required by authorities, this is

however, this is not usually the case when using third-party tools.

However, many third-party tools process user data in a

Way or to an extent that does not comply with Art. 6 (1) sentence 1 lit. f GDPR

is to be reconciled. This applies in particular to many tools for web

analysis, social plugins and almost all providers of usage-based

Advertising. The use of these services is only permitted if the respective

user has expressly consented to this. Obtaining a data protection

However, in practice, legally effective consent proves to be

difficult. For this it is u. a. required that users sufficiently above

be informed of the data processing and that the consent is voluntary

and given without coercion as well as through an active action of the user

is explained. The pure further use of an offer, clicking away from

Banners with the "close" button or pre-selected boxes

Declarations of consent are not sufficient in this respect. In addition, the services may

and tools, the use of which is to be consented to, only after this has taken place

be loaded or integrated into the internet service.

Conclusion

At present, the legal situation and reality in the case of such required consent

often diverged. Since the GDPR came into force

more and more internet services, so-called cookie banners and/or consent management

ment tools, but their content and technical function are often very

dubious and insufficient. It is to be hoped that the legislature

clear rules for data protection in electronic communi-

nication or at least some of the

open questions are clarified and more legal certainty is created.

13.3

Identification procedures of online portals

Identification procedures of online portals must have an appropriate

Have a level of security against unauthorized read attempts.

This year I received a complaint against a company

which gives customers the opportunity to view their data on the Internet.

The complainant explained that all personal data

were placed on the Internet via an online link. To access the data,

only 5-digit alphanumeric characters are necessary, which are attached to a

URL to be appended. The file number for the process appears

after calling the URL automatically. The password would be the zip code

of the customer requested. The data required for registration, URL and

Zip code and file number are sent as a sealed, enveloped letter

made available. The complainant complained that after calling

the URL as a password, only the zip code is requested and

therefore a high security risk.

I have asked the company to comment and

behavior as well as the organizational and technical measures in one

On-site appointment checked.

In doing so, I found that the individual short URL actually works with only five

appended characters are used at the end and through the further query

of the zip code is secured. This conception alone is

are not founded sufficiently because they are too short and too easy to overcome. experience

Tests from the past show that against short URLs, so-called

Brute force attacks are easy to perform. The same applies to

reading the zip code.

The brute force method is a popular way to break passwords or

find out data. To do this, she automatically tries different ones at random

sequences of letters or character strings. With increasing complexity and

length of the URL increases the number of arithmetic operations required for the

Brute force attack.

For an increased level of protection, therefore, there are usually at least ten

up to twelve characters.

Through my inspection, however, I was also able to determine that in the

further security measures have been taken in the present case, so that in

the overall view of the security measures from data protection law

view was sufficient. So the short URL was randomly generated and was immediately clicked

7 digits extended. To make a brute force attack fail,

security measures were also set in such a way that an automated

Monitoring the number of login attempts with a network

monitoring software, which immediately strikes when this number

significantly exceeds the usual. In this case, an attack is assumed

the website is disconnected from the network and the respective IT managers of the

company immediately informed. Even for the unlikely

event that an attacker discovers a valid login page

further IT security measures implemented, which make it possible to try out

Registration data prevents or reports and, if necessary, blocks the entry.

As a result, the organizational and technical measures taken

taken at an appropriate level of protection. In particular, the monitoring

In my opinion, it is essential to change the number of login attempts,

to ensure an adequate level of security.

13.4

Data protection-compliant use of web-based chat

applications

Visits to numerous websites accessible via the Internet are

Chat functionalities are offered to visitors. A minimalist

User interface often suggests clear and simple communication

cation concept, while various accompanying processes take place in the background

run. When providing such and comparable functionalities

responsible persons must pay special attention to the lawful

and transparent processing of personal data in good faith

Faith according to Art. 5 Para. 1 lit. a DS-GVO.

In the spring of the reporting period, I received a complaint against

the chat functionality on the website of a financial service provider. Over

This chat functionality gave visitors to the website the opportunity to

to contact employees of the service provider

and to find out about their offers, for example.

The user interface of the offending chat functionality was very

easy to set up. After entering a freely selectable name

the users to the actual chat interface. On this they stood

In addition to an input field for messages, there is also a send button

che available for sending the messages. The exchanged ones

Messages could be viewed through a conversation history. The

Structure of the user interface was obviously based on simplified

Form similar to that of common messenger applications.

For such a chat functionality it can be assumed that the users

expect them to enter their chat messages in the designated input field

can create and correct if necessary, as well as that one created by them

Chat message only when the send button is clicked

is transmitted to the communication partner. Only by pressing one

Such a button can also be assumed that a user in the

I consent to the transmission of the personal data from the input field.

The petitioner argued in his complaint that chat messages are not first

would be transmitted by pressing the submit button.

Rather, chat messages not intended for transmission and

directly after entering individual letters to the financial service provider

transmitted without the user being aware of it

be set. The petitioner provided corresponding information for his allegations

Supporting documents.

In response to the complaint, I performed in my IT lab

carried out a technical check of the chat functionality. As a result, could

I also accept the petitioner's allegation at the technical level of the trans-

understand the fer protocol. The chat functionality on the website of the

Financial service provider was set up in such a way that changes in the input field for

Chat messages sent to the financial service provider in near real time

became. It was not necessary to press the send button.

dumb. This transfer of personal data was for users in

The web interface of the chat functionality is not visible in any way. On

Based on the results of the technical analysis, I came to the conclusion that

that the chat functionality in this form was not GDPR compliant. She

violated the principle that personal data pursuant to Art. 5

Paragraph 1 lit. a GDPR in a way that is comprehensible for the user

need to be processed. In the present case was for processing

personal data in the context of the chat functionality as well

consent of the data subject in accordance with Article 6 (1) (a) GDPR

Internet

GMO required. Such consent was for the without actuation of

Personal data transmitted by the submit button is not provided.

I then asked the financial service provider to comment.

The financial service provider informed me that he had my legal opinion

with regard to the required consent in accordance with Article 6 (1) (a) GDPR

and its lack in the case of the data transmission in question. Further

he informed me that the objected partial functionality had been removed in the meantime

has been deactivated and thus a data transmission in the context of

Chat functionality only by pressing the send button

by the user achievements.

As part of the clarification of the facts, it turned out that the

nance service provider as the basis of its chat functionality no individual

development, but used the product of a manufacturer.

The manufacturer advertised the objectionable partial functionality for this product

explicitly on his website. For data protection-compliant use of these

and similar partial functionalities, however, bears responsibility in the specific case

literally according to Art. 24 DSGVO the responsibility. Therefore,

responsible already when choosing products and services, in

whose context personal data is processed is a special one

Pay attention to a privacy-compliant usability of the same.

After their selection form the specific configuration and design

of the context of use other essential building blocks in connection with

data protection through technology design and through data protection-friendly

Default according to Art. 25 GDPR.

Because of the use of the objected partial functionality of the principle

of Article 5 (1) (a) GDPR has not been observed and beyond

required consents pursuant to Article 6 (1) (a) GDPR were not available,

there is a violation within the meaning of Art. 83 Para. 5 lit. a DS-GVO. The processing

processing of personal data as in the present case can

Fulfill fines and will therefore after completion of the technical

Case test still to be checked and evaluated by my fines office.

technology, organization

14. Technology, organization

technology, organization

14.1

Relaunch of a customer portal on the web after a

protection violation

Those responsible according to Art. 24 DS-GVO often use contract processors

according to Art. 28 DS-GVO for the partial or complete realization and

the operation of processing activities. These processors

is, according to Art. 28 Para. 3 Letter c) DS-GVO, the seizure of all

according to Art. 32 DS-GVO necessary measures to ensure the

impose security of processing. Such contractual agreements

ments do not release the person responsible from the effectiveness of the

Measures regularly in accordance with Art. 32 Para. 1 Letter d) GDPR i. V. m.

Article 28 paragraph 3 letter c), f) and h) GDPR to review, evaluate and

to evaluate.

At the beginning of the reporting period I received a report of injuries

Protection of personal data according to Art. 33 DS-GVO

of a company in northern Hesse. A customer of the company

was it possible to use the company's web-based customer portal and

authorizes the personal data of a third party, i. H. of another

view customers.

The reason for the unauthorized disclosure of personal customer

dendaten was the inadequate authentication process in the customer portal.

Customers were sent the appropriate post to register on the customer portal

Access codes sent. The structure of such an access code

according to a fixed pattern. Did it occur when logging in to the web interface

area of the customer portal to an error, the returned error

In certain cases, a learning report can be used to draw conclusions about individual parts of the

access codes too. As a result, for an incorrectly entered

Access code the exact location to be determined for a successful

Registration had to be adjusted.

As part of the notification, the company announced that the procedure for

Generation of such access codes that are objectionable under data protection law

has been adjusted and the access codes already sent are unusable

were made. The report also stated that from view

the company's only one customer from the unauthorized disclosure

was affected.

111

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

Apparently, the measures taken were appropriate to the concrete

to fix personal data breaches and a

prevent future recurrence.

Technical external view

The customer portal affected by the report was

a web-based IT system accessible via the public internet.

In such cases, employees of my IT department regularly analyze

affected IT systems in the form of an external view. Here the

respective web interfaces are called up and the returned information

functions evaluated. This includes e.g. B.

– the recorded network traffic,

– Hypertext Transfer Protocol (HTTP) metadata and

- the Hypertext Markup Language (HTML) code of the returned

pages one.

Depending on the results, in-depth analyzes are carried out if necessary

performed. In the present case z. B. Error pages analyzed and

involved resources examined more closely. The aim of this approach is to

Impression of the underlying IT landscape and the people used in it

IT systems and the specific design of the website

to get. In the present case, i.a. two central IT systems

identified where there are signs of deficiencies in the security of the

Processing according to Art. 32 DS-GVO passed.

With a web server z. B. the display of a so-called

dard home can be effected. It contained a note that such a

side i i.e. R. would only appear if the corresponding web server is not

is configured appropriately. In addition, over

– the operating system used,

– the software on which the web server is based, including the version number,

and

– Installed components, also including version numbers, informed.

Such information should provide potential attackers with relevant clues

te deliver. It is therefore mandatory to display such a standard page

to prevent and is common practice when configuring

web servers.

For an application server, the display could have a standardized

Error page to be brought about. This included u. About

a used software framework, incl. version number. This

technology, organization

Information suggested that as the basis of the applica-

tion server, software that was more than ten years old was used. This

hasn't been provided by the manufacturer with security updates and

-Patches supplied. Such software can, particularly in the context of

IT systems accessible via the public Internet, not as the status of

Technology according to Art. 32 Para. 1 DS-GVO.

appointment on site

The above as well as other findings of the technical external view

led to further questions and indicated that the ones taken

technical and organizational measures were not sufficient to

according to Art. 32 Para. 1 DS-GVO a level of protection appropriate to the risk

to ensure. For further clarification of the facts, an in-

Analysis of the underlying IT landscape, the constitutive

IT systems and the associated technical and organizational measures

took required. An appointment was made for this at the business premises of the

those responsible, for the preparation of which my employees extensive,

Evaluate documents requested by the person responsible.

During the appointment, professional, technical and organizational topics were

connection with the customer portal and generally with regard to the enclosing

relevant data protection management at the responsible party. here

it turned out that in the context of the technical external consideration

identified IT systems within the IT landscape of the person responsible

were operated, but that all software-side maintenance activities

been outsourced to a processor in accordance with Art. 28 GDPR

were. This processor was also the

Manufacturer of the software on which the customer portal is based. at the appointment

no representatives of the processor took part, so that detailed questions

about the design of the systems could not be answered.

The results confirmed the indications from the technical field

consideration that was previously carried out on me. At the same time could

the organizational conditions that caused the situation,

be clarified during the appointment. Here it turned out that the

responsible had not taken sufficient measures to its

Obligations within the meaning of Art. 32 Para. 1 Letter d) GDPR i. in conjunction with Art. 28

Paragraph 3 letter c), f) and h) GDPR.

The appointment at the business premises of the responsible person went very

operational and productive. After the appointment, my colleagues

worked out a detailed summary of my findings

and sent to the person responsible for comment. The responsible

committed to implementing various measures to ensure safety

of processing in accordance with Art. 32 DS-GVO and to keep it permanent

ensure. This concluded a comprehensive and in-depth review of the

affected IT systems with the help of external support.

The results of the technical external observations by my employees

ter are fundamentally incompatible with a holistic security review

to equate. Your goal is to check from a technical perspective

whether there are any indications of processing that does not comply with the GDPR

result in personal data.

Conclusion

The employees of the IT department of my company regularly carry out technical

cal external observations of IT systems, e.g. B. related

with personal data breach notifications

according to Art. 33 GDPR. In the present case, the technical field

Considering strong evidence that technical and organizational

Measures taken by the person responsible were not sufficient to ensure the security of the

Ensure processing in accordance with Art. 32 Para. 1 DS-GVO.

The knowledge gained was about symptoms, whose

Causes within the scope of an appointment in the business premises of the responsible

verbatim were determined. It turned out that both technical

as well as organizational causes. A major problem lay

in the practical design of the relationship to a contract

better justified. This showed the great importance of the review

of the processor by the person responsible in accordance with Art. 28 Para. 3

Letter h) is to be attributed, even if the processor pursuant to Art. 28

Para. 3 letter c) contractually to take necessary measures according to

Art. 32 DS-GVO is obliged.

I would like the cooperative and productive collaboration with the responsible

literal in the present case. In an effective and efficient way

was it possible to significantly increase the level of data protection at the controller

increase and initiate processes that will further improve in the future

will effect. I also like the request of the person in charge

corresponded, jointly with him the present case at a meeting

to represent his association. This gave me the welcome opportunity

Manager of a trade association with similar technical solutions

with regard to necessary data protection requirements, evaluations

and to sensitize implementations.

The processor and manufacturer of the customer portal

lying software was integrated by the person responsible. This was true

technology, organization

in particular with regard to necessary adjustments to the

software used. The software is also used by the manufacturer for other

used by customers. In this context, I assume that the

necessary adjustments are also made available and included

these are implemented. Here I reserve the right to appropriate tests

to be carried out for other Hessian customers.

14.2

Decentralized data management and the rights of those affected

A decentralized management and processing of personal data can

Significant to ensure earmarking pursuant to Art. 5 Para. 1 Letter b

DS-GVO and data minimization in accordance with Art. 5 Para. 1 Letter c DS-GVO

contribute. At the same time, however, this results from decentralized data management

Challenges related to ensuring the rights of data subjects

according to Chapter III GDPR. This results, among other things, in the need for one

Comprehensive and early consideration of data protection in the

Conception and design of IT systems and landscapes in mind

of data protection through technology design in accordance with Art. 25 DS-GVO.

In the reporting period, I conducted an audit at a Hessian company

take that manufactures products for its customers.

The subject of the examination was the question of whether and, if so, in what form
(central or decentralized) the company personal data to the
processed by the products it produces. This was reason for me to
more intensively with the topic of decentralized data management in relation to the
address the rights of those affected.

The distributed data management

The starting point for the manufacture of a product is usually a purchase
contract, in the context of which e.g. the specifics of the specific product
being held. The corresponding personal data will be
for this purpose in the form of an order in a system provided for this purpose
Order processing is saved and kept available for further processing.
This is followed by production, at the end of which the delivery of the
products to the customer. Already related
with the production and delivery of customized products
personal data is transferred to other systems, e.g. B.
Production planning and control systems. As part of the delivery
personal data will then be transmitted to logistics service providers,
who act as processors in accordance with Art. 28 GDPR. After a

product has been handed over to a customer, it will be
sides of the manufacturer continues to be accompanied, e.g. as part of the product description
care and improvement as well as warranty and service.
During the life cycle of a customized product,
the manufacturer receives personal data for various purposes

raised and processed. Due to the long service life of the products

and the customer relationship that usually goes hand in hand with this comes in

A larger amount of personal data accumulates over time.

In the present case, the manufacturer opted for a largely decentralized system

data management in relation to personal data. here

the personal data relevant for the respective purposes

distributed to the purpose-specific IT systems and kept in them

and processed.

As a starting point, each of the IT systems requires personal basic

data to varying extents, depending on the respective purpose.

This data is usually obtained from the system mentioned above

related to order processing.

During the life cycle of a custom product it comes

to various events in which personal data

be practiced Examples of this are service contacts, repairs or the

Processing of guarantee cases. Depending on the relevance of the data for the respective

gene purposes and the existence of a correspondingly required

Legal basis is a distribution to the IT systems of the manufacturer.

The deletion of personal data also takes place at level

of the individual IT systems. Here, individually applicable

Deletion periods taken into account.

The rights of data subjects

To fulfill the information and notification obligations of the person responsible

as well as to exercise the rights of data subjects according to DS-GVO

by the person responsible to create the conditions and corresponding

Provide measures that address the specifics of decentralized data storage

take into account.

Provided that the underlying process of distribution

storage of collected personal data over a longer period of time

remains unchanged, there is the possibility that the

to carry out the above steps once. Subsequently, the determined

th information in the context of the collection of further personal

data are provided repeatedly. In cases of relevant changes

116

technology, organization

of the process, however, these changes must be compensated for by adjustments to the

information provided is reflected accordingly.

The information obligations according to Art. 13 and 14 DS-GVO must already

are met when collecting personal data. Already to this

Time must be determined, distribution and purposes of processing the data

stand. For this purpose, the individual target systems must be identified and

to determine and prepare the information relevant to processing.

Finally, a combination of the individual pieces of information is required.

To grant the right to information in accordance with Art. 15 DS-GVO, a

distributed data management, a process for identifying those IT systems

to implement the personal data on the data subject

process. As part of this process need for identified

IT systems all information required according to Art. 15 DS-GVO

be returned. Based on this information, a

compile and provide comprehensive information.

To grant the right to correction in accordance with Art. 16 DS-GVO, des

Right to erasure in accordance with Art. 17 GDPR and the right to restriction

18 DS-GVO are by means of corresponding

Processes to identify the affected IT systems. For each

These IT systems are then used to grant the respective

Take the steps required by law. Here are the according to Art. 19

GDPR to implement the required notification obligations.

To realize the right to data portability in accordance with Art. 20 DS-

GMO is analogous to in terms of determining the relevant information

Art. 15 GDPR to proceed. That is, according to Art. 20 Para. 1 DS-GVO

required compilation and processing of personal data

Data and any direct transmission between those responsible

according to Art. 20 Para. 2 DS-GVO are to be implemented technically.

The right to object according to Art. 21 DS-GVO is analogous to the

Articles 16 to 18 GDPR to implement.

implementation options

The concrete implementation of those presented in the previous chapter

Rights of the data subject must be in the form of appropriate data

protective legal accompanying processes take place. For the design of such

Processes have different options for those responsible. an essential

Another characteristic of a specific implementation is the degree of automation.

With an automated and largely technical implementation of the

According to Art. 15 DS-GVO, an IT-supported process, e.g.

contact all potentially affected IT systems. From these could then

all information relevant to a specific request for information can be called up

become. The processing of the information obtained could then

also be automated. The same applies to the subsequent shipment.

A manual and mainly organizational implementation of an

future process would have to adapt to the organizational structure of the responsible

chen as well as the assignment of processing activities and IT systems

Orient organizational units. In the event of a request for information

Art. 15 GDPR, all organizational units would have to be contacted, in

their context potentially personal data on the data subject

are processed. The organizational units must then manually

determine whether they actually process corresponding personal data

work. In this case, they would have to provide all relevant information

Gather and report information. Finally would have to

the reported information is brought together and the data subject

person to be transmitted.

When designing the accompanying data protection processes

Those responsible always take other framework conditions into account,

e.g. B. deadlines to be met or available mechanisms for determining the

Identity of data subjects. The two examples above represent two

opposite extremes in terms of the level of automation for

the implementation of accompanying data protection processes. In practice

the actual implementations are likely to move in between.

This is also the case in the case I examined. Like many other responsible people

the person responsible already had significant parts of his IT landscape in mind

the entry into force of the GDPR in use. From this it followed that the concrete

ten requirements from the area of the rights of data subjects

in accordance with Chapter III DS-GVO in the implementation of the processing activities

and the associated IT systems could not yet be taken into account.

Accordingly, the data protection regulations listed above were

sliding processes largely of a manual nature and by means of organizational ones

measures implemented. This resulted in, in addition to the comparatively

high effort for the manual implementation of the processes, including challenges

demands related to compliance with the relevant deadlines.

The influence of technology design

Art. 25 GDPR requires data protection through technology design and

through data protection-friendly default settings. In Art. 25 Para. 1 GDPR

it is specified that the person responsible both at the time of the

Determination as well as appropriate technical at the time of processing

technology, organization

and takes organizational measures to e.g. the rights of those affected

to protect people.

In principle, the GDPR does not require those responsible to ensure compliance

of the rights of the persons concerned, fully automated data protection

to implement accompanying processes. This applies in particular to the background

reason that the person responsible according to Art. 25 Para. 1 DS-GVO at the

Design of the measures, and thus also the data protection law

Accompanying processes, the state of the art, the implementation costs and

the type, scope, circumstances and purpose of the processing as well as

the different probability of occurrence and severity of the

Processing-related risks for the rights and freedoms of those affected

people must take into account.

Especially in complex and over a longer period of time

ten IT landscapes, the subsequent implementation of fully automated

accompanying data protection processes with significant implementation

be associated with costs. On the other hand, the implementation

predominantly organizationally implemented accompanying data protection processes

too high in each individual case compared to fully automated processes

lead to expenses. Both aspects should be considered in the concrete design

of the accompanying data protection processes are taken into account. here

the specific circumstances in the individual case play an important role,

e.g. B. the number of inquiries according to Art. 15 DS-GVO and the specifics

the IT landscape and the constituent IT systems.

It is recommended to use a strategy as part of data protection management

tegie for the realization and further development of the data protection law

to develop and implement accompanying processes. This can, for example, be a step

wise automation that both individual data protection law

Accompanying processes as well as individual IT systems are taken into account in a differentiated manner.

The coordination of such a strategy with a possibly existing one

Enterprise Architecture Management, an IT strategy and planned

IT projects should also be undertaken. For example, Syn-

energy effects are used if as part of an adaptation project for

an IT system also takes into account accompanying data protection processes

become. In projects for the realization of new processing activities and

accompanying data protection programs for the associated IT systems should

process as early as possible in terms of data protection through technology design

are taken into account.

For the duration of the existence of an accompanying process under data protection law

must be checked regularly. This applies to both that

technical as well as on the organizational environment of the process as well

with regard to the relevant processing activities.

Conclusion

A sensibly implemented distributed data management and processing of personal

personal data can comply with the principles of processing

support personal data in accordance with Art. 5 DS-GVO. this applies

in particular for the earmarking according to Art. 5 Para. 1 Letter b DS-GVO

and data minimization in accordance with Art. 5 Para. 1 Letter c GDPR. Even-

At the same time, this gives rise to specific challenges in relation to the

Protection of the rights of the persons concerned according to Art. 12 to 22 DS-GVO.

In connection with data protection by design according to

Art. 25 DS-GVO, these challenges must be taken into account accordingly

. With early and comprehensive consideration,

synergy effects are generally exploited. Conversely, one can

late consideration lead to considerable and avoidable costs.

A regular review of data protection law accompanying processes is

especially essential in dynamic environments.

14.3

Data protection requirements for system interfaces

In connection with several reports pursuant to Art. 33 DS-GVO, it must be determined

len that there are frequent violations of the protection of personal data

due to data leaks at system boundaries. This happens in particular

if those responsible according to Art. 24 DS-GVO carry out processing activities

Outsource processors in accordance with Art. 28 GDPR. For technical reasons

Better monitoring of the functionality of

Interfaces between IT systems and IT services to guarantee

data protection requirements in accordance with Art. 32 DS-GVO on a permanent basis.

With monitoring of system interfaces, the probability of

occurrence of personal data breaches

if appropriate measures are taken with regard to the results

be grabbed.

Technically implemented interfaces at system boundaries between IT systems

or IT services are also an expression of the agreements and regulations

between those responsible according to Art. 24 DS-GVO and contract

employees are implemented in accordance with Art. 28 GDPR. Inherent multilateral

Make connections between the IT systems used and IT services

from a technical point of view it is necessary that system boundaries and interfaces

technology, organization

are to be checked in particular by those responsible. One should

technical aim to control data flows on all system levels.

Because every IT system or every IT service has at least one

system boundary as well as at least one interface intended for use

Job. Only those provided interfaces should be accessed on provided

functionalities can be accessed.

Internal company or organizational monitoring should be carried out by the

be carried out precisely when corporate

or IT-supported processes are implemented across organizations.

Implementations of the respective IT systems or IT services must be compatible with the

mentioned agreements correspond and the responsibilities of a

Responsible for one or more processing operations according to

Art. 30 Para.1 DS-GVO are presented. Only if such agreements

If they are explicit and documented, they can be implemented correctly. After

their provision is the verification of processing in accordance with the

required. Likewise, such responsibilities are related

with the responsibilities of a processor (Article 30 (2) GDPR)

to see.

From a technical point of view, the design of the relationship between

Controller to his or even to several of his processors

to realize multilateral data security. On the one hand means

this is a separation of such responsibilities in the sense of clear definitions

(Art. 30 GDPR). On the other hand, to ensure functionality

of IT systems and IT services across companies or organizations

to appear fend. IT systems are used to implement IT-supported processes

or IT services integrated into a complex IT landscape. The security

the processing according to Art. 32 DS-GVO is therefore also company and

to ensure across organizations, in particular through suitable

and appropriate technical and organizational measures.

If a processor is also the manufacturer of the software used,

he has a significant influence on the technology design within the meaning of Art. 25

GDPR. This constellation results in special challenges,

to implement multilateral data security or a suitable and

to ensure appropriate monitoring by the controller.

Potential conflicts of interest should be avoided.

Company or organizational monitoring of system boundaries

zen and their interfaces are to be organized by a responsible person.

That means:

1. The monitoring of system boundaries requires a substantive consideration

tion and corresponding functional and non-functional definitions

of interfaces that comply with the data protection regulations mentioned above

requirements have to be met.

2. The actual implementation is against such interface specifications.

and their use in IT systems and IT services on a regular basis

to check, d. H. these are completed according to an agreed cycle

to monitor the person responsible, and not only in the event of

to inspect faults or even failures.

As part of this monitoring, the effectiveness must be taken

technical and organizational measures across system boundaries

be proven, e.g. B. the functionality across systems

to ensure further IT-supported processes.

3.

4. Results of such monitoring are to be protected under data protection law

evaluate.

5. Based on this data protection assessment, the person responsible should

lich, if possible in cooperation with the respective processor,

decide whether and, if so, which adjustments and improvements

at which levels are to be carried out, so that a data protection-compliant

me Processing of personal data using the IT systems

and IT services are guaranteed in the long term (Art. 32 GDPR). Therewith

should the agreements or data protection requirements

(Art. 24 GDPR in conjunction with 28 GDPR).

Furthermore, the results of these regular monitoring

the person responsible for a data protection reassessment

existing agreements on order processing or technical

nical-organizational measures in the event of major deviations

compared to the previously determined interface specification

become.

This procedure seems to be advisable because the recording

data leaks occur due to undesired side effects on system

interfaces between IT systems and IT services is to be avoided

functionalities are implemented in a distributed manner from a technical point of view. With respect to

the reports received pursuant to Art. 33 GDPR would exist for

controllers and processors the chance of such data leaks

to prevent Furthermore, it can be assumed that

also reduces the likelihood that a responsible person will

breach of the protection of personal data in accordance with Art. 33 DS-GVO

has to report.

122

technology, organization

14.4

Standard data protection model: Manual in version 2.0

The new manual 2.0 for the standard data protection model (SDM manual

book) provides guidance to controllers and their processors

how data protection requirements are divided into technical and

organizational measures to be implemented.

The SDM manual is available in an updated version (see the website of the

HBDI at https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/

SDM Method_V2.0a_0.pdf).

The entire text speaks to those responsible (Art. 24 DS-GVO) or contractual

workers (Article 28 GDPR) directly. That opens up the possibility for them

SDM for the implementation of data subject rights, also in combination with others

Procedures for the evaluation and realization of data protection regulations

Use requirements with, in and through IT. In the 47th activity report

I already presented how reference measures – so-called

Building blocks - the implementation of technical and organizational measures

(TOMs) can serve as well as the data protection test practice in the

Generally can be supported.

Version 2.0 has been restructured compared to the previous version.

Insofar as the processing of personal data to be considered is legal

assessed and declared acceptable in principle, is set out in the SDM Handbook

the further procedure for processing activities is shown step by step.

It consists of parts A to E.

Purpose of the Standard Privacy Model (Part A)

In Part A, the process model is presented with the aim of identifying suitable and

to take appropriate measures, so that particular rights

and freedoms of data subjects (Articles 12 to 15 GDPR).

are. In addition to the data protection assessment and evaluation of the

legal bases are to implement TOMs. Here, a transformation

mation performance, the corresponding TOMs both in design

of a system or a service (Art. 25 DS-GVO) as well as

makes it possible to ensure this in the long term (Art. 32 DS-GVO).

Interpretation of Technical Terms (Part B)

Part B provides interpretations of various terms with technical references.

For this purpose, 23 such terms are explained, which are used in the DS-GVO

find, such as identification, authentication, or recoverability

Remediate and mitigate data breaches. The here presented

selection of the terms used in the GDPR

the different level of abstraction of the technical ones to be treated

Requirements. Therefore, the selection and implementation of TOMs in

Reference to a specific processing activity of a more precise technical

subject to consideration using Part C.

Application of the protection goals according to DS-GVO (Part C)

Part C contains a subsumption of the selected 23 terms with technical

Reference to the known guarantee goals, which are also in Art. 5,

Art. 25 or Art. 32 DS-GVO can be found. These guarantee goals

include provisions on data minimization, confidentiality, integrity and

Availability. Furthermore, the protection goals of non-marketing

tion, transparency and the ability to intervene. Part C closes in

Section C2 of the SDM manual with a table showing a mapping of

Articles of the GDPR on guarantee goals. you are regarding

the implementation of data protection requirements trend-setting,

without the design options and degrees of freedom of actually on

limit the IT used over the long term.

Practical Implementation (Part D)

Part D aims at practical implementation. Specifications are in form

represented by generic measures that are based on common approaches in the

Refer IT (D1). This form of description makes it possible to

Representation of measures for each warranty objective in a technology-neutral manner. It will

further explains how the list of processing

activities of documentation, proof and own control

Those responsible and the processor regarding the TOMs taken

can serve (D2). Part D3 includes a new perspective on risks and

Protection requirements that both the corresponding DSK short paper and the

Working Paper 248 (Guidelines on Data Protection Impact Assessment

(DPIA) (wp248rev.01) available at the website of the Art. 29 Group (today:

European Data Protection Board, EDPB), https://ec.europa.eu/newsroom/

article29/item-detail.cfm?item_id=611236). basics of one

data protection management (DSM), as presented in the 47th activity report

now included in section D4. Furthermore, connections

such as planning and specification, implementation, controls and

of the permanently operated IT, the evaluation results

deliver and used through the record of processing activities

can become. Responsible persons and processors hereby receive a

technology, organization

Concept for a DSM cycle that will also organize their collaboration

can, so that finally the belonging to the processing operations

technical and organizational measures for systems and services on a permanent basis

are guaranteed (Art. 24, Art. 28, Art. 30 and Art. 32 GDPR).

Organizational Framework (Part E)

Part E describes the organizational framework. In addition

includes the interaction of SDM and BSI basic protection. It will be a

given insight into how the standard data protection model developed

was developed and is to be further developed.

Conclusion

With the application of the SDM manual 2.0, responsible persons receive

and processors very extensive support, the rights

data subjects with the selection of suitable and appropriate TOMs

according to the requirements of the GDPR.

14.5

Guideline of the European Data Protection Board on the subject

Blockchain

The use of blockchain is also currently being discussed in public

Technologies in very different areas of application, especially

discussed as cryptocurrencies. regulations on this technology

himself in work.

Since June 2019, the European Data Protection Board (EDPB).

Technology Expert Group1 and Finance Expert Group2 together

sam the mandate to develop a guideline on the subject of blockchain

granted. Under the leadership of France, this guideline regarding

of the various possible uses of blockchains as distributed

Ledger Technology3 elaborated. An employee from my IT department

collaborates on the creation. Other reporters come from Italy,

Lichtenstein and Spain, and also a representative of the European Data

protection officer is involved.

1 Technology Expert Group of the European Data Protection Board

2 Expert group Financial Matters of the European Data Protection Board

3

Technology used in its origin as distributed registers and today's applications

manure areas.

Technical Insights

From an initially technical perspective, this guideline describes the technical

technical requirements discussed. For this purpose, basics and different

various forms of blockchains explained. The basis of every blockchain is

a concatenated sequence of i. i.e. R. similar blocks over the entire

lifetime are updated. Each agency involved stores theirs

own copy of this chain with all blocks. Via a consensus mechanism

it is ensured that the identical chain is created for all participants.

The structure of a blockchain can be public or non-public. Out of

From the point of view of information technology, the difference lies primarily in the

Possibilities, who, under what circumstances, the structure of the blockchain

can copy and update themselves, d. H. in which way the consensus

mechanism just this produces. Thus, depending on the area of application and

to discuss application context,

– by whom the blockchain can be updated and

– who may or may not see the data stored in the blockchain;

i.e. H. should the data be freely available and therefore transparent, or should they

be confidential.

This results z. B. the question of whether a body that has such a blockchain
can update, is also responsible within the meaning of the DS-GVO. Out of
From a data protection point of view, the parties involved will be informed of their
answer and roles discussed.
Furthermore, it must be considered at which locations the blockchain
is saved. Therefore, with regard to the structure of a blockchain, its manipulation
ensure operational safety. The use of a consensus mechanism
must both ensure that only stakeholders who are authorized to block in
insert the chain as well as exclude the possibility of manipulation.
This is ensured by so-called validators. Valid
dators realized by solving mathematical puzzles, with what required
is that all blocks previously in the chain are checked at the same time
become. So if you can solve such a riddle, you have passed all the blocks.
checks and may insert a block itself. After inserting a block
is, this can no longer be changed, otherwise the principle would
of puzzle solving are undermined. The longer the chain in the block
chain is, the more computationally intensive it is to insert another block, since
every block in the chain must always be validated. – In non-public
Blockchains, there are now other consensus mechanisms that are more likely to
a vote e.g. B. based on majority rule. So they are less
computing time intensive.

technology, organization
Of course, from a data protection point of view, it is also a classi-
fication of the data in the blocks is essential. In this regard
– between data stored in blocks themselves, a so-called

called “pay load”, and

– Distinguish references to data, which means that they are not within the

Blockchain, but at a different storage location.

When data is kept confidential as a "pay load" in the blocks of a blockchain

are to be treated, then they are to be stored in encrypted form.

It is obvious that with a decentralized structure, even distributed in the network,

like the blockchain, IT security aspects to be dealt with specifically

also aim at the permanent operation of a blockchain.

Outlook: consideration of special applications of

Blockchains

The data protection criteria developed should be used as an example

special implementations of blockchains are applied. In addition

of course include different cryptocurrencies for which the

Expert group on finance a corresponding data protection law

assessment will be made. Furthermore, certain registers, such as

land registers, are considered. Furthermore, optimizations of factory

tion processes of interest if personal data is processed

become. Finally, in particular, the management of digital identities

viewed and evaluated under data protection law.

Conclusion

The technologically advanced development of blockchains and

of their diverse areas of application makes a data protection assessment

tion necessary. Here it is to be welcomed that the mandate of the EDPB

with a technical consideration under data protection aspects

was started.

fine proceedings, data protection violations according to Art. 33 DS-GVO

15. Fine proceedings, data protection violations according to Art. 33

GDPR

fine proceedings, data protection violations according to Art. 33 DS-GVO

15.1

fine proceedings in 2019

In the year under review, I had to carry out fine proceedings in which

also addressed issues of data breaches occurring in practice

unfortunately recurring. In the public sector, these are inappropriate

Data retrieval and/or improper use of data by employees

or employees. In the non-public area, non-ordering leads

by company data protection officers despite the obligation to order sanctions.

1.

Fine for so-called employee excess in the public sector

Also against employees in the public sector

fines may be imposed in certain circumstances.

That may be surprising at first glance, because Hessen has opposed the

Possibility in Art. 83 Para. 7 DS-GVO decided against authorities and

public authorities to be able to impose fines. Rather, it became

§ 36 para. 2 HDSIG explicitly included a ban on prosecution, according to which we

no fines against violations of Art. 83 (4) to (6) GDPR

Authorities and other public bodies are imposed.

An exception to this is to be made if the damaging

behavior of an employee to the public employer

is not attributable. As the two examples below show,

there are forms of employee excess that lead to fines against employees

ters and employees in the public sector.

Inappropriate data retrieval in the regulatory office

In one case, an employee of a public order office had a Hessian

City without official reason an electronic resident registration query

(Intranet information) and information on the data of a specific

th person requested. Due to a registered information block

according to § 51 Federal Registration Act (BMG) the person was informed about it in writing

informed that this employee of the regulatory office of this city

made a request for information. A letter of the same name was also sent

mailed to the person's husband's office.

The knowledge of the requested personal data was to fulfill

of the tasks incumbent on the employee of the public order office

conducive. There was no legal basis for the query and it lay

no consent of the data subject. Rather, they became

personal data obtained through this registration request

processed by the data subject for another purpose,

than for the purpose for which the data was originally collected,

used. The employee of the regulatory office has thus against that

Purpose limitation requirement of Art. 5 Para. 1 lit. b DS-GVO violate. Nonetheless

this violation is not attributable to the regulatory office. The employee

did the action from her workplace using the available

available work equipment committed, but not in the exercise of their

professional activity, but exclusively private. The employee is too

not qualify as a separate public body within the meaning of Section 2 HDSIG.

The violation was reported by me in accordance with Article 83 (5) (a) GDPR in conjunction with in conjunction with Art. 5 Paragraph 1 lit. b DS-GVO punished with a fine of 150 €. At the Zumes It was taken into account that only one person was affected by the situation was and so far no further data protection complaints templates. Fine reduction was taken into account that the case at the time the decision was already a year ago. That became a guide monthly net income added.

Improper use of data obtained for official purposes

As part of a data breach report by the chief of police Art. 33 DS-GVO I received notification that a police officer from Part of an official document, a criminal complaint, took a photo that in a so-called group chat of the instant messaging service WhatsApp has been set. The recording was captioned, off which showed that it was an advertisement by whom originated and the reason for which it was reimbursed. participant of Group chat were certain people of a club board. they all received the photo along with the comment.

The responsible clerk in my supervisory area reported this case to the fine office of my office. This opened after examination fine proceedings. It was stated that with the transmission of a Part of the criminal complaint to the members of the chat group personal data was processed for a purpose other than that for which the data was processed were originally collected. This violation was also the police department not attributable. The act was admittedly employed among other things of the work equipment available for official purposes, but not

fine proceedings, data protection violations according to Art. 33 DS-GVO

in the exercise of professional activity, but exclusively for private purposes

purposes. Therefore, the ban on prosecution under Section 36 (2) HDSIG applies

not one in this case and it is not a matter attributable to the department

appreciable behavior. The employee was also not considered their own public

body within the meaning of the HDSIG. It was due to a fine

recognized by 500 €. When measuring, it had to be taken into account that there was a

was a minor violation because only an excerpt from the criminal complaint was published

and only one person was affected. In favor of the person concerned was closed

take into account that so far there have been no data protection complaints

submitted against him. The fact that the

Incident has been fully admitted and the person concerned is responsible for his act

has excused. At the expense of the person concerned, it had to be taken into account that

he personal data by means of an instant messaging service that

forwarding of the message to a large address

satenkreis has transmitted to several people. Taken into account

was also the monthly income of the person concerned.

2.

Fine for not ordering an operational one

Data Protection Officer

The (erroneous) lack of appointment of an operational data protection

commissioned leads again and again to measures on my part.

A case that was still to be decided under the old data protection law led to

reporting year to a fine of €3,800.00. On the case was

I alerted by a complaint. A company objected

no internal data protection officer according to legal regulations

ordered. My investigations revealed, after a sluggish written

kehr that the company has a company data protection officer (bDSB)

should have ordered. After I had set a deadline, a da-

Tenant Protection Officer appointed. This order was objectionable, however,

because the bDSB has the necessary expertise according to § 4f paragraph 2 BDSG

a. F. was missing and there was a possibility of a conflict of interests. The ordered

Person was managing director of a subsidiary of those affected

Company and thus not sufficiently independent as a decision-maker.

As a result, a new internal data protection officer was appointed for the company

take ordered.

Since in the meantime a new legal situation has arisen due to the application of the GDPR

occurred, it had to be clarified first whether the new regulations of the DS-GVO

oppose a prosecution. That was not the case, even after validity

of the DS-GVO and entry into force of the new version of the BDSG on May 25th, 2018

was the non-appointment of a required data protection officer

moneyed. However, the sanction regulation according to § 43 Para. 1 No.

2 a. F. to be used, as these compared to the new regulation in Art. 83

Para. 4 lit. a GDPR i. V. m. Art. 37 Para. 4 S. 1 DS-GVO i. in conjunction with § 38 BDSG

n. F. the milder law i. S.v. § 4 para. 3 OWiG is.

For the assessment of the fine it was relevant that the negligently committed

ne administrative offense according to § 43 Abs. 1 Nr. 2 BDSG a. F. according to § 43 paragraph 3

BDSG a. F. was threatened with a fine of up to €50,000.00. the object

tive importance of the administrative offense was of average type, the
The seriousness of the offense committed was due to the significant
Duration, on the other hand, to be classified as above average. became aggravated
takes into account that the non-appointment gives the company a significant
any economic advantage has accrued. It's cost over more than
been spared seven years. The over-
lengthy procedure and the (only) negligent inspection are taken into account.
Another case that frequently occurs in practice, which leads to
can lead to a fine is the violation of the reporting obligation in the event of
a data breach according to Art. 33 DS-GVO. An example case is under clause 15.3
shown.

15.2

assessment of fines by the supervisory authority

On October 16, 2019, the DSK presented the concept for the assessment of fines
geldern presented to the public according to the GDPR. So far there was for
Information on Art. 83 Para. 1 and 2 DS-GVO a guideline (working paper
wp253), which deals with the interpretation of Art. 83 DS-GVO and such a
to ensure a uniform interpretation of the standard throughout Europe, and that
Short Paper No. 2 "Supervisory Powers and Sanctions" of the Data Protection
conference (DSK). This post deals with the current situation
to determine the fine.

On the way to the fine concept

The document wp253 was already the subject of the 46th TB (see para.
2.2.2). It essentially deals with the question of the decision of the
supervisory authority, whether a fine should be imposed. With that, however
the requirements of Art. 70 lit. k) GDPR for further guidelines for the

Supervisory authorities in relation to the application of measures under Article 58
Paragraphs 1, 2 and 3 DS-GVO and the setting of fines, in particular

fine proceedings, data protection violations according to Art. 33 DS-GVO
the amount of which has not yet been implemented. But they were the right steps
done in the right direction. The Article 29 group had, as in the 46th
TB reports at the November 2017 meeting from the Enforcement Subgroup
established a permanent task force, the Task Force Fining. to theirs
Main tasks include the harmonization of the calculation of fines
(https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610112).
The task force has been dealing with since its first meeting in December 2017
the harmonization of the sometimes very different practices in
the member states and discuss how to proceed.
A common Europe-wide framework for setting fines
there is no such thing as yet. Rather, the Member States have individually for
the transition period developed national approaches. So did the Netherlands
in Official Gazette No. 14586 of March 14, 2019 guidelines of the authority for personal
Sun-related data from February 19, 2019 to determine the amount of
Fines (Personal Data Authority Fines Guidelines
2019) published. In Germany, the DSK has dealt with the question of
monization of the assessment of fines at national level and a
first concept for setting fines for violations of the GDPR
based on the models from national antitrust law and
Securities and stock law drafted. The fine concept of the DSK was
under TOP 16 topic at the 2nd interim conference in June 2019 (protocol:
https://www.datenschutzkonferenz-online.de/media/pr/20190622_pr_mainz.

pdf). The majority of the DSK welcomed the concept as a suitable basis
for the assessment of fines and asked the AK sanctions, the
concept taking into account the practical experiences made with it
independent federal and state data protection supervisory authorities
to be further developed (16 in favor, 1 abstention, 0 against).
At the 3rd interim conference of the DSK on September 12th, 2019 in Mainz
the DSK with the question of the publication of the fine concept of the data
tenschutzkonferenz. The reason for this was the increasing number of inquiries about
sending of the draft of a fine concept created by the conference
from June 2019 (protocol: https://www.datenschutzkonferenz-online.de/
media/pr/20191126_protokoll_3_zwiko_2019.pdf).
The DSK felt compelled to review the concept for the assessment of fines
present in proceedings against companies. It is in Annex I, Section 3.1
printed and is available on the Internet in German at https://www.daten-
schutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf
or in English at https://www.datenschutzkonferenz-online.de/media/
pm/20191126_dsk_fining_concept_en.pdf available. A formal one

A resolution or decision by the DSK has not yet been made, so that
the concept is not binding in my view.
The published fine concept
The concept exclusively relates to the assessment of fines in proceedings
against companies within the scope of the General Data Protection
regulation (DS-GVO) in the territory of the Federal Republic of Germany. The

The concept is also neither for cross-border cases nor for others
EU data protection authorities binding. It takes place in particular
no application to fines against associations or natural persons
outside of their economic activity. Furthermore, it develops no bond
regarding the setting of fines by courts.
The DSK may at any time revoke, amend or extend its
decide on the concept with effect for the future. The concept loses its
Validity as soon as the EDPB issues its final methodological guidance
the setting of fines.
The calculation of fines according to the concept is based on the turnover of the
Company. The DSK is of the opinion that in a modern company
company sanction law with significant maximum fines, the
is aimed at a variety of different sized companies,
the turnover of a company a suitable, appropriate and fair
Connection to ensure effectiveness, proportionality and
represents deterrence.
Fines are assessed in proceedings against companies in five
Steps (see fine concept in Appendix I 3.1):
Step 1: First, the company concerned is
assigned to a size class,
Step 2: then the average annual turnover of the respective subgroup
the size class determined
Step 3: then a basic economic value is determined,
Step 4: this base value is determined by means of a
multiplied dependent factor and
Step 5: finally, the value determined under 4. is determined on the basis of

adjusted and other circumstances that have not yet been taken into account.

In the opinion of the DSK, the procedure guarantees a comprehensible,

transparent and case-by-case assessment of fines. So far the

Steps 4 and 5 sometimes considered too opaque by company representatives

were found to be barren, it must be stated that it is not the purpose of the concept

134

fine proceedings, data protection violations according to Art. 33 DS-GVO

to calculate the fine in advance. Steps 4 and 5 are subject to Art. 82 (1).

and 2 GDPR invoice.

DSK resolution on attribution

The fine concept of the DSK took an important step towards harmonization

subject to the fine according to DS-GVO. At the 97th Conference of Independents

Federal and state data protection supervisory authorities on April 3, 2019

the DSK passed the resolution "Companies are liable for data protection

shocks from their employees!” (see also Appendix I 1.1).

The background was that the old national liability rules had not yet been

have been adjusted to conform with the new legal situation. § 41 para. 1 of the

new Federal Data Protection Act (BDSG) refers to attribution

restrictive regulations in the OWiG. The national law with the underlying

underlying legal entity principle collides with European requirements and

also traditions. Under Art. 83 GDPR, companies are liable for

culpable violations of data protection by their employees, unless it is

is an excess. It doesn't require that for the plot

a legal representative or manager is responsible. This

Rather, liability for employee fault results from the application

of the so-called functional company concept of the European

march rights. The functional company concept from the contract on the
Functioning of the European Union (TFEU) states according to the definition of
The ECJ states that a company is “any person engaged in an economic activity
entity, regardless of its legal form and the way it is financed”,
is (ECJ in settled case law since case C-41/90 (Höfner and Elser),
1991 ECR I-1979, paragraph 21). Recital 150 of the GDPR points to the
Imposition of fines for data protection violations against companies
take it for clarification. According to the case law on the functional
Under the corporate concept, companies are liable for the misconduct of everyone
their employees. A knowledge of running a business
of the specific violation or violation of the duty of supervision is for
the assignment of responsibility is not required. actions of
Employees who, with reasonable appreciation, do not belong to the circle of the respective
can be attributed to entrepreneurial activity (“excesses”)
exempt.
With this resolution, the practice of the DSK is subject to one for the time being
deviating court decision clarified. The DSK had already
ment of the legislative process for the new Federal Data Protection Act
made the legislator aware that these provisions
135
The Hessian Commissioner for Data Protection and Freedom of Information
48th activity report on data protection
the requirements of the GDPR for liability for data protection violations
contradict. But so far without success.
It remains to be seen to what extent the agreements from the coalition
contract between the governing parties at federal level for modernization

of corporate sanctions law. This required modernization

of German corporate sanctions law would then also correspond to this

European antitrust law and the established international standard.

15.3

Fine after violating the 72-hour deadline for a report

according to Art. 33 DS-GVO by a rehabilitation clinic

The reason for the late notification according to Art. 33 Para. 1 DS-GVO

must be all the more sustainable the more serious the data breach is

and the longer the 72-hour period is exceeded. The information that employees

employees would not have known of the obligation to report, this is sufficient as a reason

usually not off.

initial case

At the end of 2018 I was injured in a rehabilitation clinic

Protection of personal data according to Art. 33 Para. 1 DS-GVO.

The point here was that a discharge report from a patient and

so that health data has been transferred to another patient.

The patient who had received the wrong letter in the mail informed the

Clinic by phone on a Friday about the incident. The notification according to Art. 33

Para. 1 DS-GVO to my authority through the clinic only took place seven days

later. As a reason for the late reporting of the incident, the

nik on the one hand that there was a weekend in between. On the other hand

such an error has not yet occurred in the clinic, which is why it has to

Failure to provide information on the part of those involved

employee had come.

Legal Assessment

The late notification constituted a violation of Art. 33 Para. 1 GDPR

The clinic justified the late notification, the reasoning

was insufficient in my opinion.

The GDPR does not provide any indication of the quality of the justification

refer to. However, it can be assumed that they will be all the more sustainable

must be, the more serious the data breach is and the longer it is

136

fine proceedings, data protection violations according to Art. 33 DS-GVO

72-hour period is exceeded (Jandt in: Kühling/Buchner, DS-GVO, Art. 33

16, 2nd edition 2018).

In view of the fact that a discharge report and thus health

data within the meaning of Art. 4 No. 15 DS-GVO to an unauthorized person

have become and that between the knowledge of the incident and

a week had elapsed since the notification was given, the reasoning was higher

to make demands. The clinic was particularly responsible for the fact that

they always keep their employees despite the validity of the GDPR since May 25th, 2018

had not yet been sufficiently informed of their duties.

I have the case because of the violation of Art. 33 Para. 1 DS-GVO

my fines office to check whether a fine has been imposed

Art. 83 DS-GVO given. The fine proceedings resulted in a fine

notice of fine imposing a fine of €6,800.

The fine is well within the lower range of the fine limit, since

various factors i. s.d. Art. 83 Para. 2 DS-GVO reduces the fine

could be taken into account. In addition to other factors,

verified that it was a negligent act that the facts

has been fully acknowledged that action has been taken to

remedy the data breach, as well as timely and unsolicited

Apologies to the patient.

Recommendation

In order to avoid late reports according to Art. 33 Para. 1 DS-GVO,

I recommend all responsible bodies to set up a procedure internally in writing

to determine how to proceed in the event of such incidents. The procedure

In particular, the instructions should provide information about:

- which people and departments when and how in corresponding

cases are to be involved (e.g. also the IT department),

– such as the substitution rules in the absence of individuals

are,

– how the reporting processes are to be carried out in detail.

It is important here that a corresponding document is not “dead” paper

is, but constantly evaluated on the basis of the experiences made and

needs to be revised/adjusted. The employee on a Friday

learns of a corresponding case, should in this way as best as possible

be informed and prepared, even if the majority of colleagues are not

is more present.

137

work statistics

16. Labor Statistics

work statistics

The statistical breakdown of the workload in "Facts and Figures"

(Section 16.1) follows the specifications of the data protection conference. The representation

is uniform nationwide and is u. a. the European Commission and

made accessible to the European Data Protection Board (Art. 59 DS-

GMO). However, it is only conditionally meaningful, since a detailed view

of things not done. Therefore, supplementing the usual detailed

Structure of labor statistics continued (Sections 16.2 and 16.3).

16.1

facts and figures

facts and figures

case numbers

01/01/2019

until

12/31/2019

a. "Complaints"

Number of complaints received under the GDPR in the reporting period

went. Such operations are considered complaints upon receipt

counted, which are received in writing and in which a natural person submits a

personal concern to which Art. 78 DS-GVO is applicable.

This includes duties. Telephone "complaints" are only then

counted if they are put into writing (e.g. by annotation).

b. "Consultations"

Number of written consultations. This includes summarily

Advice for those responsible, data subjects and the

own government.

Not: (telephone) oral consultations, training courses, lectures, etc.

c. "Privacy Breach Notifications"

Number of written reports.

i.e. “Remedial Actions”*

Number of actions taken

(1) according to Art. 58 Para. 2a (Warnings)

(2) according to Art. 58 Para. 2b (warnings)

(3) according to Art. 58 Para. 2c to g and j (instructions and orders)

(4) according to Art. 58 Para. 2i (fines)

(5) according to Art. 58 Para. 2h (revocation of certifications)

were made during the reporting period.

e. "European Procedures"

(1) Number of proceedings with concern (Art. 56)

(2) Number of lead proceedings (Article 56)

(3) Number of procedures according to chap. VII GDPR (Art. 60 et seq.)

5,081

1,610

1,453

(1)

1

(2) 13

8th

(3)

6

(4)

(5)

0

(1) 243

(2) 12

(3) 66

139

f. "Formal support for legislative projects"

Here, the total number from parliament/government is lumped together

called for and carried out consultations. this includes

also participation in public committees and opinions

to courts.

*In the year under review, 67 administrative offense proceedings were also initiated for violations of

the BDSG a. F. and the GDPR completed.

12

16.2

Additional explanations on the statistics “Facts and Figures”

The above figures only become really meaningful for my work

more precise specification and compared to the previous year. That's what they serve

the following table and the explanations. The numbers up to

or from May 25th, 2018, the day on which the DS-GVO came into force. The

calculated monthly average is intended for better understanding and

serve the purpose of comparability in view of the transition period in the previous year 2018.

The hope that the wave of complaints and requests for advice

will calm down after one and a half years DS-GVO, was only slightly fulfilled.

Had the total number of receipts to be processed increased in 2018 after the

almost doubled on the reporting date, 2019 was only a slight

noticeable decline. The excitement of last year is

given way to a more objective discussion of the new legal situation.

New focal points have emerged.

The front runner in this reporting year was the number of submissions that

data protection complaints against credit institutions. Because of

several data breaches reached me in the middle of the year within a few

Days approx. 650 complaints against Mastercard (see also Section I 11.2).

The number of submissions to credit agencies and collection agencies is consistently high

toot, above all to SCHUFA Holding AG (SCHUFA). That's why it stood

in the year under review particularly in the focus on data protection law (see also Section I 12.1).

There is a tendency towards an increase compared to previous years in the entries for

Theme complex electronic communication, telemedia, internet (social

media) to determine. There are increasingly critical questions about how to deal with them

with the rights of those affected by internet providers. This also applies in the area

of the schools, which is increasing with the request for advice in the IT area

(see also Section I 7.2) contact me.

The unbroken trend towards private video surveillance of home and property

continues to lead to corresponding complaints from neighbors, visitors

and passers-by.

work statistics

It is pleasing that the internal official and operational data

protection officers are obviously familiar with the new legal bases

have made. Here the requests for advice have decreased.

The telephone consultations reflect the inquiries, which are longer

than ten minutes lasted, found no written expression, however

could be dealt with in conversation. Here, as in previous years,

the value of the month of November, as a month without special events

se, extrapolated as an average value. On the other hand, the effort for the

Written settlement of 823 charges due to lack of jurisdiction in

Reporting year not shown separately.

The table below presents the amounts of inputs, complaints

and consultations in the year under review compared to the previous year:

141

Number 2018

01/01/2018 –

05/24/2018

~ 5 months

05/25/2018 –

12/31/2018

~ 7 months

Number 2019

01/01/2019 – 12/31/2019

= 12 months

areas of expertise

credit industry

credit bureaus,

collection

e-communication,

Internet

Schools, colleges, archives

video observation

Employee data protection

Traffic

Trade, crafts, trade

Company/official DPO

municipalities, elections

address trading, advertising

police, criminal proceedings, judiciary,

defense of Constitution

health, care

Clubs, associations

housing, rent

social

utilities

IT security, data processing technology

insurances

Radio, television, press

Data protection outside DE/EU

research, statistics

Aliens Law

taxation*

Other topics < 10

(e.g. religions, geodata,

chambers)

142

Submissions and Complaints

and consultations) / monthly Through-

cut value for comparison

54/10.8

118/23.6

178/25.4

533/76.2

120/24

414/59.1

78/15.6

amount in the

specialist topics

recorded **

59/11.8

296/42.3

amount in the

specialist topics

recorded**

197/28.1

39/7.8

30/6

4/0.8

52/10.4

71/14.2

104/20.8

142/28.4

16/3.2

148/29.6

40/8

48/9.6

30/6

17/3.4

4/0.8

0

10/2

0

4/0.8

134/19.1

275/39.3

468/66.9

172/24.6

161/23

153/21.9

397/56.7

323/46.1

248/35.4

62/8.9

76/10.9

54/7.7

35/5

21/3

5/0.7

4/0.6

2/0.3

7/1*

33/6.6

141/20.1

input

ben and

loading

difficult-

the

advice

tion

inputs and

complaints and

Consultations / monthly

average value

for comparison

949

923

512

56

253

199

240

182

16

115

174

129

101

57

54

50

76

30

46

46

3

10

3

1

33

10

19

52

312

95

131

39

58

219

112

6

32

180

77

66

63

22

57

17

1

6

1

8th

0

27

959/79.9

942/78.5

564/47

368/30.6

348/29

330/27.5

279/23.3

240/20

235/19.6

227/18.9

180/15

161/13.4

281/23.4

134/11.1

120/10

113/9.4

98/8.1

87/7.3

63/5.2

47/3.9

9/0.75

11/0.9

11/0.9

1/0.08*

60/5

BCR procedure

17

17/1.4

work statistics

32/6.4

630/90

1,253/250.6

Data breach reports

document total

ter submissions and advice

genes and data breaches

plus sum of telephone

consultations

Total entries

and consultations

*Essential areas of responsibility of the tax administration were transferred to the BfDI in accordance with Section 32h of the Fiscal Code.

** Video surveillance cases have been recorded independently since 2019.

14,382/1,198.5

9,725/1,389.3

3,673/734.6

7,338/611.5

1,453/121.1

4,986/712

4,739/677

7.044/587

2,420/484

The number of reports of data protection violations under Art. 33 GDPR

GMOs have increased from an average of 90 per month to 120 per month.

Of the total of 1,453 reports, the areas of banking,

Credit agencies, trade and commerce as well as the health sector am

most affected. The most frequently reported issues were:

Misdelivery by mail, fax and e-mail

Hacker attack, phishing, malware

Loss/theft of devices, data carriers,

Documents

557 cases

157 cases

(38.33%)

(10.81%)

148 cases

(10.19%)

In particular, extensive reports resulted from some of these reports

and time-consuming major consultations over several appointments. Pro-

Problems encountered, which the responsible persons concerned with their

internal data protection officers alone could not solve. This

concerned e.g. B. Public utilities, energy suppliers, libraries, larger schools

and a car park company.

Also demand from global companies for approval

of so-called Binding Corporate Rules (BCR) has increased significantly (see also Section I

3.2). With the BCR, the companies give themselves their own legally binding ones

and enforceable internal rules to protect personal information

Data to allow data transfers within the group of companies

Third countries that in and of themselves do not have an adequate level of data protection

offer to enable. These rules must be in a Europe-wide co-

operational procedures, i.e. by data protection supervisory authorities of several

Member States, can be examined together and after successful

positive opinion of the European Data Protection Board

the so-called lead supervisory authority with binding effect for the

be approved by other authorities.

For all 17 BCR procedures listed in the table, my official

is the lead supervisory authority for Germany and in eight of these

Procedure also in charge throughout Europe as the so-called BCR Lead.

In the year under review, there was also an increased need for advice and training

Requires on topics of the General Data Protection Regulation, the newer draft

developments and the associated IT issues. In numerous seminars and

lectures was given by my employees

specific specialist topics (e.g. on fine procedures, on the rights of those affected,

on data breaches and precautionary measures, on the international

data traffic) to users and interested parties. So had e.g. Legs

Colleague of mine also opportunity to speak in the Council of Europe at the Conference of

Children's Rights Convention on the Application of Microsoft 365 in Hessian

present to schools.

Furthermore, three trainee teachers were appointed to their administration

training stations.

16.3

sanctions

At the end of the reporting period, 80 fines had been initiated

drive. In the reporting period, a total of 67 administrative offenses

procedures, which 32 violations of the BDSG a. F. and 35 violations after

GDPR are based on. So that despite the with the

Effectiveness of the DS-GVO ongoing considerable workload

most backlogs from previous years plus some procedures over

Violations according to DS-GVO are finally processed.

A total of six procedures ended with a fine notice

and fines totaling EUR 19,500.00.

The completed proceedings were followed by a breach of supervisory duties

§ 130 OWiG for violation of § 34 BDSG a. F., contrary to § 4

f BDSG a. F. failure to appoint a data protection officer,

Late reports according to Art. 33 GDPR and violations of Art. 5 and 6

DS-GVO based.

16.4

Development of the number of reports according to Art. 33 DS-GVO since the 25.05.2018

In my 47th activity report, under item 4.11.3 the topic “Notifications of personal data protection violations

Data” (hereinafter Data Breaches) is presented in detail. In this 48 activity report, I focus on the development of the number of reported data breaches since 05/25/2018 and the possible reasons for this development.

In 2018, there were 630 cases of "data breaches" according to Art. 33 GDPR been reported. Because this over a period of just over seven months, there were almost 90 reports per month. In the 47th activity report, I therefore had around 1,000 reports for 2019 forecast.

In fact, that number was significantly surpassed in 2019. So are im In 2019, a total of 1,425 reports according to Art. 33 GDPR at my authority received. The messages thus move on a German much higher level than in 2018. In the year under review, I was able to recorded almost 120 reported "data breaches" and thus compared to In 2018 about 30 more events per month than in 2018 (in comparison: 90 per month in 2018).

The high number of reports naturally leads to one in my agency significantly higher workload, as each report is checked individually must. Even similar cases cannot be evaluated across the board. Rather, the circumstances of each individual case must be taken into

and the measures taken must be comprehensively checked.

The reasons for this significant increase in reported cases (>33.33%)

are complex. Since May 25, 2018, those responsible have had more

Can and tend to gain experience with the interpretation of the GDPR

meanwhile, irregular occurrences are also referred to as "data breaches".

to identify and report accordingly to the supervisory authority.

On the other hand, the increase is certainly due to the content of the standard itself.

For example, the requirements for a duty to report to the supervisory

trigger authority, significantly lower threshold than under the old BDSG (cf.

TB 47, point 4.11.3).

In addition, cases are currently being reported, albeit in small numbers (below 2%),

where the requirements of Art. 33 GDPR are not met. At

In such cases, those responsible will receive appropriate feedback

notification by my authority explaining the reasons for this

the reported fact is not reportable.

In addition, the regulation of Art. 83 Para. 4 lit. a) DS-

GMOs play a role in relation to the reporting behavior, since the omission of the

Notification of a reportable fact to the supervisory authority

is subject to a fine. The same applies to late reports as well as a

possibly disregarded documentation obligation of those responsible,

if, after a review and risk assessment, a report has been

is seen.

After all, it can be said that the high level of the previous year

the number of reported data breaches has increased again

beyond the forecast level.

17. Balance Sheet Reports

Balance Sheet Reports

17.1

The Hessenbox project is basically complete

The Hessian universities and the Hessian Ministry for

Science and art since 2016 pursued "Project Hessenbox",

a cloud storage solution that uses it across universities

enables documents to be made available in a secure manner, among themselves

exchange or work on together is within the scope of the data

protection assessment completed. With my participation and

after a series of meetings over a period of more than three years

with the carriers of the procedure and corresponding processing activity

was able to reach an amicable and data protection bill

supporting solution for the document management and communication

system can be found. For university administrations and teachers

as well as for the students, an instrument has been created that

is unique in this form in Hesse.

I have detailed information about the project in the 46th activity report (item 16.1).

reported. Since that time, other meetings have taken place,

which have now led to a conclusion under data protection law. Included

was considered by me that an additional functionality with names

"OnlyOffice" implemented in the Hessenbox application at short notice

became. The manufacturer of this software is Ascensio System SIA with headquarters in Riga, Latvia. OnlyOffice is an optional feature, which are integrated into the software solution PowerFolder (see also 16. TB, 16.1) can be integrated and activated. Terms and Conditions for Use of the OnlyOffice Integration Edition can be found at https://help.onlyoffice.com/products/files/doceditor.aspx?fileid=4995927&doc=bTNVWUNPTm1yM-zlRW9Eb3o1MityMWJRNGlzcTFCZFlxdFRLbEFLdmVOcz0_IjQ5OTU5Mjci0 (last accessed: 01/14/2020). A privacy statement in English from the manufacturer of OnlyOffice can be found on the web at https://www.onlyoffice.com/blog/2018/05/how-onlyoffice-complies-with-gdpr/ (last accessed: 01/14/2020), in which also some questions about data security are answered.

A corresponding German-language adaptation is included in the terms of use expected from the respective university.

With the help of OnlyOffice, Hessenbox users can also of- display fice documents directly in the browser and also col- laboratory with others (to access the document in the Hessenbox

authorized) users are working on a document. are for use separate licenses and your own server required.

The OnlyOffice server is operated centrally at the University of Giessen and used by all operator locations. This will be the case when using the function Document to the OnlyOffice server for display or collaborative Work transferred and again at the operator's site after completion

(versioned) saved. The transfer of files between the

orten only finds SSL-encrypted (TLS 1.2 or higher) via the

Hessen network (VPN) instead. The transmission for presentation and during the

Processing in the browser is also SSL-encrypted (TLS 1.2 or higher).

The Hessenbox project management was able to tell me about the added value of the application

for the users of the Hessenbox. Since in this together-

hang no negative impact on data protection and data security

are to be feared, I have the extension of the application Hessenbox

consented to the OnlyOffice functionality.

Over the years, both the representatives of the project

participating universities as well as those of the Hessian Ministry of Science

society and art competently and purposefully the high demands of the

data protection components. What made it even more difficult was that

in the course of the project, the General Data Protection Regulation became effective

scored This meant, among other things, that the procedure directories created so far

Section 6 of the Hessian Data Protection Act (old) on processing directories

Art. 30 DS-GVO to rewrite or the information i. S.v. Article 13

and 14 DS-GVO to improve or expand. In this together-

The working group has created documents that describe the processes

in order to meet the increased requirements of the GDPR.

These documents can be used for further, especially cooperation projects

serve as a template in the area of universities and on a larger scale

be reused. The constructive cooperation of the

ungsträger has made a decisive contribution to the cross-university

to lead Hessenbox to a successful conclusion.

17.2

The transnational project "Digital learning on the go"

takes more hurdles

The "Digital Learning on the Go" (DigLu) project, which takes care of the

aims to improve the school careers of children of occupational travelers

start as a pilot process.

148

Balance Sheet Reports

In the past activity reports, I have regularly reported on the progress

steps in the development of the transnational project DigLu (Di-

gitales learning on the go) reported (see 47th activity report, No. 5.1 and

46th activity report, Section 9.2). The data protection requirements

to the pilot project were enormous (see 46th activity report, point 9.2.3),

could, however, from the project group DigLu, a transnational

Working group led by North Rhine-Westphalia, step by step

be implemented.

The current efforts apply to a contract for order processing

according to Art. 28 DS-GVO, which the countries involved in the pilot project or

Education ministries are to conclude with the service provider Jordy Media.

The special feature here is that both the countries and the

Schools contractual partner of the service provider who runs the software and in a

The hardware (i.e. the data center service) is subcontracted to

provides are. It is planned to offer schools online as part of the

Registration for the procedure to allow the conclusion of the contract during

the ministries implement this in classic written form.

The DigLu project group plans to start the process in the 2020 summer school year

to roll out individual process steps. The technical, administrative

ven and data protection parameters for the operation of the process

are formulated and written down in a procedural documentation. The

Question whether a data protection impact assessment (DPIA) according to Art. 35 DS-

GMO is required is largely decided by the type and content of the

personal data of the students that are processed with DigLu.

In the first implementation phase of the pilot, the data content is on

Minimum reduced so that a DPIA appears obsolete. Should go to one

later date e.g. B. the data can be expanded or the process

change in content, a re-examination with regard to the required

required to carry out a DPIA.

The project, designed as a pilot for two years, is scheduled to end after the first

be evaluated in order to draw possible conclusions for the further

ren operation of the method and its extension to others

to let countries happen. Finally, in the years to come

the countries not yet involved can join the procedure.

149

Appendix I

Privacy Policy Materials

Appendix I - Privacy Materials

Appendix I - Privacy Materials

1. Resolutions of the Conference of Independents

Federal and state data protection supervisory authorities

1.1

Resolution of the 97th Conference of Independents

Federal and state data protection authorities

April 3, 20191 - Companies liable for data protection violations of their

employees!

Companies are liable within the framework of Art. 83 General Data Protection Regulation

(DS-GVO) for culpable data protection violations by their employees, provided that

is not an excess. It is not necessary for that

Act a legal representative or manager responsible

is. Attribution-restricting regulations in national law would

contradict that.

This liability for employee fault results from the application

the so-called functional company concept of the European

primary law. The functional company concept from the contract on

the functioning of the European Union (TFEU) states that a company

take any economic entity regardless of its legal form and

the nature of their funding. Recital 150 of the GDPR indicates for

the imposition of fines for data protection violations against companies

take it for clarification. According to the case law on the functional

Under the corporate concept, companies are liable for the misconduct of everyone

their employees. A knowledge of running a business

of the specific violation or violation of the duty of supervision is for

the assignment of responsibility is not required. actions of

Employees who, with reasonable appreciation, do not belong to the circle of the respective

can be attributed to entrepreneurial activity (“excesses”)

exempt.

The old national liability rules have not yet conformed to European law

adapted to the new legal situation. Incorrectly refers to § 41 para. 1 des

new Federal Data Protection Act (BDSG) on attribution-restricting

Regulations in the OWiG. The independent data protection supervisory authorities

of the federal and state governments (DSK) have already

drawing attention to the new Federal Data Protection Act

made sure that these provisions meet the requirements of the GDPR

Objecting to liability for data protection violations.

1 Against the votes of Bavaria and Baden-Württemberg.

In this respect, the DSK welcomes the fact that the coalition agreement provides for the

to change the general right of operation for companies in German law in such a way that

“Those who benefit from misconduct by employees

companies will be sanctioned more severely". This required modernization

of German corporate sanctions law would then also correspond to this

European antitrust law and the established international standard.

The DSK therefore calls on the federal legislature once again to

provisions of the draft of the Second Act to Adapt the Data Protection

right to the Regulation (EU) 2016/679 (DS-GVO) and to implement the

Directive (EU) 2016/680, §§ 30, 130 OWiG clarifying the application

area and thus adapt it to European law.

1.2

Resolution of the 97th Conference of Independents

Federal and state data protection supervisory authorities

Hambach Castle – April 3, 2019

Hambacher Declaration on Artificial Intelligence

Seven data protection requirements

Artificial intelligence (AI) systems pose a substantial challenge

development for freedom and democracy in our legal system.

Developments and applications of AI must be democratic and constitutional

way comply with fundamental rights. Not everything that is technically possible

and economically desired may be implemented in reality. The

applies in particular to the use of self-learning systems,

who process masses of data and use automated individual decisions

encroach on the rights and freedoms of those affected. The respect of

Fundamental rights are the task of all state authorities. essential framework

Conditions for the use of AI are to be specified by the legislature and

to be carried out by the supervisory authorities. Only if the protection of fundamental rights

and data protection keeping pace with the process of digitization is

a future possible in which, in the end, people and not machines will prevail

people decide.

I

Artificial intelligence and privacy

“Artificial Intelligence” (also “AI” or “Artificial Intelligence” – “AI”)

currently being discussed intensively, since they create new value in many areas

promised by the economy and society. The federal government has one

AI strategy published with the aim of making Germany a world leader

to the development of AI. "AI made in Germany" should simultaneously

ensure that even with extensive use of artificial intelligence

the fundamental values and civil liberties that apply in Germany and the EU,

continue to play the formative role in our coexistence. The independent

gigantic data protection supervisory authorities of the federal and state governments

this approach of designing AI in a way that is compatible with fundamental rights.

A generally accepted definition of the term artificial intelligence

does not exist yet. According to the understanding of the federal government, it is possible

with AI it is about “designing technical systems in such a way that they solve problems

work independently and thereby adapt themselves to changed conditions

can adjust. These systems have the property of new data

to ‘learn’ […].”2

For example, AI systems are already being used in medicine to support

used in research and therapy. Neural networks are already in

capable of automatically recognizing complex tumor structures. AI systems

can also be used to diagnose depression based on

behavior in social networks or based on voice modulation

Recognize the use of language assistants. In the hands of doctors

this knowledge can serve the well-being of the sick. in the wrong hands

however, it can also be misused.

An AI system has also been developed to evaluate application documents

used with the aim of making decisions free of human prejudices.

However, the company has so far had predominantly male applicants

ber hired and the AI system with their successful applications

trained. As a result, the AI system rated women much worse,

although gender is not only not a predetermined evaluation criterion,

but was even unknown to the system. This reveals the danger that

discrimination depicted in training data is not eliminated, but

be solidified.

These examples make it clear that with AI systems, personal

personal data are processed and this processing risks for

human rights and freedoms. They also show how important

it is political, social, the development and use of AI systems

and legal support. The independent data protection supervisory authorities

2 BT-Drs. 19/1982 to 1.: The Data Ethics Commission of the Federal Government also raises as

important basics for AI pattern recognition, machine learning and methods

of heuristic search, inference and action planning (recommendations

the data ethics commission for the artificial intelligence strategy of the federal government,

9.10.2018).

of the federal and state governments understand the following requirements as one

constructive contribution to this central socio-political project.

II.

Data protection requirements for artificial intelligence

For the development and use of AI systems in which personal

related data are processed includes the basic data protection

regulation (DS-GVO) important legal requirements. They are for protection

the fundamental rights and freedoms of natural persons. Also for AI systems

teme apply the principles for the processing of personal data

(Art. 5 GDPR). These principles must be carried out in accordance with Art. 25 DS-GVO

Technical and organizational measures planned at an early stage by the

be implemented by those responsible (data protection through technology design).

1. AI must not objectify people

The guarantee of human dignity (Art. 1 Para. 1 GG, Art. 1 GRCh)

offers that, especially in the case of state action using AI, the individual

is not made into an object. Fully automated decisions

or profiling by AI systems are only permitted to a limited extent. decision

ments with legal effect or similar significant impairment

must not be left to the machine alone in accordance with Art. 22 GDPR.

If the scope of Art. 22 DS-GVO is not open, take effect

the general principles of Art. 5 DS-GVO, which in particular with the

principles of legality, accountability and fairness

protect the individual. Those affected also have

men the right to the intervention of a person (intervenability).

expressing their point of view and contesting a decision.

2. AI may only be used for constitutionally legitimate purposes

and do not revoke the earmarking requirement

It also applies to AI systems that they are only too constitutionally legitimized

purposes may be used. The principle must also be observed

of earmarking (Art. 5 Para. 1 lit. b DS-GVO). Purpose changes are with

Art. 6 Para. 4 GDPR sets clear limits. Also with AI systems

extended processing purposes with the original purpose of collection

be compatible. This also applies to the use of personal data

Training purposes of AI systems.

3. AI must be transparent, understandable and explainable

Personal data must be in a manner appropriate for the person concerned

be processed in an enforceable manner (Article 5 (1) (a) GDPR). This

requires, in particular, transparent processing in which the information

Information about the process of processing and possibly also about the used

Training data is easily accessible and understandable (Article 12 GDPR).

Decisions made based on the use of AI systems,

must be understandable and explainable. The ability to explain is not enough

With regard to the result, moreover, the traceability must be

with regard to the processes and the making of decisions

to be guaranteed. According to the GDPR, this is also about the involved

explain the logic sufficiently. These transparency requirements are

to be fulfilled continuously if AI systems for the processing of personal

related data are used. The accountability of the

Responsible (Art. 5 Para. 2 DS-GVO).

4. AI must avoid discrimination

Learning systems are highly dependent on the inputs

Data. Inadequate data bases and concepts can lead to

Results come that have the effect of discrimination. discriminatory

processing constitutes a violation of the rights and freedoms of

data subjects. You violate i.a. against certain requirements

of the General Data Protection Regulation, such as the principle of processing

good faith, the connection of the processing to legitimate purposes

or the adequacy of the processing.

These tendencies towards discrimination are not always recognizable from the outset.

bar. Therefore, before using AI systems, the risks for the

rights and freedoms of

Individuals are evaluated with the aim of including covert discrimination

reliably ruled out by countermeasures. Also during the

Appropriate risk monitoring must be carried out when using AI systems

take place.

5. The principle of data minimization applies to AI

Large stocks of training data are typically required for AI systems

used. The following also applies to personal data in AI systems

Principle of data minimization (Article 5 (1) (c) GDPR). The processing

Processing of personal data must therefore always be limited to what is necessary

be limited. The necessity test may show that

the processing of completely anonymous data to achieve the legitimate

purpose is sufficient.

6. AI needs accountability

Those involved in the use of an AI system must take responsibility

determine and communicate clearly and the necessary measures in each case

meet to ensure lawful processing, the rights of data subjects, security

to ensure the processing and controllability of the AI system

afford. The person responsible must ensure that the principles according to

Art. 5 DS-GVO are complied with. He must respect his duties

fulfill the data subject rights from Art. 12 ff DS-GVO. The responsible

must guarantee the security of the processing in accordance with Art. 32 DS-GVO

and thus also manipulations by third parties that affect the results

of the systems affect, prevent. When using an AI system, in

which personal data is processed is usually a

Data protection impact assessment according to Art. 35 DS-GVO may be required.

7. AI requires technical and organizational standards

In order to ensure data protection-compliant processing,

reception and use of AI systems technical and organizational

to take measures according to Art. 24 and 25 DS-GVO, e.g. B. pseudo-

anonymization. This does not happen solely because the individual is in a

large amount of personal data seems to disappear. For the

Data protection-compliant use of AI systems currently still exists

no special standards or detailed technical requirements

and organizational measures. The findings in this area too

and developing best practice examples is an important task

of business and science. The data protection supervisory authorities will

actively support this process.

III.

The development of AI requires control

The data protection supervisory authorities monitor the application of data

data protection law, enforce it and have the task of

development for an effective protection of fundamental rights. given

the high dynamics in the development of artificial technologies

Intelligence and the diverse fields of application characterize the limits of

development not over yet. Likewise, the risks of

Processing of personal data in AI systems not blanket

to estimate Ethical principles must also be observed. Science,

Data protection authorities, users and especially politicians

are required to accompany the development of AI and, in the sense of the

to control data protection.

1.3

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

April 23, 2019

No abolition of data protection officers

The conference of the independent federal data protection supervisory authorities

and of the countries (DSK) speaks out against abolition or watering down

of the national regulations supplementing the General Data Protection Regulation

the obligation to appoint a data protection officer.

According to Section 38 of the Federal Data Protection Act, e.g. B. Companies and associations

Designate data protection officers, insofar as they are usually at least ten

Persons constantly involved in the automated processing of personal data

deal with data. This obligation has proven itself for many years and is

therefore retained in the data protection reform in German law

been.

The data protection officers ensure competent data protection law

Technical advice to avoid data protection violations in advance and

to keep the risk of sanctions low. This has been particularly the case

Transition to the General Data Protection Regulation proved successful.

Even if the national obligation to name data protection

commissioned, the obligations of data protection law remain. ver

However, those responsible lose internal consultants to questions

of data protection. The omission may be perceived as a short-term relief

become. Internal competence will be lost in the medium term.

A softening of this naming obligation, especially for smaller ones

Companies and associations will therefore not relieve them, but them

damage in the medium term.

1.4

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

September 12, 2019

Digitization of administration in compliance with data protection regulations

make citizen-friendly!

The federal government wants to modernize the registers kept in the administration

nize and plans to make it easier to access in this context

personal data stored there. According to the conference

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

countries (data protection conference) must not introduce this project

of uniform, cross-administrative personal identifiers or

carry identifiers. Rather, the protection of fundamental rights and

Fundamental freedoms, in particular the right to protection of personal data

data, have priority. It is equally important to the citizens

the better services combined with a significantly higher transport

to offer parenz.

Federal government tackles modernization of registers

With the Online Access Act, the federal government has an extensive

Digitization program started for administration in Germany.

The federal and state governments are obliged to improve their administrative services in the future

electronically via administrative portals. There should be user accounts

are provided, via the users for those in the portal network

available electronic administrative services from the federal and state governments can be identified uniformly.

In this context, the National Regulatory Control Council (NKR) spoke out in favor of modernizing the German register landscape and recommended that certain basic data from citizens and businesses only have to be notified once ("once only" principle). The NKR has also encouraged to use data protection-compliant identification numbers for Individuals, companies as well as buildings, apartments and parcels of land create and use and set up a "data cockpit" in which the Citizens can keep an eye on all government data flows.

The introduction of such identification numbers for people is becoming topical under the auspices of the Federal Ministry of the Interior, Building and Community (BMI) tracked by the federal government. The IT Planning Council has in its 28th meeting on March 12, 2019 the “Guidelines for a Modernization of the registry landscape” and the “Proposal

for the improvement of identity management as part of the register modern nisation” and welcomed the desired project.

Privacy-friendly and transparent design for Citizens

Already the creation of uniform and cross-administrative personal identifiers and a corresponding infrastructure for Data exchange entails the risk of personal data being lost on a large scale Dimensions easily collated, linked and combined into a comprehensive personality personality profile could be completed. The data protection conference

points out that the Federal Constitutional Court has been around for decades

the introduction and processing of such personal identifiers is very tight

barriers imposed, since they massively fall within the scope of protection of the right to information

mational self-determination of affected citizens intervene.

Already the possibility of a comprehensive cataloging of female citizens

and citizens by the state jeopardizes the right of personality, since they

lead people to adapt their behavior ahead of time

can. The principles of the European General Data Protection Regulation

tion and their regulations for data protection-compliant design

uniform and cross-administrative personal identifiers

Limits and require appropriate guarantees for the maintenance of rights

and freedoms of the data subjects.

Especially with regard to the planned use of modernized registers

ter for future census surveys and planned/modernized access

rights of the security authorities, special protection is required

affected persons. The high risks for the right to informational

Self-determination must be in a comprehensive regulatory, above all

but technical and organizational concept can be countered. Only this way

can do those required by German and European constitutional law

guarantees are maintained.

It is imperative that the modernization of the registers also be used from the outset

be used, the citizens the use of the online

Access Act provided services by using once back-

data to facilitate. In addition, it is of particular importance

the citizens compared to the current situation

to ensure a significantly higher level of transparency. A "data cockpit"

as the NKR has already suggested, it must be given to the citizens

Allowing citizens to see which register is which at any time

holds data about them, which authorities have accessed them and with

what other data they were linked to. At the same time,

be provided that only the citizens concerned

access is possible. On this basis, the digitization of the

Administration to be used, the informational power imbalance between

State and citizens largely repeal and give them the

significantly facilitate the exercise of their rights.

In the opinion of the data protection conference, the decentralized

Register structure preserved. The use of uniform, managed

Cross-departmental personal identifiers or identifiers for direct

The data protection conference rejects the identification of citizens

away. It calls for alternative methods of unique identification. Next to

Comparisons via the respective data record of the register would come

if sector-specific personal identification numbers are considered, which is a unique

Allow identification, prevent unilateral state comparison of data

change, maximum transparency, for example through a data cockpit

enable, reduce the risk of misuse and compromise

and ensure the uniqueness of registers.

1.5

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

November 06, 2019

Recommendations for a data protection-compliant design

of AI systems

Based on the Hambach Declaration of April 3, 2019, the conference

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

countries (DSK) in a position paper, requirements for AI systems

works, the implementation of which the DSK for a data protection-compliant design

recommended by AI systems. Those laid down in the Hambach Declaration

Legal framework conditions are thus in terms of technical

and organizational measures specific to the different

phases of the life cycles of AI systems.

The phases of the life cycle of an AI system - designs of the AI system,

Refinement of raw data into training data, training of the AI components,

Validation of the data and AI components as well as the AI system, use

of the AI system and the feedback of results - are scaled

examined by guarantee objectives. To get out of legal requirements

Derive AI-specific technical and organizational measures and

to be systematized, the guarantee goals of transparency, data

nimation, non-chaining, intervenability, availability, integrity, and

confidentiality used.

For the processing of personal data in which AI systems for

are used, the principles formulated in the GDPR apply. With the

position paper will provide those responsible in the field of AI with a framework for action

for the data protection regulations at hand, on which they

be able to orientate themselves in the planning and operation of AI systems.

The position paper is intended to make it clear that the use of AI systems

and data protection are not compelling opposites. The odds and

new possibilities for the use of AI systems are

modern data protection is not prevented. The position paper should

development and use of AI, also using personal data

Accompany data constructively. This increases operational certainty and

ensures that the fundamental rights and freedoms of the persons concerned

sons, in particular the right to informational self-determination, too

are maintained in the dynamic environment shaped by AI systems.

The DSK is also presenting this position paper to encourage dialogue with the relevant

leading players from politics, business, science and society

to further intensify consumer associations on this basis.

Note HBDI: Due to the large size of the position paper, the reprint was

renounces It is at https://www.datenschutzkonferenz-online.de, the official website

of the Data Protection Conference (DSK).

1.6

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

November 06, 2019

Healthcare facilities, regardless of their size, must

Ensure protection of patient data

The data protection conference expressly points out that the

security of patient data in medical treatment after

General Data Protection Regulation must be guaranteed across the board.

The effective protection of health data must not depend on the size of the

depend on utility.

In the recent past, incidents in which the protection

of patient data in inpatient care is at risk. So became

in July 2019 a number of institutions of a carrier in Rhineland-Palatinate

and the Saarland victims of an infestation with malware. The through this

Encryption of data in the IT network of the sponsoring company

has led to far-reaching impairments of hospital operations.

In September 2019 it became known that worldwide more than 16 million

Records, including 13,000 from German healthcare facilities

treated patients, were openly available on the Internet. cause for this

were, according to the information that has become known so far, in particular

insufficient technical and organizational precautions for protection

this data.

The use of information and communication technology in health

Health care is essential in the age of digitized medicine. All-

However, the legally required in this context and according to

precautions appropriate to the state of the art to an effective

Protection of patient data across the board

become. This includes all institutions working in this context

regardless of their size due to the General Data Protection Regulation

obligated.

Against the background of an increasing

the digitization of health care and in view of the

associated dangers, including financial ones

respect to ensure that all healthcare facilities

state-of-the-art technology to protect patient data

to take the necessary precautions.

1.7

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

November 06, 2019

Health websites and health apps - No sharing

sensitive data to unauthorized third parties!

The data protection conference is observing with increasing concern that

Drivers of health websites and health apps are also sensitive

personal data of the users without recognizable

Forward processing basis to third parties. Among other things, this happens

through tracking and analysis tools (i.e. programs that monitor surfing behavior

observe and analyze), of whose use the persons concerned

have no knowledge.

In September 2019, for example, a study by a non-governmental organization

tion known that numerous operators of health websites, their

visitors information on depression and other mental illnesses

ten offer personal usage data without adequate integration

which users are said to have forwarded to other bodies.

In some cases, even participation in depression self-tests should be recorded

have been. Of the 44 German websites analyzed, they also had far

more than half such integrated building blocks that would have made this possible. In the

Research was published in October 2019, according to which a German-

country-based diagnostics app also provides tracking and analysis services

use and in this context sensitive health data such as e.g. B.

physical complaints without prior information and legitimation of the

Transfer users to third parties.

The data recipients often include, in addition to other tracking service

are provided by large companies such as Facebook, Google and Amazon, which

primarily pursue their own business interests. The linking of further

routed data with other information creates the risk that for

each user has a personal health profile

arises, of the existence and extent of which the persons concerned are unaware

knowledge.

The independent data protection supervisory authorities of the federal and state governments

check such information within the scope of their tasks and possibilities

will sanction data breaches where appropriate. Simultaneously

the legislature is called upon in connection with the forthcoming

the introduction of digital health applications into standard care

ensure the protection of the confidentiality of sensitive health data.

For example, it would be unacceptable if the use of one of

by law

unintended forwarding of health data would be coupled.

The data protection conference demands the operators of health websites

and health apps, the legitimate expectations of confidentiality of their

to respect users. Regardless of the general

data protection requirements for the transfer of personal

General health data are the following requirements in particular

to note:

– Manage operators of health websites and health apps

forward personal usage data to other bodies, they are

responsible for this data transfer, even if they - such as

when integrating social plugins - no own access to the

forwarded data.

– As responsible persons, operators are obliged to comply with the principles

of data protection through technology design and through data protection

friendly defaults to consider. The one described above

According to Art. 9 Para. 1, 2 Letter a

General Data Protection Regulation as an exception only on the basis of a

express consent obtained prior to data processing

be casual, which also meets the other prerequisites for effectiveness

consent under data protection law must be satisfied.

– In particular, consent to the processing of

health data strict transparency requirements: among others

must specify who is responsible for the processing

and what categories of personal data, such as

health data, information about sexual orientation or

to sex life, are processed. The purposes of data processing

processing and the recipients of forwarded data are specific

to name. The users must enter this information in the

Able to find out about the consequences of their given consent

to become conscious.

– In the context of standard care, consent-based instruction would

Forwarding of user data to tracking or analysis service providers or

other third parties who are not part of the health care, if necessary

permissible if regulated by law. against such

However, legal regulations exist with regard to the requirement

serious concerns about voluntary consent.

The data protection conference also points out that the

presented circumstances again gives rise to the urgent need to

adopt an ePrivacy regulation as soon as possible. in must

the needs of electronic data traffic with the requirements

of the fundamental rights to privacy and data protection

become. In particular, regulations are required that have a high

Effectively ensure the protection of sensitive data.

1.8

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

November 06, 2019

No mass automated recording of vehicle

License plate for law enforcement purposes!

The Conference of the Independent Data Protection Authorities of the Federal

des and der Länder (DSK) points out the grievance that for some

Time actually set up for police security purposes

automated license plate recognition systems also for criminal purposes

tracking are used. They record en masse and partially

long-term vehicle data regardless of the suspected status of the

affected persons.

As part of averting danger, the police conduct searches on the basis of the respective

League Police Act according to individual vehicle registration numbers. Only

in the event of a match between the registration number and the vehicle being searched for

the individual vehicle registration number is stored.

License plates that are not being searched for by the police are searched for

deleted immediately after it was recorded.

In contrast, in the area of criminal prosecution - based on court

decisions or public prosecutor's orders - not only after

individual motor vehicles searched selectively. Rather become partial

In addition, the license plates of all vehicles that have a road with

happen to a detection device over a longer period of time

indiscriminately recorded and stored for the long term. As the legal basis for

such criminal prosecution measures is usually § 100h of the criminal prosecution

cessation regulations (StPO). This allows for observation

accused persons to use certain technical means, provided that

The subject of criminal prosecution is a criminal offense of considerable importance

is. Such measures are only exceptional against other persons

allowed. Comprehensive data processing, such as the recording of the

License plates of all motor vehicles passing a recording device

means a longer period, but means that all transactions

Road users in the detection area Target of investigative measures

are and insofar as movement profiles can arise. An extension of

Affected group in this magnitude is not supported by any facts

justifiable and unjustifiable. Therefore, in particular, she cannot

be based on § 100h StPO.

In view of the lack of a legal basis, the DSK sees in the

continued excessive use of license plate recognition systems for the

Purposes of criminal prosecution a violation of the Basic Law and a

Violation of citizens in their right to informational

self-determination. The DSK calls on the police authorities and public prosecutors

on, the comprehensive and indiscriminate collection, storage

and evaluation of motor vehicles by license plate recognition systems

for the purposes of criminal prosecution and the illegally stored

deleted data.

The DSK rejects proposals for the creation of a new legal

basis for such criminal procedural measures. after

Constitutional Court case law already provide the automated

License plate checks to search for people or things

constitute an interference of considerable importance, even if the license plates

be deleted immediately without a trace. A longer term record

of all characteristics, on the other hand, justifies a clearly difficult

major encroachment on fundamental rights.

168

2. Selected decisions of the Conference of Independent

Federal and state data protection supervisory authorities

Appendix I - Privacy Materials

2.1

Decision of the Conference of Independents

Federal and state data protection supervisory authorities –

September 12, 2019

Subject responsibility for email and other over-the-top (OTT)

services

Based on the judgment of the ECJ of June 13, 2019 (Az. C - 193/18) on

Interpretation of the term "telecommunications service" apply to the

Allocation of responsibilities between the BfDI and the supervisory authorities

of the federal states subject to a change in the legal

the following principles:

1. Webmail services are not telecommunications services i. s.d. telecom

Communications Act (TKG) in the currently applicable version. this applies

for pure webmail services and for e-mail services, which together with a

Internet access will be offered if the e-mails (at least also)

can be accessed via webmail. It follows that for

the data protection supervisory authority in the absence of other special

regulations only the respective state data protection supervisory authorities

are responsible. Previously with the Federal Commissioner for Data Protection

(BfDI) conducted procedures are sent to the responsible state

submitted to supervisory authorities for processing due to their jurisdiction.

2. Messenger services that operate in a closed system, i. H.

in which the users only among themselves and not with users

whose services can communicate, can also according to the mentioned

Decision of the ECJ as telecommunications services i. s.d. TKG

be viewed with the consequence that for these services the

BfDI is responsible for supervisory law (section 115 (4) TKG).

169

2.2

Decision of the Conference of Independents

Federal and state data protection supervisory authorities –

September 12, 2019

Responsibility under data protection law within the telematics

infrastructure

The data protection conference represents on the question of data protection law

Responsibility within the telematics infrastructure according to § 291a paragraph 7

SGB V the following opinion:

The society for telematic applications of the health card mbH

(gematik) is

a. Solely responsible for data protection for the central zone of TI

(“TI platform zone central”) as well

b. "Co-responsible for data protection within the meaning of Article 26 GDPR

for the decentralized zone of TI ('TI platform zone decentralized'). The scope

the responsibility of gematik for the decentralized zone of the telematics

Infrastructure requires legal regulation. gematik is responsible

verbatim for the processing, in particular insofar as it is carried out by you

given specifications and configurations for the connectors,

VPN access services and card terminals.”

2.3

Decision of the Conference of Independents

Federal and state data protection supervisory authorities1 –

May 24, 2019

Asset Deal - Catalog of case groups

The Conference of the Independent Data Protection Authorities of the Federal

des and der Länder has agreed on a catalog of case groups,

within the framework of the balancing of interests according to Art. 6 Para. 1 Sentence 1 lit. f

i. V. m. Para. 4 DS-GVO are to be taken into account in an asset deal. The

Case groups are:

1. Customer data for current contracts

Here, the transfer of contract requires the approval of the customer under civil law

or the customer (§ 415 BGB / assumption of debt). In this civil law

1 With the rejection of the Berlin Commissioner for Data Protection and Freedom of Information and

of the Saxon data protection officer.

Approval as a minus is also the consent under data protection law

seen for the transition of the necessary data. This means that the

interests of the customer are safeguarded.

2. Existing customers without current contracts and last contractual relationship

older than three years2

Data from existing customers for whom the last active

contractual relationship dates back more than three years, are subject to

advertiser a restriction of processing. This data may

transmitted, but only because of legal retention periods

be used.

A conceivable alternative is that corresponding customer data is not transmitted

will remain with the old company. Is a bankruptcy trustee

switched on, this endeavors to finance one from the crowd

Service provider who keeps the old data for a certain period of time.

3. Customer data for advanced

contract initiation; Existing customers without current ones

Contracts and last contractual relationship younger than three years3

Data of such customers are processed according to Art. 6 Para. 1 Sentence 1

lit. f) GDPR by way of an objection solution (opt-out model) with a

adequately set objection period (e.g. six weeks)

tell. This procedure is cost-saving for the company and

also takes interests into account through the generous objection period

of customers. Many customers are with one

Rather surprised at the request for express consent. Also

care should be taken to keep the contradiction simple –

e.g. B. in the online process by clicking on a box.

However, the bank details (IBAN) are from the transition via objection solution

except and only with the express consent of the customer

to transfer.

This does not include payment behavior.

2 The 3-year period takes into account the regular limitation of claims. Also have

Experience has shown that non-active customer data is more than three years old for the acquiring body

no longer relevant and are obsolete.

3 The 3-year period takes into account the regular limitation of claims. Also have

Experience has shown that non-active customer data is more than three years old for the acquiring body

no longer relevant and are obsolete.

4. Customer data in case of open claims

The transfer of outstanding claims against customers

under civil law according to §§ 398 ff. BGB (assignment of claims). In this

The assignor (old creditor/old company) may

take) to the assignee (new creditor/new company) – supported

to Art. 6 Para. 1 Sentence 1 lit. f GDPR (formerly Section 28 Para. 1 Sentence 1 No. 2 or

Paragraph 2 No. 2 lit. a BDSG a. F.) - transmit. Predominant opposing interests

exist, however, if the assignment is made by agreement

is closed (§ 399 2nd alternative BGB, § 354a HGB).

5. Special category customer data according to Art. 9 Para. 1 DS-GVO

Such data can only be processed by way of informed consent in accordance with Art. 9

Para. 2 lit. a), Art. 7 DS-GVO.

2.4

Decision: Planned introduction of a regular full

Registration data comparison for the purpose of collecting the broadcasting fee

stop – April 26, 2019

In the future, according to a draft bill to change the circular

radio contribution state contract (RBStV) regularly every four years

of all persons of legal age to the responsible regional

radio station to ensure that the database there is up-to-date

be transmitted. Pursuant to Art. 1 No. 7 of this draft of the 23rd Broadcasting

amending state treaty dated February 5, 2019 is part of the reporting data

in addition to name and current and last address in particular also

Birthday, title, marital status and the exact location of the apartment.

The complete comparison of registration data carried out in 2013 was already

encountered considerable data protection concerns at the time (cf.

Closing of the Conference of Independent Data Protection Authorities

of the federal and state governments (DSK) of October 11, 2010). The DSK asked

only partially withdraw their concerns because it is only a one-off

Reporting data reconciliation should be made to start the new

to facilitate contribution model. With the regulation now planned, the

- already dubious at that time - assurances from the legislature that it

with the unprovoked complete comparison of registration data from the years

2013 and 2018 would be one-off events, finally lapsed.

Against the planned introduction of a regular full reporting

data reconciliation, basic constitutional and

data protection concerns.

Such a comparison represents a disproportionate intervention in the information

functional self-determination and comes into conflict with the principles of

Data minimization and the necessity according to Art. 5 Para. 1 lit. a and c,

Art. 6 para. 1 of the General Data Protection Regulation (GDPR).

In the case of a complete comparison of reporting data, a large number of personal

Son-related data of data subjects who are not subject to contributions at all

are either because they live in a dwelling, for those already owned by others

Individuals are paid contributions or because they are exempt from the obligation to contribute

are exempted, transmitted to the broadcasters and processed by them

works. In addition, data from all those residents

collected and processed by residents who have already registered with the state
have registered with a radio station and regularly pay their subscriptions. Included
the planned comparison of registration data will affect more personal data,
than the contribution payers have to indicate when registering,
e.g. B. Doctoral degree and marital status (cf. § 8 Para. 4 RBStV). So it should
personal data are transmitted to the broadcasters that
are not necessary for the collection of contributions.
The registration data transmission ordinances of the federal states offer the
lass-related registration data transmission to the broadcasters already
an appropriate and sufficient opportunity to ensure that the data
existence of the contribution service even if the reporting situation changes
to ensure the contribution debtors. Also
if the registration authorities fail to notify a change in individual cases
should, a new complete comparison of registration data would be disproportionate
nically in the right to informational self-determination
contribution debtors intervene without this being due to other aspects,
such as the goal of fairness in fees, would be justified.
The state broadcasting corporations themselves assume that a complete
Reporting data reconciliation ultimately results in less than one percent of cases
additional, permanent registration of contributors (cf. Eva-
Evaluation report of the federal states in accordance with Section 14 (9a) RBStV of March 20, 2019).
The planned regulations also take into account the standards of the DS-
GMO not sufficient. National data protection regulations must be due
the priority of application of European regulations to an opening
clause of the GDPR can be supported. Art. 85 Para. 2 DS-GVO is
not relevant, since the data processing is for the purpose of collecting the

Broadcast contribution is not within the scope of this standard. At

Regulations based on the opening clause according to Art. 6 Para. 2 and Para. 3

i. V. m. Art. 6 (1) lit. e) GDPR are the principles

of data minimization and necessity. Member State

Arrangements for the performance of tasks in the public interest

lie, may be introduced thereafter if these do indeed comply with the GDPR

specify, but not exceed their limits. regulations that are

refer to this opening clause must therefore be included in the framework

keep, which the DS-GVO specifies. There are significant concerns here

with regard to the principles of data minimization and necessity.

It is positive to emphasize that the previous landlord information in

With regard to rental apartments deleted from Section 9 (1) sentences 2 and 3 RBStV

shall be. Likewise, the purchase of address data from private individuals

are expressly excluded. Both data processing are off

view of data protection is to be viewed critically and its deletion is to be welcomed.

However, it must not be overlooked that with the planned regular

a much more comprehensive, data

also a very dubious possibility of data collection in terms of protection law

is to be created that meets the practical need for landlord information

and the purchase of private addresses can be omitted anyway.

The conference of the independent federal data protection supervisory authorities

and the federal states calls for the planned regular full reporting

not to introduce data comparison, as this is against the intended regulations

fundamental constitutional concerns exist and these the

The standards of the GDPR are not sufficiently taken into account.

2.5

Resolution of the 97th Conference of Independents

Federal and state data protection supervisory authorities

Interpretation of the term “certain areas more scientific

Research” in recital 33 of the GDPR – April 3, 2019

The term "certain areas of scientific research" is used in consideration

Reason 33 mentioned but in the General Data Protection Regulation (GDPR)

not further defined. It is closely related to the content

with the intended purpose, as with the granting of consent

is to be designed. According to Art. 4 No. 11 GDPR, consent is always for

the "specific case", in an informed manner and unequivocally

give. The requirement of the "specific case" puts the principle into concrete terms

the earmarking within the meaning of Art. 5 Para. 1 Letter b DSGVO, according to which

personal data for specified, explicit and legitimate purposes

are to be raised.

174

Appendix I - Privacy Materials

In its working paper 259 rev 01, p. 33, the Article 29 Data Protection Group

pe also pointed out that this is why the term “certain areas

scientific research” from the broadly understood concept of

scientific research in Art. 89 GDPR. There

is about the scope of scientific research,

not about the purpose limitation in the context of a specific data processing.

In contrast, the term "certain areas of scientific research

to understand more closely.

From this follows: Only if the specific design of the research project

foreseeable until the time of data collection a complete purpose

determination absolutely does not allow (cf. recital 33, sentence 1),

For example, the broad consent approach

come to fruition. In the case of data collection that precedes in time

Consent can then, under narrow conditions, be reduced with regard to

the specificity of the purpose are accepted.

However, recital 33 does not release you from the obligation to

working out mechanisms in the context of research projects

which the use of the collected data for the data subject

understandably limited. In particular, it will not be as with that

Recital 33 deemed compatible if the use of the collected

Data is extended to certain research areas across the board. The

The requirement for informed consent requires at least that if possible

precisely the respective research project and those listed below

specific security measures covered by the declaration of consent

become.

In individual cases where working with broad consents as for

the achievement of the research purpose is considered absolutely necessary

therefore to work in particular with the following correctives. you serve

of transparency, trust-building and data security, to the more abstract

Compensate for the version of the research purpose:

A. Additional safeguards to ensure

transparency

– Use of a usage policy that is accessible to the consenting party

or an accessible research plan that shows the planned work

methods and the questions that should be the subject of research,

illuminated

175

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

– Elaboration and documentation with regard to the concrete

research project, why in this case a more detailed specification of the

research purposes is not possible

– Setting up an internet presence through which the study participants

current and future studies are informed

B. Additional safeguards to build confidence

– Positive vote by an ethics committee before use for further research

research purposes

– Checking whether working with a dynamic consent is possible or not.

Granting an opportunity to object before using the

Data for new research questions

C. Additional Data Security Guarantee Measures

Increased use of guarantees with regard to the data collected by

technical and organizational measures such as:

- No data transfer to third countries with a lower level of data protection

– separate commitments to data minimization, encryption, anonymization

ization or pseudonymization

– specific rules for limiting access to the increased

named data

The result of the test including the underlying movements

reasons and ensuring the above Security measures are to

document and to check the ethical and data protection law

Compatibility of the research project with the responsible bodies

to submit to the research concept.

176

Appendix I - Privacy Materials

2.6

Positioning on responsibility and accountability

Facebook fan pages and the supervisory authority4

– 01.04.2019

The Conference of the Independent Data Protection Authorities of the Federal

des und der Länder (DSK) met on September 5, 2018 for the (further)

Operation of Facebook fan pages after the judgment of the ECJ on June 5th

voiced in 2018. In its decision, the conference made it clear that

that fan page operators verify the legality of the jointly responsible

data processing and compliance with the principles

for the processing of personal data from Art. 5 Para. 1 GDPR

have to be able to prove. This stems from accountability

according to Art. 5 Para. 2 GDPR and in particular with regard to obligations

according to Art. 24, 25, 32 GDPR.

On September 11, 2018, Facebook published a so-called "page

Insights supplement regarding the person responsible” and “Information

to Page Insights”. This "Page Insights" published by Facebook

Supplement regarding the person responsible" does not meet the requirements

gene to an agreement according to Art. 26 GDPR. In particular, it is in

Objection to joint responsibility according to Art. 26 GDPR,

that Facebook has the sole decision-making power "regarding the

Processing of Insights data". The ones from Facebook

published information also represents the processing activities that

in connection with fan pages and in particular page insights

are managed and are subject to joint responsibility

sufficiently transparent and concrete. They are not sufficient to

Fan page operators to check the legality of the processing

personal data of visitors to their fan page

to allow. Against this background, the conference reaffirms the

Accountability of fan page operators (regardless of the degree of

responsibility) and states:

1. Each person responsible needs for the processing activities that of his

Subject to responsibility, a legal basis according to Art. 6 Para. 1

GDPR and - as far as special categories of personal data

processed - according to Art. 9 Para. 2 DSGVO. This also applies in the

cases in which they do not carry out the processing activities directly themselves

4 With the abstention of the Hessian Commissioner for Data Protection and

Ness.

carry out, but by others jointly responsible with them

be carried out.

2. Without sufficient knowledge of the processing activities carried out by the

subject to their own responsibility, responsible persons are not able

to assess whether the processing activities are carried out in accordance with the law

become. If there are any doubts, this is at the expense of those responsible,

who have it in their power to refrain from such processing. The

The ECJ explains: “The fact that an operator of a fan page

uses the platform set up by Facebook to

It is not possible to use services from

compliance with its obligations in the area of personal protection

free of personal data." (ECJ, C-210/16, para. 40)

With regard to the remarks on the "main branch for the

Processing of Insights data for all those responsible” and

to the lead supervisory authority (point 4 in the "Site Insights

Supplement regarding the person responsible”) points out the conference

point out that the responsibility of the respective supervisory authorities for

fan page operator according to the GDPR. According to Art. 55 et seq. GDPR

the supervisory authorities for those responsible (e.g. fan page operators)

competent in their territory. This applies regardless of the through

the cooperation and coherence mechanisms provided for in the GDPR.

3.

Both Facebook and the fan page operators must

fulfill their duty. The Data Protection Conference expects Face-

book will be improved accordingly and the fan page operators will be held responsible

do justice to the wording accordingly. As long as these duties do not

is complied with is a data protection compliant operation of a fan page

not possible.

and other publications of the Conference of

independent federal data protection supervisory authorities

and the countries

3.1

Concept of the independent data protection supervisory authorities

Federal and state governments on the assessment of fines in proceedings against

Company – October 14, 2019

I

Introduction

On May 25, 2018, the European Data Protection Board (EDPB) in its

first plenary session according to its task in Art. 70 para. 1 lit.

k) DS-GVO the guidelines for the application and determination of fines

within the meaning of Regulation (EU) 2016/679 of the Article 29 Working Party

from 03.10.2017 (WP 253) confirmed. This particular place the uniform

Interpretation of the provisions of Art. 83 DS-GVO and outline

uniform concept for the principles of setting monetary

atone However, the guidelines are not exhaustive and the specification

the determination methodology is reserved for later EDPB guidelines.

The concept relates to the assessment of fines in proceedings against companies

within the scope of the General Data Protection Regulation (GDPR). It

does not apply in particular to fines against clubs or

natural persons outside their economic activity. The concept

is neither for cross-border cases nor for other data protection

binding on EU regulators. Furthermore, it develops no bond

seen in the setting of fines by courts.

The independent data protection supervisory authorities of the federal and state governments

may at any time revoke, change or expand their concept

decide with effect for the future. The concept also loses its

Validity as soon as the EDPB issues its final methodological guidance

the setting of fines.

II.

fine concept

The independent data protection supervisory authorities of the federal and state governments

believe that in a modern corporate sanctions law

with significant maximum fines, while addressing a variety

companies of different sizes, the turnover of a company

a suitable, appropriate and fair connection to ensure the

effectiveness, proportionality and deterrence.

Against this background, fines are assessed in proceedings against

Business in five steps. First, the company concerned

assigned to a size class (1.), after which the mean annual

rate of the respective subgroup of the size category (2.), then a

basic economic value determined (3.), this basic value by means of a

factor dependent on the severity of the circumstances of the crime multiplied (4.) and

finally the value determined under 4. based on perpetrator-related and other

adjusted for circumstances that have not yet been taken into account (5.).

This procedure guarantees a comprehensible, transparent and individual

case-based form of fine assessment.

1. Categorization of companies according to size classes

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

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

The size classes are based on the total advance achieved worldwide

Annual turnover of the company (cf. Art. 83 Para. 4 to 6 DS-GVO) and are

divided into micro, small and medium-sized enterprises (SMEs)

as well as large companies. It applies according to recital 150 of the

DS-GVO the term "company" within the meaning of Articles 101 and 102 TFEU

(so-called functional company concept).

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

principle based on the Commission's recommendation of May 6, 2003

(2003/361/EC).

The size classes are used to more concretely classify the companies

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

D.I to D.VII).

180

micro, small and medium-sized enterprises

large companies

Appendix I - Privacy Materials

A.II

annual sales

B.II

annual sales

C.II

A

micro

company:

annual sales

up to €2 million

AI

annual sales

BI

until

€700,000

above

€700,000 up to

€1.4m

A.III Annual turnover

B.III

above

€1.4m up

€2 million

(Table 1)

(SMEs)

B

Small

Company:

annual sales

C

medium

Company:

annual sales

above

€2 million

until

€10 million

annual sales

above

€2 million

until

€5 million

CI

above

€10 million

until

€50 million

annual sales

above

€10 million

until

€12.5 million

annual sales

above

€5 million

until

€7.5m

above

€12.5 million

until

€15 million

C.III

annual sales

over €7.5 million

up to €10 million

annual sales

over €15 million

up to €20 million

D

annual sales

over €50 million

DI

annual sales

above

€50 million

until

€75 million

D.II

annual sales

above

€75 million

until

€100 million

D.III

annual sales

over 100

million €

up to €200 million

annual sales

above

€200 million

until

€300 million

C.IV

annual sales

D.IV

above

€20 million

until

€25 million

CV

annual sales

D.V

annual sales

above

€25 million

until

€30 million

above

€300 million

until

€400 million

C.VI

annual sales

D.VI

annual sales

above

€30 million

until

€40 million

above

€400 million

until

€500 million

C.VII

annual sales

D.VII

annual sales

above

€40 million

until

€50 million

over 500

million €

2. Determination of the average annual turnover of the respective subgroup

the size class

Then the average annual turnover of the sub-group in which the company

take was classified (Table 2). This step is for

Illustration of the determination of the economic

core value (3.).

micro, small and medium-sized enterprises

Enterprises (SMEs)

A

€350,000

€1,050,000

€1.7m

BI

B.II

B.III

B

€3.5m

€6.25m

€8.75 million

AI

A.II

A.III

C

€11.25m

€13.75 million

€17.5m

€22.5 million

€27.5m

€35 million

€45 million

CI

C.II

C.III

C.IV

CV

C.VI

C.VII

DI

D.II

D.III

D.IV

D.V

D.VI

D.VII

Large-

company

D

€62.5 million

€87.5 million

€150 million

€250 million

€350 million

€450 million

more concrete

Annual sales*

(Table 2)

* From an annual turnover of more than €500 million, the percentage fine is from

2% or 4% of the annual turnover as a maximum limit, so that when

respective company, a calculation is made based on the actual turnover.

3. Determination of the basic economic value

The middle value is used to determine the basic economic value

Annual turnover of the subgroup in which the company is classified,

divided by 360 (days) and thus an average, to the integer place

rounded up daily rate (Table 3).

micro, small and medium-sized enterprises

Enterprises (SMEs)

large companies

A

€972

€2,917

€4,722

B

€9,722

€17,361

€24,306

BI

B.II

B.III

AI

A.II

A.III

C

€31,250

€38,194

€48,611

€62,500

€76,389

€97,222

€125,000

CI

C.II

C.III

C.IV

CV

C.VI

C.VII

DI

D.II

D.III

D.IV

D.V

D.VI

D.VII

D

€173,611

€243,056

€416,667

€694,444

€972,222

€1.25m

more concrete

daily rate*

(Table 3)

* From an annual turnover of more than €500 million, the percentage fine is from

2% or 4% of the annual turnover as a maximum limit, so that when

respective company, a calculation is made based on the actual turnover.

4. Multiplication of the base value according to the severity of the crime

This is then carried out on the basis of the concrete crime-related circumstances of the individual case

(cf. Art. 83 Para. 2 Sentence 2 DS-GVO) a classification of the severity of the

Deed in easy, medium, difficult or very difficult.

For this, according to Table 4 below, under consideration

the circumstances of the individual case based on the list of criteria in Article 83 (2).

DS-GVO determines the severity of the allegation and the respective factor,

by which the basic value is multiplied. With regard to the different

There are fine frameworks for formal (Art. 83 Para. 4 DS-GVO) and

material (Art. 83 para. 5, 6 DS-GVO) violations each different

factors to choose. When choosing the multiplication factor one very

serious crime, it should be noted that the fine framework related to the individual case

is not exceeded.

severity of

did

factor for formal

violations according to

Art. 83 Para. 4 GDPR

factor for material

violations according to

§ 83 para. 5, 6 GDPR

Light

Middle

Difficult

Very difficult

(Table 4)

1 to 2

2 to 4

4 to 6

6 <

1 to 4

4 to 8

8 to 12

12 <

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

Concerned speaking circumstances

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

Adapted to the relevant circumstances, insofar as these are not already mentioned under 4.

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

Circumstances (cf. criteria catalog of Art. 83 Para. 2 GDPR) and others

circumstances such as B. a long duration of proceedings or an impending payment

inability of the company.

3.2

Guide to Video Surveillance in Swimming Pools –

January 08, 2019

Addition to the orientation guide "Video surveillance by non-

public bodies" of the Düsseldorf district of February 19, 2014

Since visiting swimming pools also involves some risks

can be, many operators resort to the aid of video surveillance

it, for example, to the breaking of lockers or the improper

prevent use of the slide. Swimming pools that are in public

sponsorship are to be checked according to the applicable state law.

Otherwise, the General Data Protection Regulation (GDPR) applies.

The majority of cameras located in swimming pools monitor areas

that are accessible to customers. The processing of personal

Data is lawful insofar as this is necessary to protect the legitimate interests of

Responsible or third party is required and unless the interests

sen or fundamental rights and freedoms of the data subject who the

require the protection of personal data, especially when

if the data subject is a child. Since the

Swimming pool visitors in the swimming pool for the purpose of leisure activities
stay and want to behave accordingly informally as well as
only lightly clad, they enjoy special protection. The exam
the existence of the legal requirements therefore requires special
Care. In addition, a large number of swimming pool visitors are children
also be captured by video surveillance. Your interest is in
Within the framework of the weighing of interests in accordance with the legal requirements
to be particularly weighted. When weighing up, the reasonable results
expectations of the persons concerned to be taken into account (Recital
47 GDPR). Visitors expect as part of a visit to a swimming pool
certainly not in most areas of a swimming pool, from video
to be captured by cameras.
Irrespective of the question of a legitimate interest, a video
In any case, monitoring is generally not required to prevent it
of unauthorized access to areas for which an additional charge
(e.g. to the sauna area) is to be paid. This can usually be done through
other appropriate measures, such as sufficiently high turnstiles
or barriers, can be prevented without disproportionate effort.
Particular attention is also paid to the required level of surveillance
to be addressed: If the other requirements are met, the Admissions
area of the camera exclusively on the area (e.g. pay machines)
directed to the purpose of the video surveillance. To secure
of evidence in the event of burglaries, a video recording in the
Usually outside opening hours.
To ward off the dangers associated with bathing, a video recording is
drawing not required. In exceptional cases, a pure observation

("extended eye") may be permitted if they support the bathing

supervision in particularly dangerous or unclear places. The

Dangerousness of these places must be based on objective evidence

arise, for example, because there have already been specific incidents or

Experience values for increased danger (e.g. with diving towers,

slides, children's pool). The general one is not sufficient

increased risk of accidents due to being in the water. The use of

Video surveillance technology cannot be a substitute for supervision by personnel!

A video recording exclusively to exclude the liability risk

against claims from bathers is due to the prevailing

legitimate interests of those affected by the video surveillance

persons not permitted. It is according to Art. 8 of the Charter of Fundamental Rights

European Union disproportionate, such an interference in the

interests and the right to protection of personal data

Add person for a large number of people just so that

If in doubt, the swimming pool has the opportunity to exclude its liability.

In addition, a large number of children are usually recorded, whose inter-

eat and fundamental rights are particularly protected by the GDPR

become. Such an encroachment on their interests and fundamental rights is therefore

not justified. Liability is also subject to the burden of proof of the

harmed. Case law does not require proof of sufficient

Fulfillment of the traffic safety obligation with video recordings.1

The interests or fundamental rights and freedoms of the persons concerned

sons always predominate when the privacy of the person concerned

is touched, which is why video surveillance of people in sanitary rooms

men, changing rooms or changing areas and in the sauna in general

is not permitted.

Video surveillance can be used in individual cases to secure evidence

be permitted in the case of proven locker break-ins, provided that not at the same time

Benches/storage areas or changing rooms can be recorded. Pre-condition

is that bathers are given real choice, in

which area they are going to. There are areas that are under video surveillance

become recognizable by those in which no surveillance takes place

separate them, for example by marking the floor in different colors.

In any case, video surveillance is disproportionate and therefore not permissible.

Claims due to minor damage (e.g. damage to hair dryers).

In addition, there may be other data protection requirements (e.g.

List of processing activities, data protection impact assessment,

signs) to be observed. This includes, screens so too

position that they are not visible to third parties.

1 OLG Koblenz, decision of May 7th, 2010, Az.: 8 U 810/09: The operator satisfies his

Obligation to ensure traffic safety if by means of signs with formulated warnings

or the problem areas are clearly pointed out with pictograms; LG Munster,

Judgment of 05/17/2006, Az.: 12 O 639/04: The operator of a swimming pool is sufficient

Traffic safety obligation when he provides a lifeguard who pays his attention

also - if not continuously - on the special swimming pool facilities

(here: children's slide leading to the non-swimmers' pool).

3.3

Position paper on the use of camera drones by non-public bodies – January 16, 2019

Due to the increasingly affordable prices, drones are increasingly figer bought for leisure and used by non-public bodies in the neighborhood environment or for commercial purposes.

If the drones are equipped with cameras, they enable unobserved Look into places that are not easily accessible, such as the garden or the sun neighbor's terrace, but also on public streets or squares.

This is data processing using video surveillance.

The potentially monitorable area is only covered by the technical characteristics of the device used are limited. Walls, fences or other Partitions that prevent third parties from entering the protected area or intended to make it difficult or impossible to gain insight into this is no longer an obstacle when using drones.

However, when using drones, the Air Traffic Ordinance (LuftVO) to note. This contains a ban on the operation of unmanned aircraft systems and flight models in certain locations.

According to Section 21b (1) No. 2 of the Aviation Ordinance, the operation of drones is e.g. above and at a lateral distance of 100 meters from crowds of gen, places of accident, disaster areas and other locations of Authorities and organizations with security tasks prohibited. In addition according to Section 7 of the same provision, e.g. also the operation of drones, the be able to take electronic pictures of residential properties prohibited if the affected owner or other rights of use has not expressly consented. This will make the allowed local

Area of application of camera drones by non-public bodies

limited in advance.

In addition, the use must comply with data protection regulations

of the General Data Protection Regulation (GDPR) can be measured as soon as a

Data processing not exclusively in the context of personal or family

liary activities, but e.g. B. for commercial purposes or for

Purposes of publication.

A legal basis is required for processing. For example, must

processing to protect the legitimate interests of the person responsible

or a third party may be required and, on the other hand, may require protection

Interests or fundamental rights and freedoms of the data subject

not outweigh, especially when it comes to the data subject

is a child (Article 6 paragraph 1 sentence 1 letter f GDPR). The

indicates the interests of the person responsible for using a drone

weighed against the interests of those affected. A crucial one

The intended use plays a role in each case. The prerequisites

genes are in the majority of cases due to the regular preponderance

not met by the interests of those affected. This is the case in particular

if the recordings are made for publication on the Internet.

In addition, it should be borne in mind that those affected cannot do without

further possible to contact the person responsible for the use of the drone

know. In addition, for the processing of personal data

required information obligations in accordance with Art. 12 et seq. GDPR as a rule

not be fulfilled. For these reasons, the use of drones that

are equipped with video cameras compared to the use of stationary ones

Video surveillance measures when collecting personal data

data with a disproportionately greater encroachment on the right to protection of personal

personal data of the persons concerned (Article 8 of the Charter of Fundamental Rights

of the European Union).

If drones with cameras are within the scope of the DS-

GMO are operated and unauthorized data is collected or processed

the responsible supervisory authority can impose a fine for this.

In addition to the supervisory authority procedure, those affected also have access to the

Civil law open. In the event of an encroachment on fundamental rights, a defensive

claim from § 823 in conjunction with § 1004 paragraph 1 of the civil

German Civil Code (BGB) can be asserted. Also the law enforcement

Authorities can be involved when due to the use of drones

the realization of criminal offenses threatens, such as in the

Production of photographs of highly personal areas of life

Areas of privacy (§ 201a of the Criminal Code (StGB)) or the

Recording of the non-public spoken word (§ 201 StGB).

Drone operators are therefore requested, as a matter of principle, not to use anyone without

to film his consent and to respect the privacy of others. user

drones with photo or video equipment are only allowed in such areas

use, in which an infringement of the rights of third parties is excluded

can be. Especially in urban environments, the operation of

Drones with film and video technology in accordance with current legislation

usually not possible.

Appendix I - Privacy Materials

3.4

position paper on the inadmissibility of video surveillance

vehicles (so-called dashcams) – January 28, 2019

Dashcams are also being used in more and more vehicles in Germany.

sets, mostly to understand the course of events in the event of an accident and that

Video, if necessary, as evidence when settling claims

and the clarification of liability issues. In doing so,

Fortunately, the entire environment was recorded without pixelation

carried out by people or license plates of other vehicles.

The use of such cameras is hardly permissible under data protection law.

As far as the Dashcams are filmed in publicly accessible areas

and as the primary purpose of the recordings, the use of film recordings

is given for the documentation of a possible course of the accident, is the

Use – even if the cameras are used by private individuals

– to Art. 6 paragraph 1 sentence 1 letter f of the General Data Protection Regulation

(GDPR) to measure. After that, the processing is more personal

Data is only permitted to the extent that this is to protect the legitimate interests of

Responsible or third party is required and unless the interests

sen or fundamental rights and freedoms of the data subject who the

require protection of personal data prevail. That means the

Interests of the person responsible who uses a dashcam are with the

to weigh up the interests of those affected. A crucial role

the intended use plays a role in each case.

In any case, the above-mentioned prerequisites are

uninterrupted recording of the traffic situation is not fulfilled, since this

drive form is not required to safeguard the interests of preserving evidence
and the legitimate interests of data subjects, mostly uninvolved
road users, predominate. The latter can relate in particular to her
Fundamental right from Art. 8 of the Charter of Fundamental Rights of the European Union
appointed. According to this, every person has the right to protection of those concerning them
personal data. This includes the right of individuals to
the public to move freely without fear of being unintentionally
and to be made the object of video surveillance without cause.
Permanently recording dashcams collect data constantly and without cause
Personal data, such as license plates of other road users
mer or people who are near a road, so that
a large number of road users from the processing of personal
withdrawn data is affected without them being aware of the surveillance
obtain or evade it. The interest of the motorist
as the person responsible for data protection in the event of a traffic accident

Having video recordings on hand as evidence can seriously
encroachment on the right to protection of personal data
not justify other road users.
In addition, even with video surveillance using a dashcam, the ver-
responsible ensure that he informs the persons concerned in accordance with Art. 12
ff DS-GVO on the camera-supported processing of personal data
transparently indicates, even if this is the case with moving vehicles in
poses difficulties from a practical point of view.

Even if the Federal Court of Justice in the decision of May 15, 2018 - VI

ZR 233/17 – recordings cannot be used as evidence in civil proceedings

denied, he emphasizes at the same time that the use of permanent

recording dash cams is not permitted under data protection law. a

According to this, acceptance can only be considered if (technical)

Possibilities are used that ensure that a

camera only records for a short time as required. Here they are too

Information obligations according to Art. 12 et seq. GDPR must be taken into account.

Consequently, the supervisory authorities - regardless of the usability in the

Civil process – issue bans and impose severe fines.

These fines can have the financial benefit of being in a civil proceeding

is disputed, under certain circumstances revoke it.

3.5

Guidance from the data protection supervisory authorities on this

Use of bodycams by private security companies –

February 22, 2019

I

foreword

Private security companies are now also equipping their employees

with body cams. As reasons they lead e.g. B. Protection of employees

Assault, gathering evidence for civil claims

or a deterrent or de-escalating effect. The use

of body cams, however, are opposed to data protection concerns.

encroachment on personal rights

The recording of image and sound using a bodycam affects the personal

personal rights of those affected and requires justification. For uninvolved

It is not immediately apparent to a third party whether a bodycam image and sound

records, which is why there is a possibility that the mere presence

this device is intimidating to them. The use of communicative

places harbors the danger that those present will be deprived of their basic rights, such as

for example freedom of expression, make only limited use. If

Security forces equipped with bodycams patrol a well

undertake visited terrain or cross a crowd,

those present can suddenly appear in the direct field of view of the devices

so that they fear detailed film or even sound recordings

must. Depending on how the bodycam is attached and used, it can also

come to an unnoticed, and thus secret, video surveillance.

Due to the fact that the viewing angle of the bodycam is constantly changing, it can

an extensive survey of the environment, including protected ones

Areas such as sanitary facilities or permanent workplaces of employees

come. If already video surveillance using static cameras

is set up, together with mobile devices this can become an almost

carry out uninterrupted surveillance.

The intrusion is particularly serious for those who stop using it

specific locations. The wearers themselves too

can be adversely affected by the bodycams: They record during

their own behavior at the same time as the observation.

III.

Data protection-compliant use

A data protection-compliant use of the bodycam is based on Art. 6 Para. 1 lit. f

General Data Protection Regulation (GDPR), Section 4 of the Federal Data Protection Act

(BDSG) to measure. After that, the processing of personal data

permissible, insofar as they are necessary for the exercise of the domiciliary rights or the protection

legitimate interests (1.) of those responsible or third parties (2.)

and is necessary (3.) and unless the interests or fundamental rights and

Fundamental freedoms of the data subject, the protection of personal

Requiring data prevail (4th).

191

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

1. Legitimate Interest / Purpose of Processing

Before commissioning, it must be clearly defined which authorized

Interest or what purpose is pursued with the use of a bodycam

shall be. Among other things, the protection of their own staff

Assault, the subsequent identification of a suspect and the

Preserving evidence for the pursuit of civil claims.

Assisting in law enforcement does not provide its own legitimate

interest in the introduction of bodycams. Defense against danger

and the elimination of disturbances to public security and order

is the task of the police; the prosecution of criminal offenses is the responsibility of the criminal

law enforcement agencies. The purpose of a subjective sense of security

Increasing the number of citizens is not enough on its own, an intervention

into the fundamental right to informational self-determination.

Video surveillance should not give a false sense of security,

where objectively safety is not increased.

The use of bodycams can only be permitted if it is required

for purposes that are clearly defined in advance. To one

appropriate use of the cameras must be ensured before the first

to create an operational concept before putting it into operation. The operational concept

may be part of a service or company agreement. Therein is final

define the specific situations in which the cameras will be used

are to be carried out and which procedure must be followed.

The use of bodycams is possible, for example, in situations where

which a person engages in aggressive behavior (physical altercation,

threats, insults, etc.) or to es-

threatens to cal. Non-aggressive, passive, or non-violent behavior

of a person, on the other hand, does not entitle you to take a camera

sentence. It must also be determined in which rooms filmed with a bodycam

may be. The recording of sensitive areas such as toilets, sanitary rooms,

Changing areas, break rooms or lounges are to be excluded. Around

To avoid surveillance pressure in the public, the responsible

literally limit the use of the cameras to areas in which

he is entitled to exercise the domiciliary rights. In order to be able to prove that

if the bodycam was used lawfully, every incident should be

into be adequately documented; at least with the respective occasion,

the time and the people involved. Technical and organizational

Measures to protect personal data are in the concept

record.

2. Bodycam suitable for achieving the purpose?

It must be possible to justify objectively that the use of bodycams

suitable for achieving the purpose. For this it is necessary to ask whether the

specified purpose through the use of such devices at the respective

place of use and the respective external conditions of use

can reach. It is doubtful whether carrying a bodycam through

can effectively prevent a subjectively possible deterrent effect,

that a crime occurs. One must also be considered

possible provocation effect by the bodycam. Also can

Recordings of a bodycam only the view of the wearer

carrier, which is why the reconnaissance value of these recordings in

particularly confusing and fast-moving situations is doubtful.

This means that the bodycam is not always suitable for the purpose

the clarification of incidents.

3. Bodycam required to achieve the purpose?

In addition, it must be checked whether equivalent means are available

which encroach less on the personal rights of those affected. under consideration

comes here to increase the number of security personnel per patrol,

extend the lighting, install emergency or alarm buttons

or to equip security forces with two-way radios so that these

be able to summon additional personnel in the event of a conflict. A lasting and

Unreasonable admission is usually not required to achieve the purpose

and must be ruled out.

4. Balancing interests - protective measures

If the test shows that the use of the bodycam in the above sense suitable and

is required are the interests or fundamental rights and freedoms

of the persons concerned with the legitimate interests of the person responsible

to weigh up.

Since the use of bodycams for the reasons mentioned at the outset

affected persons a deep encroachment on their fundamental rights and fundamental

means freedoms, it should only be considered if the

Weighing of interests in favor of those responsible fails. this is the

Case when at least the following measures are taken to

to take account of the legitimate interests of those affected:

– In actual use (see above), the bodycam may only be activated if

if a corresponding incident is to be expected. The target person must go ahead

be informed of the recording when the bodycam is switched on.

If the situation is already defusing as a result, the bodycam may

not be activated. Continuous operation is not permitted. incidents are closed

document.

– When activating the bodycam, an optical signal must be activated

("red light"), which indicates whether the device is collecting data. In addition, should

Security forces with bodycams should be marked accordingly, for example

with labeled high-visibility vests with camera symbols.

– Should data be collected, this is sufficiently transparent

to do (Art. 5 Para. 1 DS-GVO). The requirements of Art. 12

ff. GDPR must be observed (see below).

– A pre-recording function may only be used on an ad hoc basis.

For this purpose, it must be stipulated in the operational concept that a pre-recording

may only be activated in the event of an impending danger or a situation

where there is a certain risk potential, the security personnel
but does not yet have to intervene immediately. The activation of the
Recording function must be announced by security personnel
become. After 60 seconds, the recordings of the pre-recording
automatically deleted and recorded in a black box process
maintain. If a situation escalates, i. H. a person becomes violent or
is foreseeable that a person with all probability violent
and the security personnel have to intervene, can in a second
Stage the deletion of previous recordings suspended and permanent
Recording of the bodycam can be activated. A permanent occasionless
Pre-recording, on the other hand, is also inadmissible if the collected
Video material is automatically overwritten within a short interval
will be.

– The recordings are to be stored in a black box process. The
indicates that the recordings are to be stored in such a way that access by
unauthorized access is excluded (password protection, encryption, etc.).

– To maintain the security and integrity of the recordings, location and
Embed date/time in the videos. The videos are together with a
store hash value. To ensure that recordings are not manipulated,
to log every processing step, in particular every access.
The recording person must not be granted access authorization.

– The focus of the camera must be set in such a way that a limited
Image section recorded and thus as few bystanders as possible
are affected.

– Those responsible must be in an access and authorization concept
specify when which group of people may access the recordings.

An evaluation or access to the data may only be specified

purposes, such as sending the recordings to the responsible investigators

to transmit to the regulatory authority or to assert one's own civil claims

to justify. Unneeded data must be irreversible immediately

to be deleted. A longer storage period is only justified if

if the recordings are made for the protection of legitimate interests

are required such as B. the protection of civil claims.

– Those responsible must register the data processing in the register of

Start processing activities in accordance with Art. 30 GDPR.

– The use of the bodycam must be evaluated regularly. in particular

It is more important to determine whether and to what extent the use of the standard will lead to

e.g. B. Attacks on appropriately equipped personnel are declining.

– A sound recording is generally not permitted.2

– Recordings from bodycams allow conclusions to be drawn about behavior

and employee performance. The processing of personal

The data collected must be specifically described in a company agreement

and set (cf. Section 87 Paragraph 1 No. 6 of the Works Constitution Act).

IV

transparency

The GDPR has increased the transparency requirements. alone

Clothing label "video surveillance" is not sufficient

to fulfill information obligations. According to Art. 13 DS-GVO, data subjects must

extensive information about the data processing

be communicated that goes far beyond the mere fact of the video

go out guard.

If there are recordings, those affected are immediately in a suitable

Form to inform about the data collection, e.g. B. by delivery

a leaflet which, among other things, provides information on the legal basis and the

legitimate interest behind the use of the bodycam, the rights of those affected,

the storage period, intended transmissions and the contact details

of the person responsible.3

Also against this background is the use of a pre-recording function

not compatible with the current legal situation. At the pre-record

ding – regardless of the duration – are permanently uninvolved passers-by

2

Their unauthorized production is according to §§ 201 Abs. 1, 201a Abs. 1 Penal Code, § 33

Art copyright law punishable.

3 In detail: Guidelines for transparency according to Regulation 2016/679, WP 260 rev.01,

adopted November 29, 2017, last revised and adopted April 11

2018

recorded without this being about the circumstance of video surveillance

according to Art. 13 DS-GVO can be informed or avoid this

can. The transparency requirements according to Art. 5 Para. 1, 12 ff. DS-GVO are

also to be considered during pre-recording. If this function is permanently activated,

uninvolved passers-by are permanently recorded without them

can be informed in good time about the circumstances of the video surveillance

to avoid this. This is another reason why the pre-recording function

can only be activated on an ad hoc basis (see above).

3.6

Guidance: requirements for providers of online services

on access security – as of March 29, 2019

1.

preliminary remark

Providers of online services that collect personal data from users

and users are subject to the provisions of the GDPR.

In particular, you have the regulations on security of processing

(Article 32) must be observed. This also includes measures to safeguard the

Access to the Services.

This guidance describes measures that, according to

of the data protection supervisory authorities correspond to the state of the art and

can ensure effective protection. The selection and implementation

tation is the responsibility of the providers of the online services

(Art. 24 GDPR).

Providers of online services should also follow the recommendations

of the Federal Office for Information Security in IT Basic

protection compendium for identity and authorization management

(e.g. basic requirement ORP.4.A8 "Regulation of the use of passwords"

or ORP.4.A11 “Reset Passwords”).

2.

Measures to secure access

2.1

Measure and display password strength

The strength of the passwords chosen by the users

must be measured and displayed to ensure secure password assignment

support. In particular, the length, the use of digits/

Special characters, character strings from dictionaries, country-specific keyboard

door clusters (e.g. qwertz), insecure trivial passwords (e.g. 1234567890)

as well as unsafe trivial substitutions of characters (such as o with 0 or l

through 1) to be considered. Depending on the cryptographic memory

The search procedures are usually password lengths of at least 10

Characters required to produce a reasonable password of medium quality

to speak. In addition, it should be ensured that already compromised

Passwords may not be reused.

2.2

Only force a password change in special cases

If strong passwords (according to 2.1) are used, a regular

Password change not mandatory. Changing passwords

should be enforced in particular if the service provider

Initial password allocated in a way that requires acknowledgment

Third parties cannot be ruled out (e.g. by postal delivery),

or if there is evidence of account compromise or security

there are relevant weaknesses in the software components used.

2.3

Handling failed login attempts

The failure of login attempts must be registered and the

to be displayed to the authorized person at the next successful login. After a

The number of failed attempts to be determined depending on the application should be

Registration can be blocked temporarily or permanently. Both should

Attempts to attack a specific account with changing passwords

as well as to many different accounts with no/hardly changing ones

Passwords are effectively taken into account.

2.4

Dealing with compromised services

If a provider has become aware that the service he is offering

has been compromised, he must, in accordance with Article 33 DS-GVO

competent supervisory authority and its users without delay

inform about. Appropriate measures must also be taken to

ensure that unauthorized persons with this compromised information

not have access to the accounts.

2.5

Useful notifications

Providers should inform their users about important events, such as

over that just changed a phone number or email address

was used to allow access to an account. Which includes

also successful logins from other countries.

2.6

Secure password reset

Password reset procedures must be offered that protect against unauthorized access

attempts and social engineering are resistant. Procedures that a new

Send password by email are not suitable. are state of the art

Password reset links where the link only works once and

is only valid for a short period of time (max. one hour). Especially for

a second channel must be used to recover email accounts.

Additional security questions when initiating a password reset

driving offer greater security than sending a password

Reset links without further authentication, but can use a second secure

not replace the channel. When security issues are used,

Multiple questions should be employed and alongside pre-determined questions

user-generated questions may also be possible. Incorrect entries in security

have to ask how incorrect password entries are at least temporary

lead to blockages.

2.7

Encrypted transmission of passwords

Passwords are set by the user when registering and using a

state-of-the-art cryptographically secured transport channel

to transfer the endpoint of the service provider. There must be ensured

be that these in the server application immediately in a suitable

Hash procedure (see 2.8) can be transferred.

2.8

Store passwords encrypted

Providers may only use passwords after processing them using cryptographic

One-way methods (in particular (salted) hash methods) according to the

save technique. Storage by means of symmetrical closures-

algorithms (e.g. AES) is usually not necessary and leads to

increased risk, the encryption key should be next to the

encrypted data is stolen.

2.9

Secure password databases from unauthorized access

Providers must maintain the databases in which they store user passwords

secure against unauthorized access by your own staff and third parties.

This includes regular independent penetration and vulnerability tests

to perform.

2.10

Training of vendor employees

Providers must regularly inform their employees about data protection issues

and information security training. This applies in particular to training

to sensitize employees to social engineering attacks.

2.11

Offer two-factor authentication

In addition to password protection, two-factor authentication should

be offered. The second factor must be on another device, a

another communication channel or other sufficient separation

between password and management of the second factor. Once

activated, two-factor authentication may only be carried out using

measure safer procedures can be disabled. A two-factor

Authentication is not just a recommendation for high-risk processing

development, but necessary to achieve an appropriate level of protection.

Preference should be given to open methods such as time-based one-time password

Algorithm (TOTP) are offered, not with a disclosure

additional personal data (mobile phone numbers).

are. Are used by the provider of two-factor authentication anyway

personal data such as mobile phone numbers processed are suitable

To offer guarantees which limit the purpose of the data exclusively

for two-factor authentication permanently. Should continue

standardized procedures such as WebAuthn are supported.

2.12

Separation of authentication and user data

In order to limit the consequences of a possible compromise of data

ken, the data used for authentication, in particular passwords

words, logically separated in different database instances from the

Content data is stored. This can also be done through a separate

Encryption of the content data can be effected.

2.13

Learn about password managers

Users should have suitable password manager solutions

and informed of their use.

2.14

Security as an integrated task

To achieve an adequate level of protection, security must

application as a whole. Dealing with passwords

and the use of an effective authentication process

represents an important building block. The security concept of an application

must be regularly audited, evaluated and improved in accordance with Art. 32 GDPR

become. The principles of data protection by design and data protection

tection-by-default (Article 25 GDPR) must be observed.

200

Appendix I - Privacy Materials

3.7

Conference of Independent Data Protection Authorities

of the federal and state governments – March 2019

Regulatory guidance for providers of

telemedia

Contents

201

I

introduction

The conference of independent data protection authorities of the federal and

of the federal states published a position statement on April 26, 2018

Applicability of the TMG for non-public bodies from May 25, 2018.

At the same time, the data protection authorities decided to hold a consultation

business associations and companies concerned.

As a result of the evaluation of the statements in the consultation process

and to explain and specify the positioning

the data protection authorities formulated the following supplement. The paper

should also serve as a guide for the implementation of the data protection

legal requirements for the processing of user data4

served by telemedia services.

The orientation aid is subject to the express reservation of a future

current - possibly deviating - understanding of the relevant

Regulations by the European Data Protection Board (EDPB) as well

any change in the law due to the future entry into force of a

Revision of Directive 2002/58/EC.

II.

No applicability of data protection regulations

of the TMG

The Telemedia Act (TMG) is still in all its components

Power. An adaptation of the data protection regulations of the TMG (4.

Section; §§ 11 ff. TMG) to the General Data Protection Regulation (GDPR)

was not made. A formal act of implementation of the ePrivacy Directive

line 2002/58/EG as amended by Directive 2009/136/

EG5 (ePrivacy Directive) has not been implemented in Section 4 of the TMG.6 In particular

In particular, there is no implementation act for Art. 5 Para. 3 of the ePrivacy Directive

4 Everyone should always feel addressed. For the sake of simplicity

For readability, however, only one form is used in the following.

5 If a provision of the ePrivacy Directive is mentioned below, it is always the

current as amended by Directive 2009/136/EC.

6 So also BGH, decision of October 5th, 2017, Az.: I ZR 7/16, Rz. 16; in relation to Article 5(3).

the ePrivacy Directive 2002/58/EC as amended by the Directive

2009/135/EG see the study published by the EU Commission: “ePrivacy Directive:

assessment of transposition, effectiveness and compatibility with proposed data protection

tion Regulation” (SMART 2013/0071), Final report, 2015, Section 5.2, available at: https://

ec.europa.eu/digitalsingle-market/news/eprivacy-directive-assessment-transposition-

effectiveness-and-compatibility-proposed-data.

in German law as a whole.7 This raises the question of which

Applicability of the regulations of the 4th section of the TMG since the

Obtaining the GDPR.

1.

Priority of application of the GDPR and conflict of laws in Art. 95 GDPR

In principle, member state data protection regulations apply

superseded by the GDPR due to the priority of application,

if there are no specific regulations that already exist

order existing regulations or opening clauses for leeway

leave it open or specify it in the Member States.

Article 95 of the GDPR contains a conflict rule on the relationship between
GDPR on the ePrivacy Directive. Thereafter be natural or legal
Individuals in relation to processing in connection with the provision
publicly available electronic communications services in public
Communication networks in the Union by the GDPR no additional
Obligations imposed, insofar as they are specified in the ePrivacy Directive
are subject to specified obligations that pursue the same goal.
According to Art. 288 TFEU, directives require in contrast to ordinances
implementation by the Member States. Basically, only the in unfolds
Implementation of the directive created by Member State law Legal effect
towards individuals; a directive itself cannot impose obligations on it
Justify some. The conflict of laws rule in Art. 95 GDPR therefore includes the
Member State regulations issued in implementation of the ePrivacy Directive
ten. This applies above all to the provisions of the Telecommunications Act
(TKG), which is to be regarded as the implementation of the ePrivacy Directive 2002/58/EC
are. Directive 2009/136/EC extended the scope of the
ePrivacy policy expanded. The regulation of Art. 5 Para. 3 ePrivacy Directive
does not only address providers of public telecommunication services
but also providers of “information society services”.
These correspond to the services in Germany as telemedia services
designated and regulated by the TMG. Special data protection
legal requirements can be found in §§ 11 et seq. of the TMG. these can
however, only apply in addition to the GDPR if it is
these are implementations of the ePrivacy Directive and they are therefore
Collision rule of Art. 95 GDPR.

7 See the Final Report, fn. 3, loc. a. O.

2.

No implementation of the ePrivacy Directive by §§ 12, 15 Para. 1 TMG

From the answers to a questionnaire by the EU Commission on the implementation

5 Para. 3 ePrivacy Directive, it is clear that the requirements of

Art. 5 Para. 3 ePrivacy Directive through the already existing regulations

in § 12 and § 15 TMG as sufficient implementation of the guideline

have been. In the answers to the questionnaire, the BReg

stated that § 12 TMG makes it clear that personal data should be

connection with the provision of telemedia without consent only

processed if expressly permitted by law. One

such legal permission contains § 15 TMG. For storage and

the retrieval of information such as B. Cookies, this means that such

Procedures in Germany without the consent of the user are only permissible

if this is necessary for technical reasons for the claim.

Otherwise, such procedures should not be carried out without the consent of the user.

be applied.8 As a result, this means that the German legislature

is assumed that an implementation in the form of a statutory

Adjustment is not necessary because the consent requirement of the

Art. 5 para. 3 ePrivacy-RL already from § 12 and § 15 para. 1 TMG,9 d. H. out of

the basic concept of the ban with the reservation of permission.

In the absence of legal permission in § 15 Para. 1 TMG for the in Art. 5 Para. 3

ePrivacy Directive, the general rule of Section 12 applies

TMG, i.e. H. the implementation of the ban regulated in Art. 7 letter a GDPR

subject to permission, for use. 10 A study by the EU Com-

mission11, which deals with the implementation of the ePrivacy Directive in the individual

Member States concerned, comes to the conclusion that the provision

was not implemented by the German legislator. It says there that

in Germany the view had been taken that the existing

Provisions of the Telemedia Act on the processing of personal

gene data by (information society) service providers are sufficient,

to protect users and participants.12

8 See the Final Report, loc. a. O.

9 Conrad/Haussen in Auer-Reinsdorff/Conrad, IT and data protection law manual, 2nd ed.

2016, § 36 para. 12.

10 BGH decision of October 5th, 2017, Az.: I ZR 7/16, Rz. 22 with further evidence.

11 EU Commission, “ePrivacy Directive: assessment of transposition, effectiveness and

compatibility with proposed Data Protection Regulation" (SMART 2013/0071), Final report,

2015

12 EU Commission, “ePrivacy Directive: assessment of transposition, effectiveness and

compatibility with proposed Data Protection Regulation" (SMART 2013/0071), Final report,

204

The construction of the "implementation" through the ban with the reservation of permission

in § 12 i. In conjunction with Section 15 (1) TMG, however, already due to the

decisions of the ECJ on dynamic IP addresses and the judgment of the

BGH of May 16, 2017 on the required directive-compliant interpretation of the

§ 15 para. 1 TMG faltering. Because the directive-compliant design

requires according to the BGH that § 15 Abs. 1 TMG to that effect

is to be interpreted that "a provider of online media services

data drawn from a user of these services without their consent

only collect and use beyond the end of a usage process

may, insofar as their collection and use are necessary, in order to

to ensure the general functionality of the services". This further

Going permission goes beyond the possibilities, which after the narrow

Exceptions in Art. 5 Para. 3 Sentence 2 ePrivacy Directive without consent

are permissible, since the data beyond the usage process to the general

Functionality can be saved.

In addition, it should be noted that §§ 12 and 15 TMG are not implemented

of Art. 5 Para. 3 ePrivacy Directive, but rather an implementation

of Art. 7 Data Protection Directive 95/46/EG (GDPR). According to Art. 94

Para. 1 GDPR, the GDPR was repealed with effect from May 25, 2018.

The regulations on the legality of the processing of personal data

Data are now covered in Art. 6 GDPR. There is also found

the requirement that data processing is only lawful if

at least one of the requirements specified in Art. 6 Para. 1 is met.

For a repetition of the ban subject to permission in the national

Law in the form of § 12 TMG does not exist in addition to the GDPR.13

The collision rule of Art. 95 GDPR also refers to

"specific obligations laid down in Directive 2002/58/EC". Such

"special" obligations result from the general concept of the prohibition

not with permission.

As a result, it can be stated that Art. 95 DSGVO for § 12 and § 15

Para. 1 TMG does not apply.

2015, Section 5.2, available at: https://ec.europa.eu/digital-single-market/news/eprivacy-

directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

13 pages instead of many in Nettesheim, in: Grabitz/Hilf/ders. (Ed.), The Law of the EU, TFEU, Art. 288,

Rn. 101 f., with w. N.

205

3.

No implementation of the ePrivacy Directive by § 15 Para. 3 TMG

Unlike the federal government, the BGH takes in its order for reference

of October 5, 201714 with regard to the implementation of Art. 5 Para. 3

ePrivacy-RL primarily § 15 Abs. 3 TMG in view.15 This is logical

against the background that Art. 5 Para. 3 ePrivacy-RL also the storage

or access to information stored in the end device of the user

are recorded, such as the use of cookies. § 15 paragraph 3

TMG provides legal permission for the creation of usage profiles

available under a pseudonym, which can also mean usage profiles,

created with the help of cookies. With regard to the question of

Implementation of Art. 5 Para. 3 ePrivacy Directive is therefore a dispute

with § 15 Abs. 3 TMG and the examination of a guideline-compliant interpretation

required.

According to § 15 Abs. 3 TMG the service provider was allowed for advertising purposes,

market research or for the needs-based design of telemedia

Create usage profiles using a pseudonym, provided that the

users do not object. The purposes mentioned in § 15 Abs. 3 TMG

do not correspond to the exceptional circumstances of Art. 5 Para. 3 Sentence 2 of

ePrivacy RL. This means that for the purposes specified in Section 15 (3) TMG

According to Art. 5 Para. 3 ePrivacy Directive, the consent of the participants

mer or user is required. The consent i. See the ePrivacy Directive

is, according to Art. 2 Sentence 2 lit. f), a consent i. s.d. DSRL. According to

Art. 94 para. 2 GDPR, references to the GDPR become references to

the GDPR, so the question of what requirements for consent

are to be submitted from May 25, 2018 in accordance with the GDPR

words is. Art. 95 GDPR does not change this either. Consent is in

of the ePrivacy Directive, as mentioned, is not regulated independently, so that

insofar as there is no lexspecialis situation.16

A notice:

The decisive difference between a contradiction solution (opt-out)

and a consent (opt-in) is that in the case of an objection solution

First, data processing takes place, which is only possible by declaration

an objection can be prohibited for the future. It's different

This is the case, however, if consent (opt-in) is required. Then may

14 BGH, decision of October 5, 2017, I ZR 7/16.

15 BGH, decision of 5.10.17, I ZR 7/16, para. 13, 16

16 Kühling/Buchner, GDPR 2017, Art. 95 para. 7.

data processing can only take place after an effective

Consent has actually been given by the user.

According to Art. 4 No. 11 GDPR, the consent must be in the form of a declaration

or other clearly confirming action. consider

reason 32 it can be inferred that “silence, already ticked

Box or inaction of the data subject […] therefore no consent

[should] represent". In addition, the right to object is limited

on the consent regulated separately in the GDPR in Art. 21. Before this

Background can be ruled out that the omission of a

objection a consent i. s.d. DSGVO can represent.

A direct application of § 15 Para. 3 TMG as implementation of Art. 5 Para. 3

ePrivacy Directive in the version amended by Directive 2009/136/EC

has therefore been eliminated since May 25, 2018.

4.

No guideline-compliant interpretation of Section 15 (3) TMG

Only a directive-compliant interpretation can be considered for retention

15 Para. 3 TMG in order to continue to comply with the provision on Art. 95 GDPR

apply. The first question that arises is whether Section 15 (3) TMG, i. H.

the objection solution can be applied in such a way that this is not allowed

leads to a result contrary to the Directive. Anyway, this is it

not the case since May 25, 2018. The contradiction solution does not fulfill

the requirements for consent in accordance with Art. 7 GDPR.

5.

No opening clause for non-public bodies

The retention of the regulations of §§ 12, 15 paragraph 1 and 15 paragraph 3 TMG

for non-public bodies cannot be replaced by an opt-out clause

GDPR are justified. The regulations in the national

Law which, according to the German legislator, is an implementation of

Art. 5 para. 3 ePrivacy Directive or for such an implementation in

come into consideration, no longer applicable.

6.

No immediate application

Direct application of the ePrivacy Directive is also out of the question

consideration. According to the case law of the ECJ, individuals can

under certain conditions compared to a non-implementation

Member State directly invoked a provision of an EU Directive.17

Requirements are u. a. a lack of or poor implementation18

and that the norm of the directive is unconditional and sufficient in terms of content

is accurate.19 However, a directive cannot itself impose obligations on

Justify Private.20

7.

intermediate result

Since Art. 5 Para. 3 ePrivacy Directive has not been implemented in Germany and

neither a directive-compliant interpretation nor a direct effect

of Art. 5 Para. 3 ePrivacy Directive come into question, arise from this

for telemedia service providers in Germany no sector-specific

Obligations within the meaning of Art. 95 GDPR, so that its requirements

in this respect not applicable. In addition, there are no opening clauses in the

DSGVO, which justify the applicability of § 15 TMG. It therefore remains

in the general application of the provisions of the GDPR.

III.

lawfulness of processing

1.

introduction

For convenience when referencing specific operations in the area

of usage data processing uses the position determination e.g.

the term "tracking". Acts according to the understanding of the supervisory authorities

"Tracking" is data processing for - usually website

overarching – tracking individual behavior of users.

17 BVerfGE 75, 223; ECJ [2002] ECR I-6325, (Marks & Spencer), paragraph 24.

18 CJEU, Case 152/84 [1986] ECR 723, (Marshall I), para. 46.

19 ECJ, case 148/78 [1979] ECR 1629, (Ratti), paragraph 23. 17 ECJ, case 152/84 [1986] ECR 723,

(Marshall I), paragraph 48; Joined Cases 372 to 374/85 [1987] ECR 2141 (Traen), para. 24; Case 14/86,

1987 ECR 2545 (Pretore di Salò/X), para. 19; Case 80/86 [1987] ECR 3969 (Kolpinghuis

Nijmegen), paragraph 9; Case C221/88 [1990] ECR I-495 (Busseni), paragraph 23; Case C-106/89, ECR.

1990, I-4135 (Marleasing), paragraph 6; Case C-168/95 [1996] ECR I-4705 (Arcaro), paragraph 36 et seq.; Rs.

C-97/96 [1997] ECR I-6843 (Daihatsu Germany), paragraph 24; Case C-201/02 [2004] ECR I-723

(Delena Wells), paragraph 56.

20 EDPB, Guideline on consent, WP 259, p. 16. 21. See also letter of formal notice

the CNIL to Vectaury of 9 November 2018, information available at https://

www.cnil.fr/en/node/24929.

This understanding of the term corresponds to that used by the European

supervisory authorities in publications.21

For the assessment of admissibility, however, the sole decisive factor is whether a

certain processing activity is carried out lawfully and the

responsibly meets all data protection obligations of the GDPR.

Data processing is only lawful if at least one of the

Conditions of Art. 6 Para. 1 GDPR are present.

2.

lawfulness of processing

All permissions of the GDPR are considered equal and

to be considered equivalent. In Art. 6 GDPR, the conditions for

determine the lawful processing of personal data and

describes six legal bases that controllers rely on

can.22 For the processing of personal data by non-public

other persons responsible for the provision of telemedia services

In particular, the following permissions are considered:

a. Article 6 Paragraph 1 Letter a) GDPR – Consent

b. Article 6 Paragraph 1 Letter b) GDPR – Contract

c. Article 6 paragraph 1 lit. f) GDPR – balancing of interests

A notice:

Responsible persons must, within the scope of their accountability from Art. 5

Para. 2 DSGVO prove that the processing of personal

data is lawful. This means that those responsible check in advance

and have to document on which ones

Permission they support the processing. Users must have

the legal basis for all processing of your personal

be informed of any data (duties to provide information according to Art. 13 f. GDPR).

In the following, the above Permissions explained in more detail.

21 Art. 29 Working Party on Data Protection, WP 194 of 7 June 2012, p. 10; EDPB, Guideline on Consent,

WP 259, p. 4 (available at https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/

Content2/Article-29-Group/wp259-rev-0_1_EN.PDF).

22 EDPB guideline on consent, WP 259, p. 27 (available at https://www.ldi.nrw.de/

mainmenu_Service/submenu_Links/Content2/Article-29-Group/wp259-rev-0_1_DE.PDF).

a) Article 6(1)(a) GDPR – Consent

Art. 4 No. 11 and Art. 7 GDPR require a self-determined and informed
Consent of the persons concerned in the respective data processing.
This presupposes that any data processing is transparent and
have to be enforceable. Especially if at
data collected from the data subject by the respective service provider
(incl. integrated services) merged across websites and
are evaluated, it must be taken into account that the persons concerned
for an effective consent in advance about any form of the carried out
ten data processing and all recipients are informed in detail
and must be given the opportunity in the individual forms of
to specifically consent to data processing. In cases where there are several
(joint) controllers want to base on the requested consent
or in which the data is transmitted to or by other responsible parties
are to be processed by other controllers, these organizations must
sations all named23 and the processing activities of each
organizations are adequately described. In these cases must
all actors involved check whether an effective consent for their
activities and whether these can be proven by you
(Article 5 (2) GDPR).21 Processing of personal data without
sufficient knowledge of the persons concerned

– about the respective data processing operations,
– about the third parties involved as well as
– without the possibility of separate consent

leads to the ineffectiveness of the consent and therefore takes place without legal reason.

It is essential to provide data subjects with information

provide functions to obtain effective consent from them

to be able to Only in this way is it possible for data subjects to make decisions in

knowledge of the specific situation and the scope of consent

to understand.

Art. 4 No. 11 GDPR further requires an “un-

Misleading declaration of intent in the form of a declaration"

or any other unequivocal confirmatory action with which the

data subject indicates that they consent to the processing of them

relevant personal data expressly agrees.

This can be done, for example, by ticking a box when visiting

23 EDPB, Guideline on consent, WP 259, p. 16. 21. See also letter of formal notice

the CNIL to Vectaury of 9 November 2018, information available at https://

www.cnil.fr/en/node/24929.

a website, by selecting technical settings or by

any other explanation or active behavior happened with the

data subject clearly their consent to the announced

and intended data processing expresses.

Opt-out procedures are not sufficient for this. In this respect, recital

32 GDPR explicitly states that implied behavior such as "silent

already ticked boxes or inaction of the data subject”

do not represent consent.

Note: "Cookie Banner" & "Consent Tools"

Through an upstream query when you first visit a website or

a web app can e.g. effective consent for consent-requiring

tige24 data processing can be obtained. However, there are the following

Requirements to note:

– When opening a website for the first time, the banner appears, for example

se as a separate HTML element. Usually this HTML element consists

from an overview of all processing operations requiring consent,

those naming the actors involved and their function are sufficient

are explained and can be activated via a selection menu. active

four in this context means that the choices

must not be preset to "activated".

– While the banner is displayed, everyone will move on at first-

the scripts of a website or web app that potentially contain user data

capture, blocked. Access to imprint and privacy policy

must not be prevented by "cookie banners".

- Only when the user has given his/her consent(s) through an active action,

such as ticking the banner or clicking

has submitted to a button, the consent-requiring

Data processing actually (ensured by technical measures)

puts) take place.

- In order to fulfill the obligation to provide evidence of Art. 7 Para. 1 DSGVO, it is acc.

Art. 11 para. 1 GDPR does not require users to do this directly

be identified. An indirect identification (cf. recital

26) is sufficient. So that the user's decision for or against

consent is taken into account when the website is called up again

and the banner does not reappear, their result may depend on

24 The use of cookies does not require consent per se. Appropriate banners

should therefore only be used if consent is actually required.

211

the end device of the user without using a user ID or similar

those responsible are saved. Through such a procedure

proof of existing consent must be provided.

– Since consent can be revoked, a corresponding option must

ability to revoke be implemented. The revocation must be so simple

be possible such as the granting of consent, Art. 7 Para. 3 S. 4 DSGVO.

Controllers must ensure that consent is not just that

setting of cookies that require consent, but all consent-

Processing activities that require authorization, such as e.g. B. Proceedings

the user through tracking pixels or various fingerprinting methods, if these

are not permitted on another legal basis.

It is also sufficient for consent i. s.d. GDPR not if, as with

many simple cookie banners on the web, an indication of the setting of

cookies together with an "OK" button. In these cases it is absent

in the voluntariness required under Art. 7 GDPR if the data subjects

People can press "OK" but are not given the opportunity to do so

reject the setting of cookies.

Consent must be voluntary, i.e. given without coercion

the. Consent is only voluntary if the data subject is a genuine

and has free choice and is thus able to give consent as well

to be able to refuse without suffering any disadvantages (recital

reason 42 GDPR). Also a coupling of the provision of a contractual

Service to the submission of a data protection consent

According to Art. 7 Para. 4 DSGVO regularly leads to the consent

cannot be regarded as voluntary and is therefore ineffective.25 The

Visiting a website should still be possible even if affected

People decide against the setting of cookies and not in the

consent to personal data processing. A consent applies after

Recital 43 GDPR not given voluntarily even if to

various processing operations of personal data

consent cannot be given separately. If at sites

consent is obtained through upstream queries, the

individual processing operations can therefore be selected separately.

Finally, Art. 25 Para. 2 GDPR must be observed, which is

requires those responsible under intellectual property law to use suitable technical and organizational

to take organizational measures to ensure that data

protection-friendly default settings only processes personal data

are required for the respective specific processing purpose

25 EDPB, Guidelines on Consent, WP 259, p. 9.

are. Consequently, not least according to the principles “data

protection by design” and “data protection by default” (Recital 78

GDPR) to ensure that the technical devices work as well

are set in a data protection-friendly manner and thus obtaining an effective

allow consent. In addition, by the data protection law

Those responsible technically ensure that procedures for tracking

of user activities that require consent under data protection law,

only be used when the data subject has the information

The content of the planned data processing is recorded and a decision is made

in the form of an explicit declaration of intent.

b) Article 6(1)(b) GDPR – Contract

The processing of personal data of the contractual partner

contractual basis is only possible according to Art. 6 Para. 1 lit. b) GDPR,

if the data processing is for the performance of a contract or within the framework

pre-contractual measures are required, at the request of those concerned

person. In view of the ongoing discussions on a European

Level on the question of the applicability of Article 6 (1) (b) GDPR in addition

connection with the provision of online services is currently

waived statements on Art. 6 (1) lit. b) GDPR at this point in time.

c) Article 6 Paragraph 1 Letter f) GDPR – balancing of interests

The balancing of interests in accordance with Art. 6 (1) (f) GDPR is

a regulation with a wide and unspecific scope.

On the one hand, this has the advantage that the provision is flexible and

Variety of situations can be applied. On the other hand, this leads to

Legal uncertainties and questions regarding the application in specific individual cases.

Criteria are set out below to facilitate application

should and at the same time be able to help the accountability requirements according to the

to comply with GDPR.

When processing personal data on the basis of

Art. 6 (1) lit. f) GDPR must be taken into account that the provision does not

constitutes a catch-all event. The processing is lawful only if this

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 prevail. Whether the prerequisites

213

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

6 Para. 1 lit. f) GDPR are met, is based on a three-stage

check to determine:

1st stage: Existence of a legitimate interest of the person responsible

or a third party

2nd stage: Necessity of data processing to safeguard these interests

eat

3rd stage: Weighing up the interests, fundamental rights and fundamental freedoms

of the person concerned in the specific individual case

A notice:

This test structure is intended to verify the requirements of Art. 6

Para. 1 lit. f) GDPR facilitate and is based both on the legal

opinion of the ECJ as well as the opinion of the European

inspection authorities.

1st stage:

Existence of a legitimate interest of the person responsible or a

third party

Providers of telemedia services can use a large number of legitimate

have food.26 The GDPR defines the concept of “legitimate interest”

not and only gives isolated examples of a legitimate interest. The

legitimate interest is closely related to the processing purpose

and can be of an economic, non-material or legal nature. The concept of

"legitimate interest" can be considered the main motive for the processing

be understood and reflects the benefit that the person responsible for

want to withdraw from processing.

This includes, for example, the provision of the service in a form that

enables a user-friendly perception of the online offer.

In recital 47, the GDPR also expressly states the prohibition

fraud prevention and direct marketing as possible legitimate interests.

Legitimate means that the interest is in accordance with the law.

This means that in any case illegal or discriminatory motives

under no circumstances can justify a legitimate interest.

Other interests held by telemedia service providers for processing

of usage data include:

26 p. in detail example WP 217.

– Provision of special functionalities, e.g. B. the shopping cart function

using a so-called session identifier

– Free design of the website, also with efficiency and cost savings

security considerations, e.g. B. Embedding content hosted on other servers

be hosted, use Content Delivery Networks (CDN), Web

Fonts, map services, social plugins, etc.

– Integrity and security of the website (IT security measures are e.g.

the storage of log files and in particular IP addresses for one

longer period in order to be able to recognize and ward off abuse)

– Reach measurement and statistical analysis

– Optimization of the respective web offer and personalization/individual

of the offer tailored to the respective user

– Recognition and attribute assignment of users, e.g. e.g.

funded offers

– Fraud prevention, repelling requests that overload the service

(denial of service attacks) and bot usage

A notice:

The examples given can be a legitimate interest on the first level

justify. For the admissibility of data processing for these purposes

but it depends on the necessity and the balancing of interests.

2nd stage:

Necessity of data processing to protect the legitimate

Interests

The mere existence of a legitimate interest is not sufficient to

to legitimize data processing. It is imperative that the respective data

processing is necessary to safeguard this interest. necessity

means that the processing is suitable for the interest (motive/benefit of the

processing) of the person responsible, with no milder, equal

effective means are available. That means the responsible

limit the processing to what is necessary.

Example:

The person responsible runs a website and would like to know how

Online offer is accepted and whether improvements may be made

required are. To do this, he would like to know how many users the website is in

a certain period of time, which devices the users use

and what language settings they have. The person responsible requires

this information in order to optimize its website and the presentation

adapt to the end devices.

The measurement of reach and the resulting information

are suitable for adapting the website (legitimate interest).

If the website operator uses an analysis tool for this, which data

about the usage behavior of data subjects to third parties (e.g.

social networks or external analytics services that collect usage data about the

Merge across the website with data from other websites

ren), this is no longer necessary. The goal - reach measurement - can

can also be achieved with milder, equally suitable means that clearly

collect less personal data and do not transfer this to third parties

media (e.g. without the involvement of third parties via a local implementation of a

analysis software).

3rd stage:

Weighing against the interests, fundamental rights and fundamental freedoms of the

data subject in a specific individual case

The legitimate interests of the person responsible are the interests as well as

fundamental rights and freedoms of users.

This not only includes the right to protection of personal data

according to Art. 8 Charter of Fundamental Rights of the European Union (GRCh) or

the right to confidentiality of communication according to Art. 7 GRCh, otherwise

but also the freedom of expression and the interest in one

free information gathering, Art. 11 GRCh. Also other freedoms and

Interests of the persons concerned must be taken into account, for example

the interest in not suffering any economic disadvantages (e.g. in the case of personal

nalized pricing).

The right to confidentiality of communication protects against the use

Creation of unique identifiers, such as e.g. B. IMEI number, IMSI number,

MAC address or Ad-IDs (device-specific advertising numbers). There-

In addition to being protected, the (device) integrity is also protected. Will e.g. B. identifier

stored on the user's end device, the integrity of the device is affected.

As part of the consideration, the design of the processing of personal

personal data and the specific effects of the processing

on the persons concerned to be taken into account. at this stage of the test

is at the core of the balancing of interests.

The identified conflicting interests are to be weighted.

No general rule can be established for this. responsible

can, however, be guided by the following principles:

– A specific, constitutionally recognized interest, e.g. B. Right

on the protection of personal data in accordance with Art. 8 GRCh, has a higher priority

weight, as an interest that only simple law in the legal order

tion is recognized.27

– An interest is more important if it not only serves the person responsible,

but at the same time also to the general public, e.g. B. in research activities

s whose findings are to be used for preventive medicine.

It should be noted that within the scope of the consideration, existing

Obligations from the GDPR, e.g. B. Information requirements or the security of

Processing by pseudonymization, not in favor of the person responsible

can be taken into account. The general obligations of the GDPR

do not represent "best practices", but are legal requirements,

which must be fulfilled in any case. Nevertheless, by additional

Protective measures the impairments caused by processing

be reduced in such a way that the weighing of interests in favor of the

answerable.

A notice:

With regard to the use of pseudonyms, it should be noted in general

ken that the fact that users have about IDs or identifiers

be made identifiable, no pseudonymization measure i. s.d.

GDPR represents. In addition, these are not appropriate guarantees

Compliance with data protection principles or to protect rights

affected persons, if for the (re-)recognition of the user IP addresses,

Cookie IDs, advertising IDs, unique user IDs or other identifiers for

come into action. Because, unlike in cases where data is pseudonymised

be used to obscure or delete the identifying data, so

that the persons concerned can no longer be addressed

IDs or identifiers used to distinguish the individual individuals

and make it addressable. Consequently, there is no protective effect.

It is therefore not a matter of pseudonymization i. s.d. recital 28, the

reduce the risks for data subjects and those responsible

and the processors in complying with their data protection obligations

support. In addition, it must be taken into account that users in

in most cases sooner or later somewhere on the web

27 Art. 29 Working Party on Data Protection, WP 217.

register and in these cases also a link to e-mail addresses,

Clear names or offline addresses is possible. On the knowledge of the

However, there is a common name for the identification of data subjects

not applicable to personal reference. When using the web, as with many

people, reflects a large part of the reality of life, then it is

It is relevant whether the users can be determined via their online identifiers or

are addressable. The GDPR assumes that indirect identification

can also be done by separating (recital 26 p.3).

In order to apply Art. 6 Paragraph 1 lit. f) GDPR in individual cases, i.a. the

Recitals of the GDPR can be used in support. Out of

they result in particular from the following criteria, which apply in individual cases

The following are to be used in the context of the balancing of interests:

a. Reasonable expectation of data subjects and foreseeability

/ Transparency

b. Possibilities of intervention for the persons concerned

c. concatenation of data

i.e. Actors involved

e. duration of observation

f. Categories of Data

G. Scope of data processing

H. Group of those affected (e.g. particularly vulnerable persons)

a) Reasonable expectation of data subjects and foreseeability

/ Transparency

According to Recital 47, the reasonable expectations of the

data subject based on their relationship with the controller,

are taken into account. In addition to the subjective expectations of those affected
Person is also asking what objectively can reasonably be expected
can. The expectations cannot be
further mandatory information (Art. 13, 14 GDPR). Critical
is it to be evaluated when different actors work together and the
relationships between the actors under data protection law are unclear
or are not defined (responsible, processor, common
Responsible).
With regard to the integration of third-party services, a user expects
Usually not that to these third parties to which the user regularly
does not maintain any relationships, information about it is passed on,
which websites they visit or which apps they use. Anyway then

if the third parties process the user data for their own purposes
the consequences and potential risks to interests, fundamental freedoms and
Fundamental rights of the persons concerned neither assessable nor assessable.
This applies in particular to the risk of visiting other services or the
To be (re)recognized when using other devices and thereby e.g. B. at
to be externally controlled in the acquisition of information.
This processing does not meet the reasonable expectations of the
Users because they are only disadvantageous in terms of self-determination
affect. Likewise lie techniques, which the behavior of visitors
when interacting with an information society service
be able to understand and document, e.g. B. in the detection of
Keyboard, mouse and swipe movements on touch screens, outside of the

expectations of the user.

Example – range measurement:

The user calls up a website. He assumes that the website of

is made available to a single controller, namely by

the one with which there is a direct user relationship at the time of access

consists.

Third-party services in apps or on websites are affected by

However, people do not consciously perceive it and regularly without any action

activated because the person responsible has integrated them into his online offer

(e.g. tracking pixels of an advertising network).

In contrast, it is foreseeable for the user that the

responsible measures the reach of its online offer, around that

Customize online offerings. For this purpose there are none

ongoing recognition and ever more extensive profile building as well as

no transfer of data to third parties necessary. provide statistical information

sufficient information about the general usage behavior, so that the

Provision of individual usage profiles for the purpose of range

measurement is not required. The impairment of the user is then as

to be rated low with the result that the weighing of interests in favor

of the person responsible fails.

b) Options for intervention by the persons concerned

As part of the balancing of interests - possibly also as a compensation measure -

take into account, in which form the data subjects

have opportunities and be informed about the personal

To prevent or restrict data processing legally and technically

or subject to other conditions.

In doing so, e.g. B. the form of the identifier with which devices or users

be separated and recognized, play a role. Depends on

Identifier can be different ways for data subjects

give, a recognition or tracking of usage behavior

to restrict. In the browser settings, for example, users can

delete cookies. With device fingerprinting, on the other hand, it is practical

impossible to prevent a (re-) recognition by the user.

In addition, the data subjects can, via Art. 21 GDPR

Additional - non-mandatory - rights of objection are granted

become. Art. 21 GDPR provides that the data subject

is right, for reasons that arise from their particular situation,

against the processing of personal data concerning you at any time,

which takes place in accordance with Art. 6 Para. 1 lit. f) to file an objection. The general

The right to object under Art. 21 GDPR is therefore not unconditional. vacates

the person responsible, on the other hand, grants the user from the outset a

unconditional right of objection, this can contribute significantly to

that the balancing of interests is in favor of the person responsible.

Example – range measurement:

The website operator integrates a range measurement tool. The user

Find information about an opt-out procedure in the data protection regulations

ren, which he can carry out at any time. To do this, he clicks on a link that leads to

leads to an opt-out procedure by the provider. The opt-out procedure was

checked in advance by the website operator. Responsible for the implementation of

The website operator remains the objection, even if the provider of the

Tools for range measurement provides an opt-out procedure.

After clicking on the link, the objection will be implemented immediately. One

further processing of the usage data for statistical analyzes (reaching

distance measurement) no longer takes place.

If personal data is processed in order to operate direct advertising,

However, there is anyway a right of objection without conditions, too

for profiling in connection with direct advertising (Article 21 (2) GDPR). In

In these cases, granting the right to object does not affect the

balancing of interests. From Art. 25 Para. 2 GDPR and the recital

Reason 78 also results in the person responsible having suitable technical

and must take organizational measures that include making sure

technical default settings made by the user on their end

devices to protect their personal data (e.g. "Do Not Track")

also be complied with. A technical bypass of the desired

Preferences, such as the use of Deadline Party cookies

due to blocked third-party cookies, is not permitted.

c) concatenation of data

It is necessary to consider the possibilities of linking, duplication

of data records (e.g. due to a higher number of data processing

actors) and enrichment of data sets, in particular purpose-independent

pending, exist and what the resulting risks are for the persons concerned

develop.

It can also play a role in the context of data concatenation

Play what kind of identifiers are used. In addition,

Linking usage data and content data (e.g. from customer accounts)

as well as the cross-device concatenation of data increases the risk

works. In addition, it must be included in the assessment if over

Analysis tools Third parties are involved as service providers who have a link

carry out tests with your own data or data from different customers,

Bring sites and devices together.

In addition, these procedures must be designed technically and organizationally in such a way that

a personal reference is removed as soon as possible and usage profiles - if

at all – are created under pseudonyms. However, this turns out to be the case

usually already from the requirements of Art. 5 DSGVO and its

technical and organizational implementation according to Art. 25 GDPR, in particular

special Art. 25 Para. 2 GDPR (privacy by default).

These requirements, like the fulfillment of the transparency requirements

12 et seq. GDPR, so that these

in the context of the balancing of interests not in favor of the person responsible

are eligible. In addition, the requirements

24 and 32 GDPR must be observed and corresponding technical

to take organizational measures.

d) Actors involved

The more controllers, processors and other recipients in the

processing activities are involved, the greater the impairment

for the person concerned. This is due to the fact that, on the one hand, due to the increasing

As the number of actors increases, the risk of a data breach increases.

On the other hand, the person responsible has regular opportunities to intervene

made more difficult because the actors are geographically distant and different

jurisdictions (e.g. players with branches in different

common states). The person responsible can counteract this by

takes additional technical and organizational protective measures

about the minimum requirements of Art. 5 Para. 1 lit. f), Art. 25 and Art. 32

go beyond GDPR.

e) duration of observation

Within the framework of the ratings, it is relevant how long the possibility exists

to recognize users and information on usage behavior

to collect and assign. In this context, e.g. B.

what lifespan cookies have. A very brief recognition

phase could e.g. B. also lead to compensation in other areas.

For example, the scope of information collected about the user falls within the

Balancing interests is less important the shorter the users are separated

and can be recognized.

f) data categories

The evaluation must take into account which data categories are collected

and the level of detail in which information is recorded (e.g. pro-

logging of which files were accessed, typing history recording

tion, recording of the scrolling, collection of texts from started

forms, even if they are not sent, search queries

Etc.). The processing of pseudonymous data is generally less

distressing, since the identity of the person concerned is veiled and thus

the probability is lower that the data subject by third parties

is identified. Therefore, in the context of the weighing of interests, it is also
take into account whether the data subject is directly or indirectly identifiable.
It also plays a role whether and in what form usage profiles are created
are collected, in particular what amount of usage data
adds and whether additional interests and characteristics are subsequently assigned
be used to locate the user in a specific target group and
finally to address specific target groups (profiling e.g. for purposes
advertising or personalized information). This form of profiling
takes place largely across services and devices and can thus become one
comprehensive, profound and long-lasting invasion of privacy
of the user. Extensive processing creates risks
for the rights and freedoms of users resulting in a physical, material
material or immaterial damage. For example, the
user profiles created for discrimination, identity theft,
financial loss, damage to reputation or other significant
lead to economic or social disadvantages. This risk is

to be valued higher if personality-descriptive during profile formation
aspects such as B. Work performance, economic situation, health, personal
che preferences or interests, reliability or behavior analyzed
or be forecast. Also the creation of movement profiles and
forecasts is regularly classified as a high risk.

g) Scope of data processing

The scope of the data processing must also be taken into account. This
results from Art. 24, 25, 32 and 35 GDPR. The larger the amount of

processed data, the higher the risk for rights and freedoms

the person concerned. The more data processed, the greater

the risk that through the accumulation of large amounts of data more information

emerge that may be discriminatory or defamatory

or z. B. Conclusions about special categories of data according to Art. 9

Allow paragraph 1 GDPR. The scope of data processing is above

also closely related to the storage period. Will be over a long

If data is permanently saved over a period of time, this increases the scope

of data processing.

The number of people affected also plays a decisive role

role in balancing interests. The greater the number of affected

people, the sooner and more fine-grained comparison groups can be formed

become. This can result in an increased potential for discrimination

and the danger that characteristics are identified without considering the

comparison group would not have been recognizable.

If personal data is processed that allows conclusions to be drawn about

their categories of personal data according to Art. 9 Para. 1 DSGVO

allow, consent is required in any case. These include

for example dating portals, websites of political parties, religious

Associations, online health portals or websites for

effects. Therefore, in these cases, special care must be taken when obtaining them

of informed consent covering all aspects of data collection

explained, including the fact that information about sexual

orientation or interest in the respective political parties

be passed on to third parties.

h) Group of persons concerned (children and others in need of protection

Persons)

When balancing interests, it must be taken into account which persons

are affected by processing measures. If an increased protective

need of persons is given, this leads to the fact that the interests,

Fundamental rights and freedoms of the persons concerned are given higher priority

become. This applies in particular to children who are expressly referred to in Art. 6 Para. 1

lit. f) GDPR. In addition, such considerations

also play a role if B. the collection of usage data and

the profiling of users also serves to identify special vulnerabilities

or to recognize and utilize situations of defenselessness.

It is also the relationship between the controller and the data subject

to consider. So there can be situations in which between the

an imbalance of power between the controller and the data subject

stands. This is the case, for example, in an employment relationship or when

the person responsible has a monopoly position. Is there a power imbalance

weight in favor of the person responsible, this also means that

the interests, fundamental rights and fundamental freedoms of the persons concerned

are to be weighted higher.

Example:

The website operator offers a counseling platform for addicts.

On the website, users can find information on contact options

from local advice centers also information about the disease and first

To find help. The website operator binds a variety of tools from advertising

network, which uses the website visitors' usage data for their own

processing purposes. There is a special relationship between

Website Visitors and Operators. Due to the information offered

n conclusions about special categories of personal data

pursuant to Art. 9 (1) GDPR. In addition, it is to be assumed

that users accept the information offered because they are personally affected

claim and therefore because of their special interest in

Confidentiality or largely anonymous use

are worth protecting.

IV

Conclusion

Those responsible should be aware that the balancing of interests in

A substantial discussion within the framework of Art. 6 (1) (f) GDPR

with the interests, fundamental rights and fundamental freedoms of those involved

and must be related to the specific individual case. Insufficient or

general statements that data processing pursuant to Art. 6 Para. 1

lit. f) GDPR is permissible, do not meet the legal requirements.

224

Appendix I - Privacy Materials

If the person responsible comes to the conclusion that the balancing of interests

in favor of the data subject and no other legal

basis is data processing – if at all

– only after prior informed consent (Art. 6 Para. 1 lit. a) GDPR)

lawful ("at least then...").

Appendix I – Example of a balancing of interests

Example tracking pixel:

A company (online shop for medicines and cosmetics, im
hereinafter referred to as "company") places advertisements on a social network
show. In order to be able to control and evaluate advertising in the social network,
the company binds a tracking pixel, so-called counting pixel, of the social
network on its corporate website. Using the pixel
The social network directly collects data from website visitors
recorded. The company receives information based on this user data
to the website. This includes, for example, information about how the user
arrived at the website, how he uses the website, how many users signed up for
Sign up for the newsletter and add products to your shopping cart. This information
tion uses the company to run the advertising campaigns on the social
network and avoid wastage. For an evaluation
of usage behavior and targeted advertising
switch, the social network also uses the data from the online shop
for its own purposes and draws on data from its own sources.
The company initially does not want to obtain user consent
and wonders whether data processing in accordance with Article 6 (1) (f) GDPR
can be supported.
Assessment: lawfulness of processing
According to Art. 6 Para. 1 lit. f) GDPR, the processing is personal
Data lawful if they are used to protect the legitimate interests of the
Responsible or a third party is required, unless the interests
sen or fundamental rights and freedoms of the data subject who the
require protection of personal data prevail. After that is one
Balancing the interests of the company and the interests
of the persons concerned, d. H. of the company's customers.

1st stage - Determine the legitimate interests of the controller

The company's interest in advertising on a social network

can be regarded as justified as an economic interest.

2nd stage – Necessity

The necessity for the processing of the personal data would be

given if the method described is suitable for the advertising

to optimize for the company, and alternative, equally effective means

were not available.

3rd stage - interests, fundamental rights and fundamental freedoms of those affected

Person and consideration in individual cases

On the other hand, there are the basic rights of the users of the company website

respect for their private and family life and protection of personal

General data according to Art. 7 and Art. 8 GRCh.

Within the framework of the consideration, the effects of the given processing are taken into account

not just abstract or hypothetical to consider, but it's on

to eliminate the specific effects on the individual data subject.

Among other things, the the above Criteria:

a. Reasonable expectation of data subjects and foreseeability

/ Transparency

b. Possibilities of intervention for the persons concerned

c. concatenation of data

i.e. Actors involved

e. duration of observation

f. Categories of Data

G. Scope of data processing

H. Group of those affected (e.g. particularly vulnerable persons)

By embedding the pixel on the company's website,

causes the company to collect information through the social

Network which specific users when the individual pages of the website

call. This gives the social network additional knowledge about

website visitor that it would not obtain without a tracking pixel. This

The social network uses additional knowledge for its own advertising purposes,

to determine the target groups for advertising measures. There will be one

A large amount of usage data is collected, which enables extensive profiling of the

allow users. This information is used by the social network for

uses its own profiling of users. The website visitor

cannot easily recognize integrated tracking pixels, nor

he expects his usage behavior to be recorded across websites and

is used for profiling by the social network.

While users of social networks expect personal

Data are processed by operators of social networks, which they

left directly on the social network after active use.

This includes, for example, posted photos and messages or that

"Like" posts by other users. You may also agree in general

Form aware of the profiling by operators of social networks.

However, the average social network user does not expect that

Websites integrate "invisible" pixels in order to carry out data processing

Induce third parties (reasonable expectation of data subjects) and

social networks so that data is supplied, which in turn is used to

use profiling. In any case, this is outside of what users

must reasonably expect objectively, because such data collections

by third parties only have a negative effect on the ability of users to

to control and determine the use of their own data.

In addition, the user has no possibility of data processing

to object or to express in any other way that

he does not wish to be profiled by a third party (no intervention

possibilities). Even if a right of objection were available,

the intervention would only be possible after the data processing and

would be too late to provide the necessary intervention in view of the intensity of the intervention

develop a protective effect.

When creating a profile, not only the usage data is stored over a longer period of time

period saved. Based on the usage data, the social network

work characteristics and interests of the user in order to subsequently target him

to assign. This is not only done on the website of the above company.

Since a large number of websites integrate the pixel, the data of the

Users can be tracked across websites and even across devices. The user

can no longer grasp the extent of data processing and is too

unable to determine who and to what extent his data

processed (concatenation of data, actors involved, transparency).

Since the company runs an online shop for medicines, is not

prevent users from adding products to the shopping cart or opting for

Articles that allow conclusions to be drawn about the state of health are of interest.

Here it is already questionable whether the legal basis of Art. 6 Para. 1 DSGVO

can be considered at all. Do these sensitive in-

227

If information is entered into the usage profile, the risk for those affected increases

Individuals (categories of data, group of individuals affected) in any case.

A consideration of the above Interests in the specific individual case shows that the

Interests of the persons concerned the interests of the company

predominate and consequently the integration of the pixel not in accordance with Article 6 (1).

lit. f) GDPR is permissible. The legal basis would then come - if at all

– only the consent into consideration.

228

3.8

Position paper on biometric analysis

Version 1.0 as of April 3, 2019

Adopted by the 97th Conference of Independents

Federal and state data protection authorities

April 3rd and 4th, 2019 against the votes of Bavaria and Baden-

Württemberg.

Table of Contents

The use of modern optical-electronic processes is another

Building block for an ever more comprehensive profiling of people in all

Day. Based on video recordings and the evaluation of the face of a

Person can determine their age and gender quite reliably

become. By analyzing the facial expressions, conclusions can also be drawn

the emotional state of a person is possible (emotional decoding). All this

can take place technically without the knowledge and consent of those affected.

Such methods are used, for example, to measure the effectiveness

of advertising to measure and more precisely to the desired target groups

to be able to crop.

The conference of independent data protection authorities of the federal and

of the federal states has set up the working group "Technical and organizational data

protection issues" to work together with the working group "Vi-

deomonitoring" on the topic of processing data using sensors

and video technology and their classification under data protection law.

The aim is to improve the performance of biometric sensors including

Identify video cameras and associated processing systems

as well as to describe processing goals and processes. Subsequently

which these elements are legally evaluated and recommendations for design

derived from procedures.

2 Basics of biometric recognition

2.1

definitions

The terms and definitions are translations from the ISO/IEC JTC

SC37 Harmonized Biometric Vocabulary (HBV) as defined in the SC37 Working

Group 1 for the international standard ISO/IEC 2382-37.

– Anonymized biometric record

Biometric data record that is deliberately processed from personal meta-

data has been decoupled

- Affected person

Individual whose individualized biometric data is within

of the biometric system

- Biometric Application Database

Database of biometric data and associated metadata that

were generated by the operation of a biometric application and

should support them

– Biometric characteristic

Biological or behavioral characteristic of an individual

ums, from which to distinguish usable, reproducible

biometric characteristics can be derived for the purpose of biometric

detection can be used

– Biometric data28

Biometric sample or collection of biometric samples in each

the processing stage, biometric references, biometric sample,

biometric feature or biometric properties

28 The definition differs from the definition in Art. 4 No. 14 GDPR; please refer

also Section 6.1 Definition of biometric data according to Art. 4 No. 14 GDPR. Article 14.

Number 14 reads: "Biometric data" (are) personal data obtained with special

son-related data on the physical, physiological or behavioral

Characteristics of a natural person that uniquely identify that natural person

Enable or confirm person, such as facial images or dactyloscopic data.

232

Appendix I - Privacy Materials

– Biometric enrollment

Process of generating and storing a biometric enrollment

record in accordance with the enrollment rules

– Biometric enrollment database

Database of biometric enrollment records29

– Biometric enrollment record

Data set relating to a data subject, non-biometric

contains physical data and a biometric reference identifier

is associated

– Biometric detection device

Device capable of reading from a biometric characteristic

collect a signal and convert it into a captured biometric sample

convert

- Biometric detection subsystem

Biometric capture device(s) and associated sub-processes required for the

Carrying out a biometric registration process is necessary

– Biometric recognition

Automated recognition of individuals based on their behavioral

genetic and biological characteristics

– Biometric identification

Process to search a biometric enrollment database

the identifier of a biometric reference, which is assigned to a single

can be assigned to viduum

29 A database of biometric data not associated with a data subject

is a biometric database, but not a biometric enrollment

Database. A biometric enrollment database can contain the biometric reference data

tenbank included, but does not have to. A separation of the databases can be for reasons

security, data protection, the legal situation, the system architecture or the

recognition performance may be required.

– Biometric verification30

process, a biometric assertion by a biometric ver-

to confirm immediately

– Biometric feature

Numbers or identifiers extracted from a biometric sample

were and used for comparison

– Biometric feature extraction

Process applied to a biometric sample with the aim of generating numbers

and to isolate and output distinctive identifiers in a repeatable manner,

those with different numbers and distinctive marks, those from others

biometric samples were obtained are comparable

– Biometric sample

Biometric samples or biometric characteristics taken as input

serve an algorithm for comparison with a biometric reference

– Biometric reference

one or more stored biometric samples, biometric temperature

plates or biometric models assigned to a data subject

and used as an object for biometric comparison

– Biometric reference database

Database with biometric reference data sets

– Biometric sample

Analogue or digital representation of biometric characteristics

of biometric feature extraction

30 The concept of biometric authentication was developed in the process of standardization

deprecated by ISO/IEC 2382-37. The term authentication is used in this

Paper is therefore used as specified by the Federal Office in the security of information

technology in the glossary of the IT-Grundschutz Compendium (https://www.bsi.bund.

de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html):

“Authentication means the proof or verification of authenticity. The

Authentication of an identity can include: by entering a password, chip card or bio

metry, the authentication of data e.g. B. by cryptographic signatures.

The term authenticity refers to the quality that ensures that a

communication partner is actually who he claims to be. At authentic

Information is guaranteed to have been created by the source stated. The

Term is not only used when checking the identity of people, but

also for IT components or applications.”

– Biometric system

System for the purpose of biometric recognition of individuals

their behavioral and biological characteristics31

– Biometric identification system

System for the purpose of biometric identification

– Biometric template (synonym: reference feature vector)

Set of stored biometric features that can be directly compared

bar to the biometric characteristics of a biometric sample

– Enroll (register)

Create and store a biometric enrollment record in

Compliance with a biometric enrollment rule

– Non-authentic person

Biometrically subversive target subject attempting to

matches another person's biometric reference

to get

– Unidentified biometric data

biometric data whose data subject is currently unknown

– Presentation, conscious

Presentation under the awareness of those concerned to be recorded

person

– Presentation, collaborative

Presentation by a cooperative data subject to be recorded

– Presentation, indifferent

Presentation in which the data subject to be recorded is aware of the

performed biometric registration process is not aware

– Presentation, uncooperative

Presentation of an uncooperative data subject to be recorded

31 A biometric system contains biometric and non-biometric components.

- Concealer of an identity

Subversive subject to be captured attempting to become a

Match decision with own biometric reference

to withdraw

- Comparison

Estimation, calculation or measurement of similarity or difference-

between the biometric sample and biometric references

2.2

How biometric recognition works

2.2.1

general description

Biometric recognition methods are always part of a larger one

biometric system. With the biometric recognition is to be determined

whether a presence compared to a biometric detection system

animal biometric characteristic with a known biometric

reference matches. Examples of biometric systems are in chapter

5 shown. It can be determined whether a person is known

i.e. H. whether biometric data are available from her, or whether even more extensive ones

Data such as name, address, etc. are known. Depending on the result of

Testing is then continued in the system.

Three phases can be distinguished in biometric recognition:

In the initial phase, the biometric characteristics are determined for the first time

recorded, features calculated and references saved. in case of a

Enrollments, this biometric data is linked to other data.

The actual (re)recognition takes place within the framework of the biometric

system takes place if, after re-entering the biometric characteristics

tika the characteristics are calculated and compared with the existing ones

Reference data is used to determine whether the person is known.

The final phase is deleting the biometric feature and

the associated data.

2.2.2

enrollment

Basically, as a result of the first phase, the reference values

be won. This is done by taking biometric samples

as well as characteristics are calculated, which in the case of an enrollment by further

Data is supplemented and then stored in a reference database.

In this phase, a recording device (cf

Section 3) a biometric characteristic belonging to a person

cum presented. From this, a sample or template is generated and

in a decentralized database, for example the access control system

the establishment of a responsible person, a central database of a

persons responsible or even for several persons responsible, such as

in the police department. There are also systems in which

the biometric data is stored on a data medium (chip card).

that is in the possession of the data subject. In addition to

In addition to the biometric data, information about the person is also stored.

In the case of travel documents, an image of the fingerprint is created as a sample

and this image is stored (signed) on a chip of the document.

There are also developments, templates in addition to a pure access
control in such a way that they can only be used in a specific system
can be used (biometric template protection).
The amount of personal data stored may vary
differ significantly by application; see the
different scenarios from Chapter 5.
There may be errors in enrollment known as FTE (Failure to Enrol Rate)
be referred to; for example, there is the biometric feature
"Fingerprint" Persons whose fingerprints are not sufficiently pronounced
are and therefore cannot be recorded.
Regardless of these very technical aspects, it is also relevant whether the
Collection of the data without the knowledge of the data subject (such as when searching
according to criminals of whom only one biometric feature is known),
with knowledge (as with a reference to the use of video technology) or
through a conscious presentation of the person concerned (as with access control
systems) takes place.

2.2.3

Match Check

After the recording, i.e. usually the enrollment, the refer-
benchmarks available. If within the framework of the biometric system
a biometric characteristic is presented to a recording device,
the characteristics are generated from this. These are associated with the characteristics
compared, resulting from the data of the reference database or from the

presented chip card. The result of the comparison is in the form

a percentage spent.

A threshold value must therefore be specified when configuring the process

must have been established from which a match between the references

and the value just calculated is accepted. As a result of this system

technical blurring, there are cases where there is a match

is accepted although it was not available (FAR: False Acceptance Rate),

and there are cases when a person was not recognized (FRR: False

rejection rate). Depending on the application, the threshold value must

are set and this results in FAR and FRR. For example, will

one with an access control system to a high-security wing

want to prevent unauthorized access with high probability, why

the threshold is set high. This reduces the FAR. At the same time increases

the FRR, i. H. there will be more cases in which an actually legitimate

person is prevented from entering.

Depending on the biometric characteristic used, the cooperation

tion of the data subject is required during enrollment and reconciliation

be or not. For example, while a photo easily without knowledge

and cooperation of the person concerned must be

palm vein scanner the person places their palm on the sensor.

The fingerprint can often even be added later in places where

the person concerned has stopped, taken and opposite

procedures are presented.

2.2.4

resistance to adulteration

Another area to consider is circumventing the procedure.

These can be concealers of an identity or non-authentic persons,

i.e. H. Individuals presenting fake biometric characteristics.

Keywords here are live detection and non-falsification. Straight

biometric procedures in which the cooperation of the data subject for

capturing the characteristic is not required are vulnerable. If

and the extent to which data protection risks arise from this can only be determined

be assessed based on the entire application. So it can be significant

affect the rights and freedoms of natural persons,

if by presenting fake characteristics a foreign identity

can be accepted.

3.

Systems for capturing biometric characteristics

A large number of technical systems already exist in which

NEN biometric characteristics a central part of the processing

are. Biometric systems, the purpose of which is the biometric recognition of

Individuals through biometric characteristics, can be based on the

systematize the following criteria:

– Which specific biometric characteristics are used in the respective

cell system is used (biological characteristics, see Chapter 3.1,

and behavioral characteristics as well as medical data as

specific subset of biological characteristics)?

– With the help of which sensors that are part of a biometric detection system

councils, the biometric characteristics are recorded (optical,

acoustic or other sensors, see chapter 4)?

– For what purpose is the processing of biometric characters

carried out?

It can be assumed that the number of these systems and the inte-

integration of the systems into complex applications over the next few years

will gain significantly in importance since

– the users are willing to use these systems (e.g. use of

Wearables for activity tracking, smartphone unlocking by

fingerprint or face recognition),

– the integration of sensors into digital infrastructures is increasing (e.g.

Contact lenses that can measure and transmit blood sugar values) and

– innovative, new business models are being developed, the biological

Use properties (e.g. insurance tariffs for "healthy" people

sting).

However, not every biometric characteristic can be used for every purpose

be used.

For example, biometric characters are used for identification or verification

teristics that are “static” or are very difficult to move (e.g. due to

plastic surgery) (e.g. face, fingerprint, voice).

or the human genome).

For business models that focus on sales (advertising

or products for people who have special biological properties

sen), biological properties are used that are “dynamic” (e.g.

blood pressure, weight), which can therefore change over time. With that can

e.g. B. Target groups can be defined and economically developed. That's the way it is

possible, through certain behavior (e.g. purchase and use of a

product) to cause a change in this biological property.

3.1

Collection of biometric characteristics

3.1.1

Fingerprint/Finger Image

The fingerprint is an imprint of the papillary ridges on the end segment of a

Fingers (fingertip or fingertip). Since so far no two people

known with the same fingerprint, one assumes the uniqueness

activity of the fingerprint. Biologically it is a papillary crest

an elevation of the epidermis on the palm or sole. In very

In rare cases, the fingers are missing as a result of a genetic defect

Papillary ridges and they leave no imprints. A comparable one

Phenomenon can occur in people whose fingers are at work or

are heavily loaded in sports; Examples are tilers or handball players.

A distinction is made between the following characteristics of the fingerprint: basic

pattern, gross features, finer features (minutiae) and pore structure.

Based on these characteristics and their distribution within a finger

impression, a unique distinguishability can be guaranteed.

A special algorithm is used to extract the minutiae,

through which the minutiae are brought into a mathematical form. Out of

the image supplied by the fingerprint scanner, for each fingerprint

Imprint-specific data collected for enrollment or later

Comparison with existing fingerprint data is sufficient. A concrete one

fingerprint can no longer be reconstructed from the minutiae data.32 Es

but a fingerprint could be created that would match an identical template

delivers on an exam.

3.1.2

iris

The iris is part of the human eye. For iris recognition, over

a camera captures the color pattern of the iris and looks for certain characteristics

(dots, speckles, stripes, threads).

32 Source: https://de.wikipedia.org/wiki/Fingerabdruck

Between the iris (iris) and the cornea of the human

Complex band and comb-like structures of connective tissue lie in the eye. The-

These structures are different for every person. you differentiate

itself in identical twins. Also, they change in one

healthy eye during a lifetime little. That with a conventional

Camera (e.g. a CCD camera33) captured image of the iris from the outside

allows these structures to be recognized and is therefore suitable as a biological one

characteristic.

In people with dark eyes, the structures are visible

However, the light is difficult to see. biometric iris recognition system

me therefore illuminate the iris from a distance of about one meter

near-infrared light that is almost invisible to the naked eye. This

penetrates the "dye" of the human eye (melanin) better than

visible light. In this way, a recording of the iris structures can be

be made with healthy eyes without dazzling. From the

captured images is using specially designed for this purpose

mathematical methods formed a unique data set, which served as the basis

for biometric recognition.34

3.1.3

retina

The retina, like the iris, is part of the human eye and is designated

the arrangement of the blood vessels in or behind the retina. The blood vessels in

Fundus forms a pattern. By the reflection of the irradiated

light on the retina, a characteristic structure develops that is

camera can be recorded.35

The retina is individual in the distribution, shape, and pattern of its blood vessels

clearly characterized. Because the exact pattern of blood vessels not only through

Genetic factors is determined, even identical twins

distinguished by their retina. Like the iris pattern, this remains

Vein pattern of the retina is largely constant over the course of life and

makes the retina a very consistent identifier.

However, the pattern of the blood vessels can be impaired by diseases

33 CCD: charge coupled device, denotes a shape

of image sensors

34 Source: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/Biometri-

scheverfahren/iris-recognition/iris-recognition_node.html

35 Ottenberg, Retinakennungssystems, p. 1, available at https://www2.informatik.huberlin.

de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/07Hand_Retina/retina.pdf

units or injuries, which then temporarily or the image of the retina

constantly changing. These diseases include, for example, diabetes

or a degeneration of the macula as well as due to high blood pressure

ruptured capillaries.36

With retina recognition, the back of a person's eye is identified using

made visible by an infrared light. In contrast to iris recognition,

in which a conventional camera can be used, in which

Retina detection of the head in a specific position relative to the capture device

to be brought.

3.1.4

Face

With the biometric recognition of the face, the biological

Characteristics of the facial features based on a digitized image, the

recorded with a camera.

Above all, those characteristics of the face are used that

do not constantly change due to facial expressions, i.e. upper edges of the

cavities, the areas around the cheekbones and the sides of the

mouth. Basically, the characteristics are compared with the

corresponding biometric reference using classic image processing

processing and image analysis methods, such as after locating the eyes

the calculation of facial features using a grid that is over

the face is laid.37

3.1.5

hand geometry

Every human hand is unique. From the age of about 20 years

the changes in the human hand are usually only minor.

For the biometric recognition of the hand geometry, an image of the hand (im

reader, mirrored by a camera) taken from above and from the side.

The contours of the hand are generated from these images. become of it

then various biological characteristics are extracted and determined, e.g. B.

Values for thickness, length, width and area of the hand or fingers that

Fingertips and points between the fingers, hand width, distances and

36 Ottenberg, a. a. O., p. 2

37 Source: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/Biometri-

scheProcedures/face recognition/face recognition_node.html

Angles between different interfinger points, finger curvature and

Palm and finger height.

Appendix I - Privacy Materials

3.1.6

vein pattern

Human hand vein patterns are complex and location

of the veins is different for each person and remains throughout life

unchanged unless the hand is injured.

When recognizing the vein pattern, either the veins of the hand

inner surface, the veins of the back of the hand or the veins of the fingers with a

palm vein recognition sensor and used for identification

the. To do this, the sensor uses infrared LEDs to emit near-infrared radiation

direction of the palms. The oxygen-depleted blood in the veins

absorbs this infrared radiation more than the surrounding tissue. With it

a clear image of the veins of the hand/finger can be obtained

and used for detection. The veins are in front

Abuse and tampering well protected within the body; for the

The features are not visible to the human eye. skin impurities
or superficial injuries have no influence.

Palm vein recognition

With this method of recognition, the vein pattern of the palm of the hand
recorded and compared with later recordings. For identification
a person must have their palms flat in front of the sensor of the
Place the palm vein scanner without touching it (non-contact
capture). The detection rate for the method is currently almost
100%, the FAR as 0.000 08%, the FRR as 0.01%. This is
thus considerably more accurate than e.g. B. fingerprint recognition.
Areas of application of this method are electronic access controls for
Areas that require the highest level of security, such as B. data centers,
Power plant areas, restricted zones at airports and much more. m., but also as
protection for computers. In some countries (e.g. Japan), the system
already used in ATMs for secure payment transactions.
The vein detection of the palm of the hand was considered one of the safest methods
ren with extremely high accuracy in biometrics until December 2018, then
became public that the system could be defeated with the appropriate technology
is. An assignment under organizationally secured conditions and with
Two-factor authentication is still possible. Furthermore,
Additional laser systems for blood flow detection (live detection).

be used as protection. Regarding ATM security
further considerations will have to take place in order to

secured application.

Back of the hand vein detection, finger vein detection

With dorsal vein detection, the back of the hand is detected by the sensor

scanned. While on the palm of the hand there are pigment spots or hair

play no role, it can inevitably correspond to the back of the hand

the disturbances come. Likewise, terminals are usually built in such a way that a

handle must be grasped and the back of the hand pressed against the sensor

is, whereby no non-contact method is given.

With finger vein detection, the finger is scanned from the top as well as the

illuminated on the left and right side and the vein pattern inserted from below

scans. The vein pattern of a finger is smaller and less complex than

the pattern of the palm. Added to this is the greater sensitivity of the

Finger veins in the cold. If your fingers are cold, the capillary veins can contract

contract completely so that they may no longer be recognized.

The finger vein recognition is not contactless, since the corresponding

finger must rest completely on the sensor.

In summary, regarding the dorsal vein detection and

Finger vein detection can be said to be due to susceptibility to interference

are negligible and rarely used.

4.

Biometric sensors

A biometric recognition system consists essentially of the

Components sensor (measurement recorder), feature extraction and feature

times comparison together. What types of sensors are used

depends strongly on the biometric characteristic.

The sensor component supplies a biometric sample as a result. The

Feature extraction removed using image or data processing and analysis

analyze all information supplied by the sensor that is not required

Fulfill feature properties, and delivers the biometric as a result

Characteristics. Resulting from the clearly defined linking of the characteristics

then so-called templates, which do not allow any conclusions to be drawn about the actual

allow common raw data. As permanent storage usually come

central databases are used, so usually none remain in the device

further data.

Finally, the feature comparator calculates a comparative value (similar

value; Score) between that obtained in the learning phase or off

an external database stored biometric template and the

current data set provided by the feature extraction. exceeds

this comparison value is a threshold, the detection is considered successful.

By performance criteria is meant that the biometric sensor

supplied samples are subject to statistical fluctuations, which

require detections. Reliability is mainly after two

Criteria judged: by Unauthorized Admission Rate (FAR) and by

the rejection rate of authorized persons (FRR).38 All biometric procedures

do not work properly. They only provide statements about probability

the degree of agreement between currently measured and stored

biometric templates.

Due to the complexity of the topic of biometrics, this is limited

Position paper below on such systems that use biometric features

generate by using the appropriate biometric characteristics of a

depict the person concerned based on optical sensors. Should these

Systems also usually include other sensors such as acoustic

or include haptic sensors, so will for the following systems only

the optical component considered.

4.1

video cameras

Video cameras are devices for recording image sequences in electrical signals

nals. In contrast to film cameras, the stored image signals can

nale directly visible, since films do not have to be developed first.

Modern digital video cameras usually use a CCD chip

as an imager. The larger the area of a camera's image sensor,

the more light it can capture. Sensitivity to light increases and that

so-called image noise is reduced.

Due to the widespread use of video cameras, smartphones and

Webcams carry out the biometric evaluations made possible with them

to a rapid technical development in this area: The

Face recognition is currently one of the most advanced

forms of biometric analysis. Here, between methods in 2D

and 3D differentiated, with 3D methods more accurate detections as well

Should provide security against overcoming, so that the face detection of

systems can no longer be manipulated.

38 https://de.wikipedia.org/wiki/Biometrie

With biometric facial recognition, a person's face is

recorded with one camera and then with one or more

compared to previously saved facial images. Does the camera supply analog

Face image values are converted into digital formats

(digitized). The recognition software locates the face and calculates

its characteristic properties. The result of this calculation

gen, the so-called template, is created with the templates of the previously saved

Face images compared.39

The process of using video cameras for facial recognition allows

can be represented schematically as follows:40

– Image capture

– Localization of the face

– Localization of the eyes and other facial areas

– Normalization of the face

- Feature Extraction

– Template creation

The image of a person's face is captured using a camera in the current

Environment recorded or in the form of a scan of an existing one

Image of the person captured. The next step consists of a facial

tektion that examines the image information for face-like shapes.

Provided one face has been located, typically the next

Step the eyes are detected as they are usually due to different coloring

stand out from the rest of the face. Depends on the algorithm used

further facial areas are localized and then the face

normalized to make the data invariant to rotation, stretch, and

save compression. Based on these normalized faces

then the feature extraction, which also depends on the method used

is dependent. In the last step, the characteristics are

matic formulations feature vectors generated.

39 BSI, facial recognition, p.1, available at https://www.bsi.bund.de/SharedDocs/Down-

loads/DE/BSI/Biometrics/Face Recognition_pdf.pdf

40 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtskennung_

pdf.pdf

4.2

infrared cameras

Unlike video cameras, infrared cameras do not capture the for that

human eye visible light, rather than electromagnetic radiation

in the infrared range.

Use for thermal imaging

In thermal imaging, the intensity of the radiation in the infrared

red area closed to the temperature of an object. the together

The relationship between radiation and temperature is determined using Boltzmann's constant

(radiation intensity = Boltzmann constant * temperature).

The electromagnetic spectrum for infrared radiation is between 0.8

and 14 µm wavelength, so does not fall within the range for the human eye

visible range from 0.4 to 0.7 µm.

Use as depth cameras (e.g.: Apple FaceID, Microsoft Kinect)

Depth cameras were originally designed to detect motion as natural

Introduced human-computer interaction.41 An IR projector

emits a signal that is invisible to the human eye in the near infrared range

res encoded dot pattern. A CMOS sensor42 receives this from the

Scene reflected image and calculated based on camera distance above

the parallaxes of corresponding points, a depth image. points equal

Size appear different in size at different distances

known point size, the distance can be inferred.

Use for vein detection

Vein recognition is a biometric process that is used to identify people

be detected by infrared technology based on their hand vessel structure

can. The course of the arteries and veins is just as unique as

the fingerprint. Sensors that measure the temperature of the vascular structure in the

react by hand, in combination with complex filter technology

so-called live detection and are thus intended to protect against attempts to deceive

by non-biometric means or by simulating biometric ones

protect features.

41 http://www.scanner.imagefact.de/de/depthcam.html

42 CMOS: complementary metal oxide semiconductor

ter"): a specific form of semiconductor device

4.3

fingerprint reader

The process of a fingerprint analysis can be broken down into the following steps

show schematically:43

– Capture the fingerprint image

– Image quality improvement

– Image processing

– pattern classification

- Feature Extraction

– verification phase

The basic structure of an optical fingerprint reader consists of

a light source, a glass prism, a lens and an image sensor. The

Finger is pressed on the glass prism, elevations have direct

Contact with the prism, only between the valleys and the prism is still

Air. The light is sent into the prism from one side. It will then be sent to the

reflected at the valleys and absorbed or randomly scattered at the peaks.

The reflected rays leaving the prism are passed through outside

the lens focuses on an image sensor where the recording takes place.

With every sensor, the end product is generally a shade of gray

fingerprint image. To generate a grayscale image there

There are two modes: With the live scan, the fingerprint is scanned by a sensor

recorded, in offline mode, a recording of left behind

fingerprints, e.g. B. glasses made. The raw data are processed using

Image processing improved and processed. Subsequently, the location of

Minutiae (bifurcation and line ending) detected in the fingerprint and

extracted. In practice, the recorded fingerprint images show a

different quality. The performance of the algorithms can

due to poor image quality caused by dirt or injury,

be affected.

Finally, decisions are made as to whether the determined feature vector is a

corresponds to an existing entity, based on comparisons of two characteristic

vectors performed.

43 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometricVerfah-

ren/fingerprint-recognition/fingerprint-recognition_node.html

4.4

hand geometry reader

For hand recognition, relevant biometric features are height

and width of the back of the hand and fingers and their relative positions.

The imprint of the palms of the hands and the fingertips are not relevant

the nails will grow back and be trimmed.44 The components of a

Hand geometry readers are usually integrated into a device. These include one

CCD camera for capturing the features in the form of a 3D image recording,

a display for interaction with the user (display of faulty areas

che), a processor for creating and checking the templates and, if necessary,

Readers for ID cards or PIN entries. Software Side Components

depend on the respective application.

Hand detection requires correct hand positioning. This

is facilitated by orientation aids and by visual feedback

shown on the display.

The feature detection is done by a CCD camera, which at least

created two 3D images, one from above and one from the side. defined

Characteristics are captured and incorporated into the characteristics in templates with a

size of a few bytes. Typically, just about the

100 characteristics recorded, which directly results in a low uniqueness

has. Therefore, this method is less suitable for the unambiguous

Recognition of a person as e.g. B. Vein detection. However, it can

Example, be "optimized" by using robust algorithms.45

4.5

iris scanner

The process of iris scanners can be represented schematically as follows-

put:46

– Imaging of the iris (the iris of the eye), mostly in the near-infrared

Area

– Iris recognition

44 https://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/

Biometrie/07Hand_Retina/Hand-Recognition-Elaboration.pdf

45 Singh, Hand geometry verification system: A review, p. 4, https://www.researchgate.net/

profile/Amit_Singh202/publication/224086092_Hand_geometry_verification_system_A_

review/links/5681052908ae1975838ead2f/Hand-geometry-verification-system-A-review.

pdf?origin=publication_detail

46 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Iriskennung_pdf.

pdf

249

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

– Iris segmentation

– Transformation of the circle segment to a strip

– Binarization and template creation

In the iris scanner, the iris is captured by a camera and image processed

beitung isolated by using two circles (outside and inside) as the boundary of

serve iris. The resulting ring is represented by polar coordinates,

allowing for invariances in iris size/thickness. Then takes place

a spiral scan of the shot and a grouping into bright ones

and dark areas (binarization). By "unrolling" the spiral, a

Graphics, similar to a barcode, are generated, corresponding to the

templates is compared.

Commercial detection methods detect about 260 individual optical

Characteristics of the iris. These traits develop from a random

controlled, morphogenetic process in the first months of life

person and remain largely unchanged over the rest of the lifetime.

Identical twins do not have identical iris structure either.47

4.6

retina scanner

The process for retina scanners can be represented as follows:

– Image recording of the retina (retina of the eye) by circular scanning

tion with a laser

– Image correction for ametropia of the lens

- Fixed head/retina twists

– Binarization and template creation

The retina scanner scans the retina in a circular manner with an infrared laser.

Any existing ametropia of the people can and must

be corrected up to certain characteristics, since otherwise no standard

configuration within the template database would be given. The phase cor-

rektur module takes care of the image correction if the head or the retina in the

Recording was captured upside down. To do this, the digital image must be

moved in small steps to the reference object in the database and

the correlation between the respective shifts and the reference

are formed. Because veins on the retina make the laser beam stronger

absorb than the surrounding tissue, they stand out with greater contrast. For

the binarization and template creation, threshold values are defined, see above

47 https://de.wikipedia.org/wiki/Iris-Recognition#Properties

that the image information of the bloodstream differs from the remaining structures

separate.

Depending on the manufacturer, the scanning process takes place on differently defined

way, so that it is not directly possible to use systems from different manufacturers

to compare with each other.

Furthermore, the retina is subject to degenerative changes, so that in

In the course of life, different templates can occur. the retina

identical twins is also different.

5.

Collection of possible application scenarios ("Use Cases")

5.1

Overview of usage scenarios

There are numerous scenarios where biometrics are used

come. On the one hand, these are scenarios in which biometric recognition

systems with the immediate aim of identifying or verifying

people are operated. There are also scenarios in which data from

Usage contexts (e.g. video surveillance, audio recordings)

evaluated using biometric methods. With some of these

procedure is also an identification of persons the goal; other

Procedures aim at recognizing persons or a group

pen assignment (feeling recognition, age estimation). Scenarios include:

– Identification

– verification

– recognition

– profiling

– Feeling Analysis

– Observation/monitoring

- Registration

– behavior control

– Advertising / Marketing

– communication

– Interaction (human – machine)

The application scenarios from section 5.1 can be classified under different

group perspectives. These include, on the one hand, technical and functional ones

Aspects of the biometric process, on the other hand, the purposes associated with the

be tracked.

5.2

Classification of the scenarios according to technical and functional aspects

5.2.1

Cooperative Biometric Verification

A typical function of biometric procedures are authentication procedures

drive (e.g. access control, login, unlock) that are carried out cooperatively: The

The person to be authenticated deliberately uses the biometric method

with the aim of being recognized by the system (conscious and cooperative

Presentation). Automated passport controls, where the agreement

matching of the biometric data stored in identity papers

currently obtained data of the traveler are compared, fall into this

Category.48 If necessary, several attempts until a positive

Authentication required. Identification and processing

verification procedure.

5.2.2

Non-Cooperative Biometric Recognition

Other typical use cases are monitoring scenarios where

an identity verification (identification) or verification of an identity

done in a way that does not require the person to cooperate. This is

the case when the biometric characteristics without conscious actions

(cooperative presentation) of the person (can be recorded). examples

are video or audio recordings that are created openly or covertly

or the evaluation of data collected in other ways (e.g. video recordings,

Telephone calls, keyboard usage) with the aim of biometric processing.

This can be done in the mode of conscious or indifferent presentation.

Typical scenarios are manhunts or comparisons with biometric

Reference databases in terms of identification.

A compulsory procedure would also be included in the category of non-cooperative procedures

use of biometric processes from Section 5.2.1.

48 In connection with border controls, further uses of the currently gained

biometric data of travelers conceivable, such as comparison with biometric data

databases (e.g. search databases) in the background. Such usage is dem

Scenario 5.2.2 Map non-cooperative biometric recognition.

5.2.3

Assignment to groups

Biometric processes are not only operated with the aim of

establish a clear personal reference. Applications can also have a

automated estimation of demographic data (e.g. age, gender)

or assignment to a group (e.g. age group, wearers of glasses, hair

and eye colour, assignment to an ethnic group, etc.). Not this one

Personal characteristics are also referred to as "soft biometrics".

The main focus here is on images of faces and the iris

Mission; Speech and dialect recognition are also conceivable.

Allocation to groups with the help of "soft biometrics" can also be used

det to specify the number of biometric data to be compared in

Reduce identification methods when used for comparison

biometric data are also classified (example: gender

Identification of the current person and search in databases only for persons

same sex).

5.2.4

profiling, chaining

Furthermore, biometric methods can be used with the aim of

Link actions of individuals. A typical example is the

"Tracking" of people during a video surveillance: technically lying

video recordings as a data stream consisting of individual images (frames)

consists. The rapid sequence of playback gives the impression of a film

(like the flip book). Should people be counted or a dwell time

are determined, a comparison must be made over several frames,

whether it is the same person or not. An identification of

person is not required.

5.2.5

behavior detection

Procedures can also be operated with the aim of behaviors

to recognize and assign the persons concerned to a behavioral group

to. For example, emotions (excited,

friendly, negative etc.)49 close; also from sound recordings.

49 See e.g. B. the "Emotion API" from Microsoft, https://azure.microsoft.com/de-de/

services/cognitiveservices/emotion/?cdn=disable or https://www.heise.de/newsticker/

report/software-recognizes-feelings-2123851.html

5.3

Consideration of the scenarios according to purposes in terms of data protection law

5.3.1

Sovereign authentication procedures

Typical examples of sovereign authentication procedures are automated ones

Checks of biometric data (facial image, fingerprint).

Official documents (passports, identity cards, residence permits)

with the biometric characteristics of the ID card holder.

5.3.2

State Identification Procedures

Identification methods are used, on the one hand, to identify unknown

to identify people for the first time (identity verification) or to duplicate

to discover pel identities. An example of the first case is matching

Perpetrator photos (e.g. surveillance cameras from ATMs)

or video recordings with databases where the biometric

Data is associated with identifying metadata (such as a name).

An example of the second case is the use of recognition systems

to uncover double identities, for example in the case of asylum seekers.

5.3.3

access control

The biometric process is used to control physical access

rooms or buildings used. Typical biometric characters used

rakteristica are face shape and fingerprints; other characteristics

such as hand geometry and iris are also used.

5.3.4

access control

The biometric process is used to control access to data

working systems used. Typical scenarios are unlocking

from mobile devices using the biometric characteristics of face shape

and fingerprint, but also authentication mechanisms (log-in).

Operating system level using face shape and fingerprint.

5.3.5

advertising, marketing

Advertising and marketing measures can be carried out using biometric methods

on certain groups, individuals or their behavior

must be cut.

In the first and third cases, the target persons are assigned to groups

(e.g. age, gender, beard wearers, glasses wearers in the first case, group of
Angry, friendly or neutral in the third case) and corresponding ones
group-specific advertising measures selected. An identification is
not required and usually not striven for; the assignment to
one group is sufficient. As with biometric recognition can
assignment to a group may be faulty.
Depending on the constellation, the assignment to a group under the category
special data fall, for example, when groups are classified according to sexual
ferenzen50, skin color or physical limitations.
In the second case (advertising measures for individuals), a biomechanical
tric detection required. This can refer to known names
People (e.g. VIPs, regular customers) and thus to people with acquaintances
get metadata. However, cases are also conceivable in which only one
Recognition (“visits the supermarket for the third time this week”)
takes place without metadata being used for identification.

5.3.6

Measuring the reach of advertising

In another scenario, biometric methods are used to detect
through which groups and for how long advertising is viewed. become
recorded the viewers during an advertising measure and a group
assigned (e.g. gender or age, see Section 5.3.5 Advertising,
Marketing, 1st case) and the viewing time are measured. Likewise,
seeks to record reactions to advertising measures (emotions).
Primarily methods are used here that use the biometric
Evaluate facial characteristics.

50 See e.g. B. http://www.spiegel.de/netzwelt/netzpolitik/software-kann-homosexuale-an-

recognize-hand-from-photos-a1166971.html

255

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

5.3.7

observation, surveillance

In a surveillance scenario, biometric characteristics (in

primarily facial images and speech) (video and audio recordings

men) and with known biometric data, for example from a blocking list (e.g.

Persons banned from entering) compared (“watch list”). This can be done with sovereign

applications are linked (see Section 5.3.2).

5.3.8

Human-machine interaction, control

In the case of interactions and controls of machines, bio-

metric methods are used. Examples here range from one

pure presence detection via the detection of attention and

Position of people in motor vehicles (semi-autonomous driving), a

Assessment of current behavior (defensive/sporty driving style)

up to a personal identification of the driver with the aim of an individual

configuration of the vehicle (seat and mirror positions, radio stations).

A group assignment of persons falls into a similar area of application.

Sons from the environment of the vehicle (e.g. to differentiate between age groups

of passers-by with the aim of being ready to brake when they see children).

Other control mechanisms are based on speaker recognition,

for example in the field of home automation.

Not all of these applications require personal identification.

Biometric methods can be used to determine whether drivers are

Drivers are sufficiently concentrated.

6.

Legal Assessment

According to Art. 9 Para. 1 DS-GVO the processing of biometric data for

unequivocal identification of a natural person is strictly prohibited.

In the cases standardized in Art. 9 Para. 2 DS-GVO it is exceptional

permitted. If the processing of biometric data does not take place for unique purposes

identification of a natural person, but for another purpose,

their admissibility is based on Art. 6 Para. 1 DS-GVO. In any case

the suitability of biometric data for unique identification on the way

biometric analysis methods in risk assessment and selection

of the technical and organizational measures must be taken into account.

256

Appendix I - Privacy Materials

6.1

Concept of biometric data according to Art. 4 No. 14 DS-GVO

According to the definition in Art. 4 No. 14 DS-GVO, biometric data are included

personal data obtained through special technical processes

the physical, physiological or behavioral characteristics of a person

natural person who uniquely identifies that natural person

enable or confirm, such as facial images or dactyloscopic data.

6.1.1

Personal Data

According to Art. 4 No. 1 DS-GVO, personal data is all information

relating to an identified or identifiable natural person

hen; a natural person is considered to be identifiable who directly

or indirectly, in particular by association with an identifier such as a

Names, to an identification number, to location data, to an online identifier

or to one or more special characteristics that express the

physical, physiological, genetic, psychological, economic,

cultural or social identity of that natural person

can be. In principle, each unique biometric feature is an individual

visual personal identifier51 and therefore a personal date.

In order to determine whether an individual is identifiable,

Recital 26 all means taken into account by the responsible

verbal or another person's reasonable discretion

appearing to be used to identify the natural person directly or indirectly

to identify, such as weeding out. When determining

whether means reasonably likely to identify

of the individual, all objective factors

such as the costs of identification and the time required for this,

be used, whereby the data available at the time of processing

bare technology and technological developments into account

are. Through the explicit reference to technological development

the GDPR makes the concept of identifiability dynamic and obliges

Those responsible, supervisory authorities and courts, in the future of this development

development and, if necessary, the identifiability of databases

to reevaluate. For the purpose of protecting data subjects

against their fundamental rights being affected by the processing of data

51 Weichert, Biometrics – friend or foe of data protection? in: CR 1997, p. 369.

to achieve it must be actually available and not just legally available
permissible options are taken into account.52

The principles of data protection should not, according to recital 26
apply to anonymous information, d. H. for information not related to
relate to an identified or identifiable natural person, or
personal data that has been anonymized in a way
that the data subject cannot or can no longer be identified.

However, nothing about the personal reference of the processed data changes theirs
pseudonymization. According to Art. 4 No. 5 DS-GVO, pseudonymization is the
Processing of personal data in such a way that the personal
related data without consulting additional information
can be assigned to a specific data subject, provided that
this additional information is kept separately and technically
are subject to technical and organizational measures that ensure
that the personal data does not belong to an identified or identifiable
assignable natural person. Since the responsible
continues to be able to identify the data subjects
receive the personal reference of pseudonymised data. That also turns out to be the case
from recital 26.

According to the former Article 29 Working Party53, a refer-
renz template created from the image of a person as per-
sun-related datum since it has a set of distinctive characteristics
of a person's face, which is then associated with a specific person
is linked and used as a reference for later comparisons for identification and

verification is saved.

6.1.2

Data on the physical, physiological or behavioral

characteristics of a natural person

With biometric data within the meaning of the DS-GVO, characteristics of being such as

addressed physical characteristics or behaviors that

can be directly assigned to a person and usually permanently

are bound to a person. A (intended or involuntary) separation

52 Klabunde, in: Ehmann/Selmayr, DS-GVO, Article 4, paragraph 13

53 The Article 29 Working Party was an independent advisory body to the Euro

European Commission on data protection issues. With the entry into force of the

General Protection Regulation, the Article 29 data protection group was established by the European

Data Protection Board (EDPB) superseded. The EDPB has not yet commented on this.

of the person cannot take place.54 The biological or

behavioral characteristics of an individual from which

reproducible biometric features that can be used for differentiation

can be derived for the purpose of automated biometric recognition

information that can be used is called “biometric characteristics”. you are the

Starting point for all biometric recognition systems.

6.1.3

Data that uniquely identifies a natural person

enable or confirm

Biometric data are used to uniquely identify a natural

person appropriate if the characteristics measured are unique. Not

it is necessary that the information is unambiguous worldwide. It is enough that

an exact identification in a described with abstract features

a group of a large indefinite number of people is possible.

It is relevant that the data collected about the natural person is objective

are distinctive. Because of their connection with the human body

they are difficult or impossible to change or falsify. Whose

regardless z. B. due to age or illness

Changes occur that make assignment difficult or even impossible

make light. Also the lack of certain biometric features

(e.g. fingerprints) for a specific person can lead to their

be suitable for identification.55

6.1.4

Data obtained with special technical processes

The definition refers to "special technical processes". in the english

The term "specific technical processing" is used here,

i.e. "certain technical processes".56 It can only be such

Procedures that provide data that are state-of-the-art

unique identification of a natural person with a biometric

Enable detection system.

For this it is necessary that the information content of the data for a

clear identification is sufficient. Biometric data are therefore both

54 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/AllgemeineEinfueh-

tion/ introduction.html

55 Weichert, in Kühling/Buchner, DS-GVO, Art. 4 No. 14, para. 2.

56 In the following, this understanding of the term is therefore used as a basis.

the biometric samples, i.e. those recorded directly with a sensor
Features, as well as the so-called templates, i.e. those from biome-
tric samples obtained and typed feature vectors that on
based on a mathematical model and recorded in a standardized way
are regularly taken as the basis for digital assignments.57

6.1.5

Relationship to the concept of biometric data according to ISO/IEC JTC SC37

According to the biometrics internationally standardized by ISO/IEC JTC SC37
tric vocabulary are biometric data or biometric samples
Accumulations of biometric samples at each processing stage, bio-
metric references, biometric samples, biometric characteristics or
biometric properties. In contrast, biometric data is
Within the meaning of Art. 4 No. 14 DS-GVO with special technical processes
Obtained personal data on the physical, physiological or
behavioral characteristics of a natural person that are unique
enable or confirm identification of that natural person. So-
probably have the GDPR as well as the internationally standardized vocabulary
however, the processing of biometric methods for the purpose of unique
Identification in focus.

The concept of biometric data from the internationally standardized
Biometric vocabulary can therefore be used to further define the term
of the biometric data according to Art. 4 No. 14 DS-GVO.

However, according to the standard biometric vocabulary, these also count
biometric properties to the biometric data, not for themselves

taken to enable the clear identification of a natural person

chen. Data such as age, height and gender, which are true

biometric data is in the sense of the biometric standard vocabulary,

should in principle not only be the clear identification of a natural

allow a person within the meaning of the DS-GVO. Depending on the individual case, it can

make exceptions to this. One is sufficient for clear identification

natural person specifying the gender if it is in a group

of humans there is only one person of that sex.

As biometric data within the meaning of Art. 4 No. 14 DS-GVO can then

both the biometric samples, i.e. the analog or digital representations

Sentences of biometric characteristics before the biometric feature ex-

traction, as well as the biometric features, that is, the numbers or

57 Weichert, op. a. O., para. 7.

distinctive identifiers extracted from a biometric sample

were and can be used for comparison.

The concept of biometric data is also given clearer contours by

that the internationally standardized biometric vocabulary

tric detection as automated detection, i.e. as the

Detection by means of a computerized system. It means that

there can only be talk of biometric data if this is for a

automated processing are suitable. This understanding of the term fits

to that of the DS-GVO: According to this, biometric data with special technical

data obtained by mechanical processes. This uses an at least partially automatic

matized method of extraction ahead. In addition, an automated

Processing of biometric data using biometric recognition methods

for the purpose of unique identification for the data subjects

associated with increased risks. The data processed in this way are therefore

according to Art. 9 Para. 1 DS-GVO as a special category of personal data

Classify data whose processing according to Art. 9 Para. 2 DS-GVO

requires special justification.

6.1.6

Examples of biometric data according to Art. 4 No. 14 DS-GVO

6.1.6.1

fingerprints

A photograph of the papillary ridges on the fingertip is one with one

personal data obtained using special technical processes

to the physiological characteristics of a person.

It can be clearly assigned to a natural person and made possible

thereby the clear identification of a natural person. At a

Such recording is a biometric date in the sense

of Art. 4 No. 14 GDPR and at the same time a personal one

Date within the meaning of Art. 4 No. 1 DS-GVO.

6.1.6.2

Images of the iris structures

A recording of the iris structures is one with a special technical

Process obtained personal date to the physiological

characteristics of a person. It leaves a natural person unequivocal

assign and thus enables the clear identification of a natural

person. Such a recording is a biometric

cal date within the meaning of Art. 4 No. 14 DS-GVO and at the same time also at a

Personal data within the meaning of Art. 4 No. 1 DS-GVO.

6.1.6.3

retina scans

A retina scan is a scan obtained using a special technical

nenes personal data on the physiological characteristics

one person. It can be clearly assigned to a natural person and

thereby enables the clear identification of a natural person.

A retina scan is a biometric data in the sense

of Art. 4 No. 14 GDPR and at the same time a personal one

Date within the meaning of Art. 4 No. 1 DS-GVO.

6.1.6.4

palm vein pictures

An image of the palm vein pattern is one with a special technical

Process obtained personal date to the physiological

characteristics of a person. It can be unique to a natural person

assign and thus enables the clear identification of a natural

person. An image of the palm vein pattern is

a biometric date within the meaning of Art. 4 No. 14 DS-GVO and at the same time

also a personal date within the meaning of Art. 4 No. 1 DS-GVO.

6.1.6.5

hand geometry

Recordings of the hand geometry are made with a special technical process

ren obtained personal data on the physiological characteristics

one person. They can be clearly assigned to a natural person

and thereby enable the clear identification of a natural

Person. The recordings are biometric data in the sense

of Art. 4 No. 14 GDPR and at the same time also personal data

within the meaning of Art. 4 No. 1 DS-GVO.

6.1.6.6

facial images

A facial image is then one with a special technical process

obtained personal data on the physiological characteristics

of a person if this involves the processing of biometric characteristics

of the face to create a biometric template or more structured

Collections of face images enabled. The facial image can be

then as part of an automated procedure of a natural person

clearly assign and thus enables clear identification

a natural person. A facial image is one of the

above requirements by a biometric date within the meaning of

Art. 4 No. 14 GDPR and at the same time also a personal date

within the meaning of Art. 4 No. 1 DS-GVO.

In contrast to facial images (as in Art. 4 No. 14 DS-GVO as biometric

called cal date) are photographs or video recordings of people

not per se biometric data according to Art. 4 No. 14 DS-GVO.

However, biometric data can be found on photographs or video recordings

be included if a person's face is in appropriate resolution

ment, orientation and size on the photograph or video recording

is mapped.

6.2

Requirements of Art. 9 GDPR

6.2.1

principles

The processing of biometric data for unique identification

of a natural person is fundamental according to Art. 9 Para. 1 DS-GVO

prohibited. A processing within the meaning of Art. 9 Para. 1 DS-GVO is given,

if the clear identification of a natural person in the foreground

stands. The English version is even clearer because of "the purpose

of uniquely identifying a natural person". This makes clearer than

the German "um ... to" that here the purpose (purpose) of a clear

Identification must be behind the processing.

Identification within the meaning of the Regulation does not include any recognition

possibility related to biometric data. direction of

Art. 9 DS-GVO is to prevent the processing of particularly sensitive personal

to restrict the data collected and only under special conditions

allow. Biometric data only count because of their diversity

to this data, in contrast to the others mentioned in Art. 9 DS-GVO,

if they are used with a special purpose, namely for clear identification

fication and thus processed in a particularly risky manner.

This increased risk only exists when automated biometric

detection methods are used. In Art. 9 Para. 1 DS-GVO

term used in the processing of biometric data for unambiguous

Identification of a natural person corresponds to that of biometric

Recognition in the internationally standardized biometric vocabulary.

Biometric recognition can only be assumed in the case of automated recognition

be mentioned, i.e. in the case of a detection by means of a computer-aided

systems. According to this understanding, a manual visual inspection would not be necessary

the term biometric processing used in Art. 9 Para. 1 GDPR

shear data to uniquely identify a natural person.

Biometric recognition includes biometric verification and biometric

ric identification. According to the international

tionally standardized biometric vocabulary the process in which a

biometric claim is confirmed by a biometric comparison.

The term biometric assertion refers to the assertion that

a data subject to be recorded is the physical source of a specific

ten biometric reference. Biometric reference is called an or

multiple stored biometric samples, biometric templates or

biometric models assigned to a data subject and

used as an object for biometric comparison. The biometric

Reference can be in a database, distributed on a network or across

a smart card.

Biometric identification is the process of searching in a biometric

enrollment database for the identifier of a biometric

reference that can be assigned to a single individual.

A biometric enrollment database consists of records enrolter

Individuals, non-biometric data as well as biometric identifiers

include references. As an identifier of a biometric reference,

one draws the pointer to a biometric reference data set in the

biometric reference database. A reference record is an indexed one

Record containing biometric references. It should be noted here

that a single biometric reference (e.g. a on a memory card

stored fingerprint) in some transactions as biometric

enrollment database can be viewed.

While the user uses his biometric system for verification

identity in advance (e.g. the user ID via keyboard or card) and

the system then only recognizes the biometric feature with the one to

User-ID has to compare the matching reference feature (1:1 comparison).

when identifying the biometric feature with all the biometric

compared to reference characteristics stored in the system (1:n comparison).58

Also Recital 51 suggests that the processing of biometric

Data for clear identification according to Art. 9 Para. 1 DS-GVO as well

Process for identification and authentication includes. The Ver-

only differ in the number of

Genetic reference data records: During authentication, exactly one

Reference data set checked against several when identifying. Like that

used term of authentication corresponds in the biometric standard

standard vocabulary the term biometric verification.

Biometric data thus only falls under the term “special cases”.

Categories of personal data" according to Art. 9 Para. 1 DS-GVO, if

they to uniquely identify a natural person, i.e. to

processed for the purpose of automated biometric recognition. In

In this case, the scope of the above regulation is opened.

6.2.2

Selected exceptional circumstances of Art. 9 Para. 2 DS-GVO

The processing of biometric data for the clear

gen Identification of a natural person in the cases of Art. 9 para. 2

GDPR.

6.2.2.1

Article 9(2)(a) GDPR

The data subject has to consent to the processing of their biometric data

Identification expressly consented. The consent must be there

explicitly refer to the use of biometric data. It must

thus an explicit reference to the data in the consent

present. This assumes that the sensitivity of the data separately

is pointed out.59 Through the DS-GVO, all personal

Genetic data are protected, but those mentioned in Art. 9 Para. 1 DS-GVO in

special way. The information should enable the person concerned to

will decide whether he may consent to

58 BSI, Introduction to the Technical Basics of Biometric Authentication, p. 1,

Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/

Technical_Basics_pdf.pdf

59 Weichert in Kühling/Buchner, DS-GVO, Art. 9 para. 47

data processing outside of this special legal protection

located. Implied consent is therefore not possible.

The specific purpose of the data processing must be stated. This would be according to

Art. 9 para. 1 DS-GVO at least the purpose of clear identification.

The requirement for voluntary consent to the processing of biome-

tric data are subject to particularly high requirements if they are

As part of a dependency relationship, such as in employment

relationship, is granted.

6.2.2.2

Article 9(2)(b) GDPR

The processing is necessary so that the person responsible or the

person affected by him or her from labor law and the law of

social security and social protection rights

and can fulfill his or her obligations in this regard. Article 9

Paragraph 2 lit. b GDPR is not an independent applicable one

Permissibility, but rather requires that the necessity

the data processing for the aforementioned purposes from a separate,

specific Union law or national norm, including

company agreements and collective agreements count, results in.60

Biometric data can be used in the operational context for access authorization

authorization, authentication on IT systems or at admission control

areas that are particularly worthy of protection are used. The required

principle is to be interpreted narrowly in this area.61

6.2.2.3

Article 9(2)(e) GDPR

A processing of sensitive data according to Art. 9 Para. 2 lit. e GDPR

also be permitted if the data subject is aware of the data

has made public. The public in this sense is the general

means to understand a group of people that cannot be individually determined.

In addition, the "data subject" must "obviously"

have made public. This sets an unequivocal, conscious will

lensakt ahead, the final on the release of the date in public

is directed in the sense explained. This feature is intended to prevent

60 Schulz, in: Gola, DS-GVO, Art. 9 para. 18

61 Weichert in Kühling/Buchner, DS-GVO, Art. 9 para. 54

be that a person concerned loses the special protection that

a third party makes their sensitive data public, or that this

happens unintentionally by the person concerned.62

The mere "existence" in public space does not fall under the concept of

publication in this sense. Because the alienating character of a

Act of will, certain data accessible to an indefinite group of people

Doing something cannot be equated with moving in public space

become. In particular, this excludes the possibility of taking pictures of

persons in public space in order to use a

to process visual recognition programs or to identify people on political

to register events in public space.63

6.2.2.4

Art. 9 Para. 2 lit. f GDPR

According to Art. 9 Para. 2 lit. f GDPR, processing is also permissible if

if they are used to assert, exercise or defend legal

claims is required. Claims within the meaning of lit. f do not have to

be pending, so that the pre- and extra-judicial legal

traffic is recorded.64

6.2.2.5

Art. 9 (2) lit. g GDPR

The processing is based on Art. 9 Para. 2 lit. g GDPR

of Union law or the law of a Member State for reasons of a

significant public interest required. This is not the point

a separate permit, but an opening clause.

Particularly worthy of protection are interests of the common good or

common goods recorded. The public interest must

personal rights of the data subject prevail.

6.3

Application of Art. 6 Para. 1 GDPR

In addition to the special requirements for processing special

According to recital 51, categories of personal data should be

62 Weichert in Kühling/Buchner, DS-GVO, Art. 9 para. 79

63 Schiff, in: Ehmann/Selmayr, DS-GVO, Article 4, paragraphs 40, 41

64 Schulz, in: Gola, DS-GVO, Art. 9 para. 27

general principles and other provisions of the GDPR, in particular

other regarding the conditions for lawful processing, apply.

In the case of particularly sensitive data, the intensity of the intervention is regular

higher, therefore higher requirements to justify the intervention

are to be asked. As a result, Art. 9 GDPR supersedes Art. 6 GDPR

not superseded, but that its requirements are in addition to those

of Art. 6 DS-GVO must be present.

In addition, if biometric data is not used to uniquely identify a

of a natural person, but processed for other purposes, is Art. 6

Para. 1 DS-GVO relevant. Thereafter, the processing of personal

drawn data only lawful if at least one of the regulated therein

conditions is met.

6.3.1

Consent to data processing in accordance with Article 6 Paragraph 1 Clause 1 Letter a GDPR

According to Art. 6 (1) sentence 1 lit. a GDPR, the processing is lawful if

the data subject has given their consent. A consent is only

under the conditions of sufficient information and voluntariness

possible. Special constellations such as consent in

The labor law context must also be taken into account here.

6.3.2

Necessity to fulfill a contract or a pre-contractual one

Relationship according to Art. 6 Para. 1 S. 1 lit. b DS-GVO

According to Art. 6 (1) sentence 1 lit. b GDPR, the processing is lawful if

they for the fulfillment of a contract or for the implementation of pre-contractual

action is required. Next to the "fulfillment" are the preparation

and initiation of the contract, its implementation as well as its

Processing, in particular to fulfill warranty obligations or

secondary performance obligations. Also pre-contractual measures

can legitimize processing, but only if it is “on request

of the data subject”.65

Processing is only necessary for the fulfillment of a contract if

if it is necessary for the purposes of the contract. Such is the case with the

Saving an iris image to create a decorative object

of this figure, the communication of credit card details for processing the

Payment of an online purchase, the customer's address for the contractual

65 Plath in: Plath, BDSG/DSGVO, 2nd edition 2016, Article 6 GDPR, paragraph 10

conditional correspondence or when providing bank details for the

payroll transfer. On the other hand, the storage of customer preferences

for marketing purposes not required for the performance of the contract.66

6.3.3

Necessity to safeguard the legitimate interests of the

Responsible according to Art. 6 Para. 1 S. 1 lit. f DS-GVO

According to Art. 6 (1) sentence 1 lit. f GDPR, the processing is lawful if

they to protect the legitimate interests of the person responsible or one

Third party is required, unless the fundamental rights and freedoms of

data subject prevail.

The data processing must be in the legitimate interest of the person responsible

chen or a third party. The legitimate interest can be more legal,

be of an economic or non-material nature. In EG 47 are examples of this

legitimate interest listed. These are fraud prevention and

Direct Marketing Purposes. The first thing to determine is the interest of the

responsible body on the basis of the intended purpose.

The processing must also protect the legitimate interests of the

those responsible may be required.

The legitimate interests of the responsible body must not be overridden

overriding interests or fundamental rights or fundamental freedoms of the persons concerned

oppose person.

In doing so, the interests of both parties must be weighted. The to

The weighting factors developed to date are retained

also in view of the DS-GVO their validity, whereby in future the outflow

European fundamental freedoms and rights are of particular importance.67

Reasonable expectations are another criterion for consideration

of the data subject (EG 47). As part of the balancing of interests

It must therefore be taken into account whether a data subject at the time of the

Data collection and given the circumstances under which it takes place,

can reasonably foresee that processing for

this purpose will be done. Especially when personal

data are processed in situations where a data subject

reasonably does not have to expect further processing

the interests and fundamental rights of the data subjects prevail.68

66 Heberlein, in: Ehmann/Selmayr, Art. 6 GDPR, para. 13

67 Schulz, in: Gola, DS-GVO, Art. 6 para. 53

68 Schulz in Gola, DS-GVO § 6 para. 55

Figure 1 - Flowchart for classification of processing of data on physical,

physiological or behavioral characteristics of natural persons

Figure 1 - Flowchart for classifying processing of data on physical,

physiological or behavioral characteristics of natural persons

6.4

Legal assessment based on selected use cases

6.4.1

Case 1: Payment for school meals using fingerprints

A business used by a caterer for billing purposes

Lunch offers several methods by which

the school children can identify themselves when the lunch is handed out. To

These methods include identification using biometrics

Data. The fingerprint is electronically scanned and saved

and used for identification purposes; the generated template will be

used for identification within the respective student body. Want

If a child identifies himself when serving lunch, he puts his

Open your fingers, a template is calculated again and with the saved

different templates compared. If there is a match, so be it

Child identified, receives booked meal and financial statement

can be done digitally.

Acts on the processed electronic fingerprints of the students

it is dactyloscopic and thus biometric data in the sense

of Art. 4 No. 14 GDPR. These are also used within the meaning of Art. 9 Para. 1

DS-GVO processed for the purpose of clearly identifying the students,

since the meals served are intended for students for billing purposes

are to be assigned. As the only legal basis for this processing

A consent according to Art. 9 Para. 2 lit. a GDPR is possible.

The consent must be effective. Among the elements of an effective

Consent includes voluntariness and being informed. As long as a caterer

offers several equivalent and non-discriminatory methods

whose help the students can identify themselves when the food is served,

may be one granted by the parents or the students able to consent

Consent to the processing of biometric data as "voluntary"

will be In view of the special need for protection of this data

are strict about the voluntariness - also with the offered alternative

to set standards. It has to be real – and not just formal

– Act as an alternative, e.g. B. is only in the terms and conditions.

In the case of biometric processes, high levels of information must also be

demands are made. Since biometric data as individual and

universal identifiers can serve, the provision is clearer and

easily accessible information about the use of the respective data

as a sine qua non for fair processing.

In particular, if the algorithm used is the same biometric

templates are also generated in other biometric systems, the

affected person know that they are also in other biometric systems

can be recognized.69

6.4.2

Case 2: Access to company premises using fingerprints

A company that deals in wooden windows on the Internet and has about 50 employees

beiter plans to use a biometric access system

Fingerprint. The company has no safety-related field of activity; it

there is no difference to other, "normal" companies. The intended one

Purpose (access control) could also use a chip card, a PIN code

or a password.

Acts on the processed electronic fingerprints of employees

it is dactyloscopic and thus biometric data in the sense

of Art. 4 No. 14 GDPR. These are also used within the meaning of Art. 9 Para. 1

DS-GVO processed for the clear identification of the employees, since only

they should have access to the company premises. As the only legal

9 (2) lit. a

GDPR under consideration.

In order to be effective, consent must be given voluntarily

be. In accordance with recital 43, consent is then

not to be considered voluntary if there is a clear imbalance between

affected person and the person responsible for data processing.

This is generally to be assumed in the context of employment relationships.

Nevertheless, according to the European Data Protection Board

also in the context of employment situations conceivable in which

an employer can demonstrate consent to processing

occurred voluntarily, especially if the refusal of consent

would not have had any adverse consequences for the employee.70

Also according to § 26 paragraph 2 BDSG a processing of personal

Employee data is always based on consent

take place. However, when assessing the voluntary nature of consent

in particular the dependency existing in the employment relationship

69 Article 29 Working Party, WP 193, Opinion 3/2012 on developments in

Field of Biometric Technologies, p. 13.

70 Article 29 Working Party, WP 259, Guidelines on Consent under Regulation 2016/679,

p. 8. The European Data Protection Board has the working group related to the GDPR

Article 29 Working Party papers agreed at its first meeting.

of the employee and the circumstances under which the consent

has been granted to be taken into account. Voluntary can then in particular

are present if the employed person has a legal or economic

economic advantage is achieved or employer and employed person

pursue parallel interests. Neither one nor the other is

however, the case here.

Effective consent to the processing of dactyloscopic and thus

biometric data is ruled out in any case, if not as an alternative

Use of other means of access control, such as chip card, PIN code

or password, is offered.

6.4.3

Case 3: Biometric photo comparison by ski lift operators

The customers of a ski lift facility are photographed when entering the facility.

The facial images collected in this way are compared with reference photos, which are

Purchase of the ski pass were automatically compared. purpose of

Processing is the prevention of fraudulent performance in shape

misuse of the ski pass by unauthorized third parties,

who either only borrowed the ski pass or through a private, cheaper one

acquired resale.

The photographs taken are personal

Genetic data within the meaning of Art. 4 No. 1 DS-GVO and based on the mapped
Detected faces with biometric data within the meaning of Art. 4 No. 14 DS-GVO.
The recordings are biometrically matched to the person concerned
to be clearly identified. Article 9 (2) is a possible legal basis
lit. f GDPR into consideration. This is followed by processing of biometric data
allowed to uniquely identify a natural person if they
to assert, exercise or defend legal claims
is required, be it judicial or extrajudicial
Procedure.
The question arises whether an automated comparison is really necessary here
is. It should be borne in mind that such a comparison violates fundamental rights
and fundamental freedoms of the persons concerned. If
also isolated fraudulent performance in the form of an abusive
use of the ski pass by unauthorized third parties, it is
nor usually assumed to be the vast majority
the customer behaves in a lawful manner, i.e. for such types of controls no
any reason, unless there are specific circumstances in the individual case (e.g.

Evidence of abuse in a not inconsiderable number) the necessity
justify such a measure.
Against this background, the ski lift operator should carry out about
of spot checks based on the issued ski passes as a milder means
to be expected. For this purpose, the ski lift operator can use ski passes
those on which, from a certain period of validity, a photo of the holder

is printed.

6.4.4

Case 4: Access control with palm vein scan for airport employees

F-GmbH operates two airports. To secure the airport area

access to the security areas is only permitted to authorized persons

tet. Access authorization is granted by presenting the airport ID card

proven. In addition, an additional biometric identification

verification of the persons who have access to the security restricted areas of the

port, namely via the procedure of palm vein biometry. At the

Reading in the biometric data creates a corresponding palm vein pattern

created, which is encoded on the chip of the airport ID card

is deposited. A new palm vein recording is made at the checkpoints

created and with the recording stored on the chip of the ID card

compared. The hand vein scan brings the currently highest achievable

Security level in the unique identification of a person and be

also as an effective deterrent against any attempt at manipulation

to see, it is said from airport circles.

The recordings of the hand vein patterns are personal

data within the meaning of Art. 4 No. 1 DS-GVO. Since these for an automatic

tized biometric recognition can be used, it is

also biometric data within the meaning of Art. 4 No. 14 DS-GVO.

The processing of the recordings of the palm vein patterns is carried out in the sense

of Art. 9 Para. 1 DS-GVO for the clear identification of a natural

Person. The identity of the card holder should also be verified by the comparison

of the palm vein recordings are checked.

The legal basis for this procedure could be Art. 9 Para. 2 lit. g GDPR

be used. This is followed by processing of biometric data

then not prohibited if for reasons of significant public

interest is required. There is one thing about air traffic safety

significant public interest.

However, Art. 9 Para. 2 lit. g GDPR is not an independent act of permission

duration. There must also be a legal basis of Union law or

the law of a Member State. Section 8 (1) No. 4 comes into consideration here

Aviation Security Act. After that, the operator of an airfield for protection

of airport operations from attacks on air traffic security

obliged to protect the airside areas against unauthorized access

Secure and, as far as security areas or sensitive parts of the

Security areas are, only specially authorized access to them

allow people. The use of the palm vein scanner is intended here

serve.

However, the processing must be carried out to ensure the safety of air traffic

to be required. Two computer scientists showed in December 2018 that

how palm vein scanning devices can be outwitted. A use of this technique

under organizationally secure conditions and, as here, with a

Two-factor authentication, is still considered permissible in this case,

especially since it is equally effective, but with a view to informational self-determination

ment of the persons concerned probably not less intrusive means

be available.

6.4.5

Case 5: Targeted outdoor advertising through biometric facial analysis

A company operates an outdoor advertising system. This enables
using sensors on information screens, biometric features
of bystanders and the age and gender of these persons
analyze. The product serves to display the information displayed on the screen
Advertising messages to the age and gender of the people around
to fit. Detect camera sensors attached to a screen
and first capture the face of the viewer. These pictures will
temporarily stored as a video stream in the camera's buffer,
before the built-in software converts them into histograms. The Ka-
mera also has a calibration mode that allows visualization of the
recorded images. Other transfers of image data
do not take place, there is also no possibility of access to image data
for the company, advertising partners or third parties.
Variation: A company sells software for outdoor advertising.
The licensee installs the software on his hardware and brings over
the advertising screen a commercially available one to be purchased by himself
video camera on. This sends a video stream to the computer where
the software the detected faces (view towards the camera) and their

Evaluate direction of movement. Then the detected faces with
Using an algorithm based on biometric features (e.g. hair,
pronounced Adam's apple, wrinkles). After the
person has left the camera field, the result will be this
Evaluation recorded in a log file. The ones in RAM

Image information is automatically deleted when it is created.

The video recordings are personal data

Within the meaning of Art. 4 No. 1 DS-GVO, even if this is only for a very short time

period are stored.

The video recordings are evaluated using biometric features.

However, this is not done to clearly identify those affected

person, but rather to automatically assign them to a specific category

(e.g. age, gender). The legal basis for this processing

processing is therefore not in Art. 9 Para. 2, but in Art. 6 Para. 1 DS-GVO

to search.

According to Art. 6 (1) sentence 1 lit. f GDPR, processing is lawful if

if they are to protect the legitimate interests of the person responsible

is necessary, unless the interests or fundamental rights and fundamental freedoms

units of the data subject, the protection of personal data

require, prevail. The purpose of direct advertising pursued here can be

a legitimate interest within the meaning of Article 6(1)(f) GDPR

serving processing are considered. Equally appropriate means

to record the target group fairness of the advertising spots played

should not be available with the accuracy provided here.

In the weighing required under Art. 6 (1) sentence 1 lit. f GDPR

It is crucial whether the specific processing situation

emanating dangers so great and the occurring in their realization

Disadvantages are so significant that the interests of the persons concerned

can claim priority over those of the person responsible.71 Each

stronger the extent of the impairment caused by the respective data processing

is, the more "worthy of protection" are the interests of the data subjects.72

On the one hand, it speaks in particular for the fact that the interests of the

Affected people outweigh that here by the short-term inclusion

of facial images and the acquisition of individual biometric characteristics

tika fundamentally biometric data are processed. The processing

biometric characteristics of people's faces holds significant

71 Scholz, in Simitis, BDSG, § 6b marginal number 93.

72 Scholz, op. a. O., paragraph 94.

Security risks and where appropriate are from a compromise of these

data subjects lifelong consequences of identity theft

suspended because this data cannot be changed.

On the other hand, the software used does not collect data to a sufficient extent

Data in order to permanently identify the data subjects

to allow. In addition, the existing for the data subjects

The risk is rather low due to the relatively short storage period. That's true

however, only if the storage period is not extended

can, identification (i.e. recognisability) and profiling

of the persons concerned is excluded, the software used

cannot be manipulated in such a way that data is collected

can, which enable a clear identification, and which actually

The data processing that takes place and its purpose are sufficiently transparent

be made (Art. 13 Para. 1 DS-GVO).

Regarding the modification: Unlike the original case, the modification

conversion is not a closed system. In the form of the video

Personal data collected may be stored longer

and for other purposes, such as the clear identification of those affected

people, are reused. In this case, they move

technical and organizational measures taken on a German

lich lower level, so that in the result the interests of those concerned

people predominate here. The requirements of Art. 6 Para. 1 Sentence 1

lit. f GDPR are therefore not fulfilled.

6.4.6

Case 6: Access control on cruise ship

On a cruise ship, a photo is taken at check-in and

saved. Every time you leave and board the ship, the chip

card is read and the passenger uses the information stored in the system

photos checked.

When a person's face is clearly visible on a digital image

is shown, it is a personal data in the

Within the meaning of Art. 4 No. 1 DS-GVO and at the same time a biometric date in the

Within the meaning of Art. 4 No. 14 DS-GVO, as it is for an automated biometric

detection can be used.

Processing of biometric data to uniquely identify a

natural person within the meaning of Art. 9 Para. 1 DS-GVO is not here

before. The images are not used for automated biometric purposes

277

Recognition processed, but intended for a manual image comparison

come into use.

The legal basis for the processing is Article 6 Paragraph 1 Letter f

GDPR under consideration. The shipowner has a legitimate interest in

only passengers board the cruise ship. Exit control

of the ship gives the crew an overview of who is on

shore leave. Both also correspond to the interests of the passengers, so

that the processing can be considered lawful.

6.4.7

Case 7: video camera in jewelry store

The owner of a jewelry store installs a video camera and saves

chers the recordings for 48 hours. He does not have any software for

sight recognition, but intends to pass it on in the event of a crime

of video recordings to the police for the purpose of identifying

potential criminals through manual image comparison and, if necessary

through biometric methods.

The video recordings are personal data

Within the meaning of Art. 4 No. 1 DS-GVO. Video recordings, especially of faces

can, depending on the functionality of the technical system, basically for a

Evaluation (e.g. identification) based on biometric features

be. They then contain all the information required for such an evaluation

are relevant.

Such video recordings are therefore classified as biometric data within the meaning of

Art. 4 No. 14 DS-GVO. Prohibited is according to Art. 9 Para. 1 DS-GVO

only processing of biometric data for clear identification

a natural person, i.e. for the purpose of automated biometrics

Recognition.

However, such processing does not take place here, since the jeweler does not

has a biometric identification system. It is understood as

a system for the purpose of biometric identification of individuals

their behavior or biological characteristics.73

Also, keep in mind that it is not up to the jeweler to potential

identify criminals. This is the task of the police and state

73 ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV) as defined

in SC37 Working Group 1 for the International Standard ISO/IEC 2382-37

administration. In the event of a crime, the jeweler will give you the recordings

for a closer evaluation.

Article 6 (1) sentence 1 lit. f

GDPR. It can remain undecided whether the video surveillance through

Private individuals § 4 BDSG or Art. 6 Para. 1 S. 1 lit. f DS-GVO to apply

because both regulations lead to the same results in many cases.

According to Art. 6 Para. 1 S. 1 lit. f GDPR, processing is lawful if

they are necessary to protect the legitimate interests of the person responsible

is, unless the interests or fundamental rights and freedoms of

data subject who require the protection of personal data,

predominate. The purposes pursued of preventing criminal offenses on the one hand

as well as the conviction of criminals on the other hand can be considered legitimate

Interests within the meaning of Article 6 (1) sentence 1 lit. f GDPR are considered.

Equally effective, but with a view to informational self-determination

of the persons concerned are probably not available

available.

In the weighing required under Art. 6 (1) sentence 1 lit. f GDPR

it is decisive whether that depends on the specific processing situation in each case

emanating dangers so great and the occurring in their realization

Disadvantages are so significant that the interests of the persons concerned

can claim priority over those of the person responsible.74 Each

stronger the extent of the impairment caused by the respective data processing

is, the more "worthy of protection" are the interests of the data subjects.75

To ensure that the interests of the data subjects worthy of protection

weigh, the recording and storage of facial

images and their basic suitability for clear identification

natural persons. The resulting risks to the rights

and freedoms of the data subjects must be carried out by the person responsible

minimize technical and organizational measures. In favor of

However, those responsible can only go out of the balance if he

ensures that a storage period of 48 to a maximum of 72 hours is not possible

is exceeded that there is no face recognition software on its hardware

ware is installed and used and that the data processing that takes place

and their purposes are sufficiently transparent to the data subjects

be made (Art. 13 Para. 1 DS-GVO).

74 Scholz, op. a. O., para. 93.

75 Scholz, op. a. O., paragraph 94.

6.4.8

Case 8: VIP guest detection in hotels

A hotel uses a video surveillance system with facial recognition

system that alerts the hotel manager to arriving VIP guests

might. Recordings of these VIP guests were previously made with their consent

included in a database. However, everyone else will too

Guests made video recordings, templates created and with the content of

database compared.

If a person's face is clearly visible in a digital image,

is formed, it is a personal data in the sense

of Art. 4 No. 1 GDPR. The here with the help of the video surveillance system

processed facial images are also considered biometric data within the meaning of

Art. 4 No. 14 DS-GVO, as they are for an automated biometric

detection can be used.

The video recordings are also processed for the purpose of clear

identification of a natural person within the meaning of Art. 9 Para. 1 DS-

GMO. The hotel manager wants to draw attention to arriving VIP guests

be made, can address them by name and not as

Distinguish between guests classified as VIPs.

The processing affects all persons entering the entrance area of the hotel

enter, i.e. guests registered and unregistered as VIPs. purpose of

Processing is biometric recognition. Become of all guests

digital facial images created. The facial images become biometric

Characteristics extracted and compared with those present in the hotel's own database

data compared. Whether the result of this comparison is a meeting

Whether or not this occurs, it does not matter for the purpose of the processing.

Theoretically, every person who enters the entrance area of the hotel,

be a VIP guest. The inclusion of data from persons whose

Comparison ultimately leads to non-match is a necessary and desired part

of the procedure and gives it its meaning.

For processing the facial images of guests already registered as VIPs

can, in accordance with Article 9 (2) (a) GDPR, give their express consent

be used. For processing the facial images of others

A legal basis is not apparent to guests. In its current form

the procedure cannot be brought into line with the GDPR.

280

Appendix I - Privacy Materials

7.

Selection of measures and conclusions for the

process design

7.1

model and assumptions

7.1.1

methodology

Because the processing of personal data always involves a risk for the rights

and freedoms of data subjects are those responsible for it

obliged to comply with the principles of Art. 5 DS-GVO. The hit

Any measures must be documented in accordance with Art. 5 Para. 2 GDPR. The

Non-compliance with the principles enshrined in Art. 5 can, according to Art. 83

Paragraph 5 lit. a GDPR can be punished with a fine.

In order to be able to comply with these principles, according to Art. 32 DS-GVO

suitable technical and organizational measures are taken,

to ensure a level of protection appropriate to the risk. responsible

literal and processors have the respective measures below

Considering the state of the art, implementation costs and

the type, scope, circumstances and purposes of the processing as well as

the different probability of occurrence and severity of the risk

for the rights and freedoms of natural persons. biomet

Technical data usually requires special attention because

an individual is irrevocably affiliated with and based on them

Data due to their individual behavioral or physiological

characteristics can be identified without a doubt.

The independent data protection authorities of the federal government and the

Country-developed Standard Data Protection Model (SDM) provides appropriate

Assistance to put the legal requirements of the GDPR in concrete terms

to transfer technical and organizational measures, even if the

Work on individual parts is not yet complete. The SDM

structures the legal requirements in the form of the following guarantees

performance objectives: data minimization, availability, integrity, confidentiality,

Transparency, non-chaining and intervenability. these requirements

aim at characteristics of a legally compliant processing, which through technical

niche and organizational measures must be "guaranteed".

The warranty consists in the exclusion of deviations from one

lawful processing. Through these guarantee goals

the legal requirements of the DS-GVO in the regulation

required technical and organizational measures. The

SDM contains a listing of generic technical and organizational

Measures. With the help of this generic catalog, each individual

Processing both by the person responsible himself and by the

supervisory authority to check whether the on-site measures are in place

meet the legally required target of measures.76

Due to the diversity of the systems considered, a complete and detailed

detailed description of the risks and appropriate technical measures to be taken

nical and organizational measures within the framework of the present

paper not possible. In accordance with the principles of data processing

In order to be able to comply with Art. 5 DS-GVO, those responsible must use their systems

examine individually.

7.1.2

system build

The first step is the system to be used

analyze. The investigation of a system first requires the

tuning of the system boundaries and the basic structure of the system.

Systems for processing biometric data, as in the present

Paper presented typically consist of the following

Components:

– biometric capture devices

– Processing logic (in particular, performs the biometric feature

extraction and biometric recognition by)

– Actor(s) (output devices connected to the processing logic)

– Reference database, enrollment database

– further input interfaces

– further output interfaces

– Maintenance interfaces

– Connections between the components

The actors involved in the processing must then be identified.

Actors who have an influence on the processing of the data in the system

or may have are usually:

– system operator

- Affected

– maintenance company

76 Standard Data Protection Model (SDM), version 1.1, adopted by the 95th Conference of the

independent federal and state data protection supervisory authorities on April 26

2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Method_V1.1.pdf, p. 5.

- Manufacturer

– if necessary, bodies that make data available to the system or data

obtained from him

In addition, such actors must also be considered who have an interest

in improper processing of data in or out

the system could have. This is necessary in order to be able to check

whether the security measures taken by the person responsible, the

Protect those affected sufficiently against misuse. here

become both personal and economic or political motives

be taken into account. Figure 2 - Overview of typical components

biometric systems shows the actors and components of biometric

systems and their connections.

Figure 2 - Overview of typical components of biometric systems

Each of the components mentioned is not found in all systems. So

the reference database is omitted for range measurement and in authentication

verification procedure, the reference database can refer to a data record

be restricted if, for example, the identity of a person exclusively

is checked using the data stored in an identity document.

The maintenance interface, on the other hand, will usually have to be taken into account:

Embedded systems contain such an interface for purposes of

programming and diagnostics; on open systems such as PC technology

based solutions allow the use of remote maintenance technology without any problems

or have the corresponding components already pre-installed.

7.1.3

Overview of the processing typical for biometric systems

According to the previously considered biometric systems and case studies,

essentially three types of biometric systems are distinguished

are each having different risks to rights and freedoms

Affected bring:

– systems for biometric search,

– systems for biometric comparison or

– Systems for biometric property derivation.

Currently practically relevant biometric systems have in common that

a collection of biometric characteristics of data subjects in the

The form of biometric samples takes place and from these biometric features

be extracted. Processes for biometric searches also require

naus that biometric data in a database (usually together

with additional data) are recorded, the so-called enrollment. Therewith

can basically six different types of processing

be differentiated (recording, feature extraction, enrollment, search,

comparison and property derivation).

In biometric enrollment, a biometric enrollment device

a biometric characteristic of a data subject in the form of a

biometric samples.

For further processing of the recorded biometric samples

must be extracted from these biometric features. Dependent

whether the biometric system is biometric features or biometric

ical samples are used, this processing step occurs directly after

biometric registration or feature extraction is part of the

processing logic (enrollment, search, comparison or property derivation).

At enrollment, a biometric probe (sample or feature) is used as a

biometric reference together with other data of the data subject,

which are collected via a corresponding input interface, in a

stored in a biometric reference database.

The biometric search checks whether a given biometric

Sample with biometric references in the biometric reference data

bank matches and a list of possible candidates is sent to a

given output interface.

Compared to the biometric search, the biometric comparison

merely checked to what degree a given biometric sample is used

matches a biometric reference and the corresponding

equal value is forwarded to an output interface.

When deriving biometric properties, a biometric

Sample biometric properties are calculated and sent to an output interface

pass on. The biometric samples can be from a

biometric detection device, via an input interface or from

come from a biometric reference database.

Should future procedures, for example, supported by Artificial

intelligence, perform biometric recognition in a different way,

the processing steps carried out would have to comply with the specifications

of this paper are considered separately.

7.2

risks

In order to be able to guarantee an adequate level of protection, the

Responsible for the risks related to the processing of the rights

and freedoms of natural persons.

The concept of risk is not explicitly defined in the GDPR. Out of

the recitals 75 and 94 sentence 2 GDPR, the following definition can

tion can be derived: A risk within the meaning of the GDPR is the existence

the possibility of the occurrence of an event that itself causes harm

(including unjustified interference with rights and

freedoms of natural persons) or to further damage to

one or more natural persons. It has two dimensions:

First, the severity of the damage, and second, the likelihood

that the event and the consequential damage occur.77

The GDPR gives the person responsible two levels in recital 76

to determine the risk of a personal processing activity

before, namely "risks" and "high risks". To determine the risk level

are the type, scope, circumstances and purposes of the processing

activity and the specific probability of occurrence and severity

of the risks involved in the respective processing activity.

Especially when processing biometric data for unique identification

cation of a natural person, the specific risks must be considered

77 Conference of the Independent Federal and State Data Protection Authorities (DSK),

Policy Brief No. 18, Risk to the rights and freedoms of individuals, p. 1.

which result solely from this circumstance.78 For the identification of

It is advisable to start with data protection risks by asking the following questions:

– What damages can be based on natural persons

of the data to be processed arise?

– By what, i. H. through what events can damage it

come?

– What actions and circumstances can lead to the occurrence of this

Events coming?79

In the procedures considered here, predominantly biometric data are used

for the clear identification of a natural person within the meaning of Art. 9

Para. 1 DS-GVO processed. Regardless of the probability of occurrence

of possible damage can at least regularly be inferred from a particular

ren severity of the damage can be assumed. This is already evident

from the fact that it is partly a special processing

Categories of personal data within the meaning of Art. 9 Para. 1 DS-GVO

acts for which the GDPR provides for an increased need for protection.

In addition, the damage should not or hardly be reversible, since the identity

a natural person, as already mentioned, irrevocably and

is inextricably linked to their biometric data. The processing

biometric data for the unique identification of natural persons

therefore an important indication of a "high risk" within the meaning of the recital

grundes 76.80 The short paper no. 18 of the DSK on the topic “Risk for the

Rights and freedoms of natural persons" provides for the assessment of the

Risks a matrix that helps those responsible to determine the risk

of the processing activity they intend to use.

Should those responsible come to the conclusion that the

intended processing activity is likely to pose a "high risk" for the

represents the rights and freedoms of natural persons is the implementation

a data protection impact assessment according to Art. 35 DS-GVO is necessary.

78 European Data Protection Board: Working Paper 193 “Opinion 3/2012 on

Developments in the field of biometric technologies”, p. 5.

79 Conference of the Independent Federal and State Data Protection Authorities (DSK),

Policy Brief No. 18, Risk to the rights and freedoms of individuals, p. 2.

80 See also: European Data Protection Board: Working Paper 248 “Guidelines on

Data Protection Impact Assessment (DPIA)”

7.3

Measures

If you follow the system of the standard data protection model, the

protection goals mentioned at the beginning (securing data minimization

tion, availability, integrity, confidentiality, transparency, non-chaining

and intervenability) also when processing biometric data or

can be achieved when using biometric methods. There they are

specific risks associated with the use of biometric methods and

associated with the processing of biometric data.

Each of the protection goals can be defined by certain technical and

organizational measures are achieved that are included in the standard data

protection model are described at least in generic form.81 In addition

the generic measures written in the SDM for the implementation of the

Guarantee objectives is another component to consider, provided for

an intended processing activity poses a "high risk" for the rights

and freedoms of the persons concerned. A "high ri-

siko" corresponds to a "high protection requirement" and leads to measures

according to higher requirements for their effectiveness or required

even additional measures.82 In concrete terms, this means that each of the

fenen protective measures themselves based on the protection goals

must be assessed. if e.g. B. the protection goal "confidentiality"

in a biometric system is to be achieved by a rights and

Role concept is determined according to the principle of necessity, so must

this rights and role concept available, with integrity, confidentially,

be non-linkable, transparent and intervenable. Or, to

another example: if there is a high risk, it is not enough to

to log systems; the log data must in turn be available

be, the audit strength can z. B. by using signatures

secured, it is important to consider whether log data is only encrypted

are stored, etc. It is also crucial that in the case of high risks

According to the SDM, a data protection management system is to be operated that

ensures that identified weaknesses and deficiencies are also sustained

can be lifted.

81 Standard Data Protection Model (SDM), Version 1.1, Adopted by the 95th Conference of the

independent federal and state data protection supervisory authorities on April 26

2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Method_V1.1.pdf, p.22 ff.

82 Standard Data Protection Model (SDM), Version 1.1, Adopted by the 95th Conference of the

independent federal and state data protection supervisory authorities on April 26

2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Method_V1.1.pdf, p.32.

287

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection

7.4

residual risk

After the selection of technical and organizational measures and

their implementation must reduce the remaining risk for the persons concerned

be assessed. If, after the implementation of a data protection

If there is a high residual risk according to Art. 35 DS-GVO, the responsible

supervisory authority can be consulted (Art. 36 DS-GVO).83

83 Conference of the Independent Federal and State Data Protection Authorities (DSK),

Policy Brief No. 18, Risk to the rights and freedoms of individuals, p. 6.

288

Appendix I - Privacy Materials

3.9

Conference of Independents White Paper

Data protection supervisory authorities of the federal and state governments 07.

Nov 2019

Technical data protection requirements for messenger services

hospital area

Messenger services have paralleled the spread of smartphones in the

central importance for the exchange of messages in recent years

reached, other communication services such as e-mail or SMS in many cases replaced

and are among the most popular forms of communication in private everyday life.

The reasons for this are in addition to the fact that it can be used at any time via smartphone

and the ease of use of the range of functions, which allows next

exchange text messages including pictures, videos or voice messages,

to carry out voice and video calls and optionally with individual sub-

to communicate with other participants or in the group. On top of that it is

are often offers that can be used free of charge.

Due to the widespread and established use in the private sector

is increasingly relying on these messenger services in the health sector

resorted to, often combined with the use of a private terminal

rats.84,85,86

The professional or commercial use of messenger services is subject to

legal data protection requirements that common messenger services

long do not correspond or only to a limited extent. Especially the widely used one

When used for business purposes, the WhatsApp service leads to a number of

Problems87 that largely rule out use in hospitals.

The same applies to other services that are frequently used in the private sector.

With a view to the sensitivity of the data concerned in the health sector

and the special protection that this according to Art. 9 General Data Protection

ordinance (DS-GVO) are therefore more suitable when making your selection

Messenger services for the transmission of patient data in the hospital

area of the person responsible for the following data protection requirements

to consider. The specifications that can be derived from this also serve as

84 https://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/902262/klinik-jeder-drit-te-arztverschickt-patientendaten-via-apps.html

85 https://www.kardiologie.org/kardiologie/whatsapp-und-co--kennen-aerzte--was-sie-do-/15742284

86 https://deutsches-datenschutz-institut.de/wp-content/uploads/2018/05/FAZ_Messen-eng-2018.pdf

87 https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/

Orientation for the use of messenger services in private practice

Area.

The use of messenger services in the hospital sector can be

different scenarios (e.g. internal hospital use, consultation,

Communication with emergency services, communication with medical practices, communication

communication with other service providers, communication with patients).

Depending on the scenario, different requirements can arise.

The following requirements relate primarily to the actual

Messenger application, communication between participants who

platform used and the devices used. The actual operation

of messenger services in the hospital is only taken into account to the extent

than general requirements. Not considered

are used in this paper due to the heterogeneity of the conditions of use

functional requirements of hospital operations including necessary

technical and organizational precautions.

Significant risks", as formulated in the GDPR, are in the processing

of data categories mentioned in Art. 9 DS-GVO such as health data or

always accept genetic data. The need for protection lies in the

personal data itself. If in this paper the processing in

is approached in a hospital, then because the data protection

Legal requirements are fundamentally addressed to "the" person responsible (in the sense of

Art. No. 7 DS-GVO) and in hospitals i. i.e. R. always one too

extensive processing of personal data takes place.

Insofar as the following text formulates mandatory requirements, these are

required by data protection law and must therefore be implemented

become. Target requirements, on the other hand, can have different characteristics

have: If there are equivalent authorities to ensure data protection

alternatives exist, it is sufficient if one of them is implemented. Included

it remains with the person responsible within the scope of Art. 24 Para. 1, Art. 32

Para. 1 DS-GVO leave room for maneuver which the possibility

ten he actually chooses. In addition, should-requirements

one that is desirable from the point of view of data protection, legally

but do not describe a mandatory circumstance. Here he decides

Responsible himself whether he meets the requirement.

I

messenger application

1. The application must offer the possibility to

according to Art. 13 DS-GVO about the use associated with

teach data processing. The information must be in one

clearly recognizable area (e.g. information on data protection, data protection

declaration) for access at any time.

2. The application must be able to use or

access to the data stored about it to its own previous

authentication (e.g.

3. PIN, fingerprint etc.). This can be done on the operating system side

functions, but must move from protection to unlocking

of the mobile device (see III.1).

4. The application must have the option of receiving contact data from

communication participants in a separate ad-

memory separate from the smartphone's memory. she should

in this context have a possibility of contacts and

to import related information from other sources.

She must still have the ability to send messages as well

File attachments such as images, videos, documents, etc. exclusively in one

own, from the general memory areas of the smartphone

separate storage in encrypted form. It can open

cryptographic functions present in the operating system

be grabbed. The application should be able to

Import messages and file attachments from other sources.

5. The application should offer the possibility for the server-side

identification, encryption or digital signature required data

(e.g. certificates, keys) to import. A communication about

the messenger application should only be used on the basis of a reliable

chen identification and authentication of the communication partners

to be possible.

6. Are electronic signatures or other electronic certificates

used, a certificate management must be available. This

includes ensuring that electronic keys or certificates

be clearly assigned to a legal or natural person,

but also checking the validity of the electronic keys

or certificates. In particular, compromised keys or

Certificates can be rendered unusable. It is irrelevant

whether the management of the used Public Key Infrastructure ("PKI")

is operated by the controller himself or by a third party

is made available.

7. The application should have an interface that allows it

to be integrated into the IT structures and processes of a hospital (e.g.

Upload of security profiles or presets, synchronization

with the hospital information system, transfers of treatment

relevant messenger messages as part of the patient documentation).

8. The application must have the option that it

managed to delete data specifically or generally (messages, files,

contacts, etc.). You should be able to set a deadline

after which such data will be automatically deleted.

9. Insofar as third-party services are used within the scope of using the application

error analysis are integrated (e.g. Crashlytics), this must be open

displayed recognizable and marked as optional; the for

a transmission for troubleshooting intended data categories

must be clearly recognizable. A corresponding data transfer
must be disabled by default. It must be ensured,
that data subject to medical confidentiality or data about the
Messenger users' usage behavior is not affected in this way
be disclosed without authorization.

10. With regard to the availability of the data according to Art. 32 (1) lit. b DS-GVO, the application must have the option of backing up the
contact data/content data/communication processes. So far
the storage in compliance with Art. 28 DS-GVO by a
service provider is taken over who does not meet the requirements of the
Art. 9 Para. 3 DS-GVO, there must be the possibility to use the data
to be encrypted in accordance with the state of the art before handing over
that decryption is only possible with a key,
which is not disclosed to the service provider and is secured separately.
A backup to ensure availability is off
data protection reasons from storage to documentation
tion purposes. The relevant from a professional point of view
Medical documentation obligation (see § 10 MBO-Ä, § 630f BGB) remains
unaffected by this; it must not be lost when using messengers
be neglected. A documentation (partially) in Messenger
has taken place and cannot be traced in the patient documentation,
must stop. Treatment-related content data relating to
refer patients and are generated on the end device (e.g. by
camera recordings) must be in the IT structure of the hospital
stored and can be found in the treatment documentation
can, insofar as this is required from a professional or civil law point of view.

This does not necessarily require a special to the HIS

customized function in the messenger application as long as the

Process can be mapped efficiently in other ways. Requirements of the professional and

Civil law remains untouched.

11. If images are sent via the application (e.g.

Patient recordings, screenshots) in which personal

personal data for the purpose pursued and identity

medical point of view are not required, and the patient's identity before

Background of a careful treatment exceptionally dispensable

it should be possible to black out parts of the recordings

or otherwise excluded from the presentation (data minimization,

cf. Art. 5 (1) lit. c, Art. 25 (1) GDPR).

12. For the messenger solution, the hospital and possibly the

commissioned processors to provide suitable proof of this

lead to the fulfillment of the data protection principles and the

Ensuring the security of processing in accordance with Art. 25 Para. 1 or

32 DS-GVO have been effectively implemented or

the specifications of the GDPR for the respective processing operations

are complied with (e.g. certification according to Art. 42 DS-GVO (if

available), certification according to European Privacy Seal, BSI basic protection certificate

certification). On the part of the hospital, the messenger application

also based on the test catalog for technical data protection at Apps88

evaluated and the result within the framework of accountability (Art. 5

Para. 2 DS-GVO) are documented.

13. The application must comply with the configuration settings

Principle of data protection-compliant default settings (Art. 25 Para. 2 DS-

GMOs).

14. The application should have (semi-) automatic update procedures.

II.

communication

1. The confidentiality and integrity of the data managed via the messenger service

ten medical communication must take into account the status

of technology via end-to-end encryption between the

communication participants are guaranteed (Art. 32 para. 1 lit. a

GDPR).

88 https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf

2. As far as the integrity of the data communicated via the messenger service

is important for subsequent actions, should the possibility

exist, taking this into account by cryptographic functions

of the state of the art (Article 32 (1) sentence 1 GDPR).

Furthermore, to ensure the integrity of the information,

if this is important for subsequent measures, ensure that

ge borne that all communicated data at the recipient

arrive. If a message from one messenger to several

Messages are distributed (e.g. because Messenger only sends one message per message

certain number of characters or file size) must have mechanisms

be integrated that tell the recipient whether the message sent

has arrived in full or whether individual messages are missing. This

can e.g. B. by adding a check number "message x from y"

happen so that the recipient sees whether all the messages are with him

arrived.

3. Connection data for the communication conducted via the messenger service

communication (e.g. communication participants, time, device and

Location data) may only be stored for as long and to the extent as

it for the transmission of messages by a service provider or

is required as part of a necessary documentation. the com

Communication or metadata may only be used for your own purposes

of the hospital are used. A use for other purposes

by the manufacturer of the solution or the platform operator (e.g. Wer-

purposes) is not permitted.

4. The use of open communication protocols should be used at least as an option

kolle (e.g. XMPP89) to be able to communicate with others

enable messenger services.

III.

Endpoint security

1. The end devices used must have effective access protection

(e.g. PIN/passphrase, biometric solutions). The internal

Device memory must be protected by encryption in such a way that

that decryption requires knowledge of the login data.

2. Only devices may be used whose operating system

version by the manufacturer of the operating system platform (Google or

Apple) are currently supplied with security patches and where all

89 Extensible Messaging and Presence Protocol (XMPP) of the IETF, as a protocol standard

such security patches have been applied. This requires,

that the manufacturers of the end devices make any necessary adjustments

the respective device type immediately.

3. The end devices must have a mobile device management service

(MDM) are subject to a secure configuration

of the devices and data connections the risk

a. the infiltration of malicious code (e.g. via vulnerabilities in the

Browser, file viewer, operating system platform and interfaces

of the device),

b. unauthorized access by third parties to the device itself and to

the processed data

minimized, prohibits processing when the operating system

of the device does not have the properties mentioned under 2, the

application of security patches and updates and the

Installation of apps monitored. The service should also provide a location

and allow the devices to be locked or wiped if lost, wherein

However, a permanent localization of the owner can be ruled out.

IV

Platform/Operation

1. As far as the messenger service used is concerned

to provide a publicly available telecommunications service i. s.d. § 3

No. 17a Telecommunications Act (TKG), this must

because we meet the applicable requirements of the GDPR and TKG, below

in particular Section 6 and Part 7 TKG. He is in terms of compliance
of telecommunications and data protection requirements
choose carefully. The conclusion of a contract in accordance with Art. 28
Para. 3 DS-GVO (see below) is not necessary in this case.
2. It must be ensured that only authorized users participate in a
message exchange can participate. This applies to both the
communication of a defined, closed user group (e.g.
hospital) as well as for communication with other participants
mers of the messenger service. A suitable one is required for this
registration process or corresponding authorization/authentication
tification mechanisms, for example through a centrally administered identification
activity management system.
3. For the processing associated with the use of the messenger service
If these are extensive, a data
protection impact assessment (DPIA) carried out in accordance with Art. 35 GDPR

become. If a non-public used by several responsible
public platform, it is sufficient to create a DPIA once for the
perform platform.
4. For the messenger solution, the hospital is a regular
Verification, assessment and evaluation of the effectiveness of the
technical measures taken to ensure the security of the processing
and to take organizational measures (Art. 32 Para. 1 lit. d
GDPR).

5. The messenger solution should be both an operation and a service

service provider/processor as well as in the technical infrastructure

structure of the hospital (on-premises).

6. Insofar as the operation of the process relies on processors

is used, it must be ensured that these comply with the regulations

subject to the General Data Protection Regulation and the requirements

of Art. 9 Para. 3 DS-GVO i. V. m. § 203 Abs. 3 StGB and others

comply with any relevant regulations (e.g. hospital laws). For this

should refer to service providers in Germany, the European Union or the

European Economic Area can be used.

7. A contract is concluded with the contract processors involved in this respect

Art. 28 Para. 3 DS-GVO to close. Looking at the sufficient

Guarantees of technical and organizational measures, processing in

Compliance with the GDPR and the protection of the rights of those affected

The service provider should have appropriate evidence

(e.g. certification according to Art. 42 DS-GVO, certification according to European

Privacy Seal, BSI basic protection certification).

8. For the service provider as part of the messenger solution

stored data must be regularly deleted (cf.

TZ. I.8). Personal patient data must be on the servers

of the person responsible are stored. The temporary storage period

on the end devices should therefore be kept as short as possible and in

zen cyclic intervals from the end device to the designated server

be relocated. This also applies to any container solution in the

Mobile messenger app.

9. As soon as they are available, security-related updates of the

App to be carried out promptly on all devices used.

296

4. Briefing Papers of the Conference of Independents

Federal and state data protection supervisory authorities

Appendix I - Privacy Materials

Short Paper No. 20

Consent according to the GDPR

This short paper by the independent federal data protection authorities and

of the countries (Data Protection Conference – DSK) serves as a guide, in particular

others for the non-public area, as in the opinion of the DSK

General Data Protection Regulation (GDPR) applied in practice

should be. This view serves as a summary or supplement

the Guidelines on Consent of the European Data Protection Board

(WP 259 rev.01 “Guidance on Consent under Regulation

2016/679").

Prerequisites and differences to the until May 24, 2018

applicable law

Even under the GDPR, consent is a key legal

basis for the processing of personal data. General Rules

ments to this can no longer be subject to the Federal Data Protection Act

(BDSG), but directly from the GDPR (Art. 4 No. 11, Art. 7).

A consent is only effective if it is voluntary and related

in a specific case – is given in an informed manner. The writing is

not mandatory; rather, an unequivocally given

Bene expression of will in the form of a declaration or other clear

confirmatory act by which the data subject gives their consent

granted unequivocally for data processing. The confirming act

If these requirements are met, it can also be done electronically, by "clicking

cken" of a field on the Internet, or also verbally. At the election

the appropriate form, it should be noted that the person responsible for the issuance

must be able to prove consent (see below).

From Recital (Recital) 32 of the GDPR it can be seen that

Silence, already ticked boxes or inaction of those concerned

person does not constitute consent. This is also not the case in my opinion

of the European Data Protection Board for easy continued use

of a service. For the granting of consent is rather an active

behavior of the persons concerned required. Different than before

issued case law (Federal Court of Justice, judgment of July 16, 2008, VIII ZR 348/06; Federal Court of Justice,

judgment of 11.11.2009, VIII ZR 12/08) it is no longer sufficient to

To refer people to contract clauses which are fictitious statements

included and for which it was considered effective consent if

a pre-formulated consent text has not been crossed out or

A cross was not set to deny consent.

Particular attention is paid to the General Data Protection Regulation

to direct the voluntary nature of consent. It can only then

be gone that a data subject gave their consent voluntarily

given, if she has a real and free choice, i.e. is able to make that choice

Refuse or withdraw consent without suffering any detriment

(see recital 42). This is not usually the case, for example, if

the fulfillment of a contract from consent to data processing

is made dependent, which is not necessary for the fulfillment of the contract

(Art. 7 para. 4 in conjunction with recital 43 GDPR, so-called ban on coupling).

In addition, consent does not regularly provide a valid legal basis,

if there is a clear agreement between the data subject and the controller

imbalance and it is therefore unlikely that the

consent was given voluntarily. This also results from Recital Gr. 43

Consent must be given in an informed manner. In recital 42 of the DS

GMO is specifically designed to ensure that a person responsible

pre-formulated declaration of consent in a comprehensible and easily accessible

provided in a clear and simple language

will contain no misleading clauses and the affected

person is at least informed as to who is responsible and

for which purposes your personal data is processed

should. In addition, according to the opinion of the EU

European Data Protection Committee on the type of data processed,

about your right to revoke your consent at any time, if necessary about the

use of the data for automated decision-making and about

possible risks of data transfers to third countries without existence

of an adequacy decision and without appropriate safeguards

Article 46 GDPR to be informed.

According to Art. 7 Para. 1 DSGVO, the person responsible has an express

Obligation to be able to prove the granting of consent. This

Obligation stands with the calculation regulated in Art. 5 Para. 2 DS-GVO

duty in connection. This applies not only in the sense of

last rule if the existence of consent is disputed, but

generally. Also with controls of the supervisory authorities must therefore

proof of consent can be provided. Becomes

consent is given electronically, the person responsible must ensure

lend that the consent is logged. It is not sufficient, for example,

if merely to the proper design of the appropriate

Website is referenced without in individual cases the proof of actually

to provide the consent given. The person responsible has appropriate

technical and organizational measures to ensure that

the data protection principles, in particular accountability, to

be set. To do this, he must use technical systems that

Data protection through technology design and through data protection-friendly

enable presets.

The data subject has the right to withdraw consent at any time.

The revocation applies with effect for the future. Based on Consent

Processing operations in the past therefore remain lawful. On

the revocability of the consent must be given to the person responsible before submission

indicate the consent. Withdrawal of consent must be so easy

how to grant.

Survival of Consents

Consents granted before the GDPR came into effect are effective according to recital

171 of the GDPR, insofar as they are of the type according to the conditions of the GDPR

are equivalent to. This includes the following points in particular:

- The granting of an effective consent must, according to Art. 7 Para. 1

DS-GVO can be proven, which is a corresponding do-

documentation required.

- The consent must have been given voluntarily (Art. 4 No. 11 DS-

GMO), whereby the special requirements according to Art. 7 Para. 4 DSGVO

i. V. m. ErwGr. 43 DS-GVO must be observed.

– A declaration of intent is required for the specific case, in

in an organized manner and in an unambiguous form (Art. 4 No. 11 GDPR),

whereby the requirements according to Art. 7 Para. 2 DSGVO i. V. m. ErwGr. 32

and 42 GDPR must be observed.

– The person responsible must have mechanisms in place that allow the revocation

enable consent and provide information such as the

Consent can be revoked.

– In the case of consent by a child in relation to services of information

mation society must meet the requirements of Art. 8 DS-GVO

present.

If the above conditions are not met, previously granted consent

don't go. In addition, the data subject must at the time

the information is available when the declaration of consent is submitted

have had, which is necessary for the submission of an informed consent

are. After recital 43 this is at least information about who the

Responsible is and for what purposes the personal data

are processed.

This information is partly identical to that according to Art. 13 DS-GVO

intended information obligations. The additional information

Information obligations must be met for the continued validity of previously granted consent

on the other hand, have not been fulfilled in principle. Regardless of the

mentioned conditions for granted consent must in future

information obligations according to Art. 13 GDPR are observed.

Consequences of invalid consent

Consent that does not meet the requirements presented is

ineffective and cannot be used as a legal basis for data processing

be used. The data processing in this case to another

to support a legal basis, for example the protection of legitimate interests

food of the person responsible or a third party (Art. 6 Para. 1 lit. f DS-GVO),

is fundamentally inadmissible, because the person responsible must comply with the principles

of fairness and transparency (Art. 5 Para. 1 lit. a DS-GVO). Je-

otherwise is an arbitrary alternation between consent and others

Legal bases not possible.

If the consent proves to be ineffective or the person responsible

cannot prove the existence of consent, the processing of

data on this basis unlawful. In the event of violations of the basic

rates of processing, including the conditions for consent,

can by the competent supervisory authority in accordance with Art. 83

Paragraph 5 lit. a DS-GVO a fine can be imposed. Also come

Depending on the circumstances of the individual case, claims for damages by

data subject into consideration.

Special categories of data and consent of a child

According to Art. 9 Para. 2 lit. a DS-GVO is special for the processing

Categories of data (health data, genetic and biometric

data, etc.) express consent is required for this; implied

Actions are therefore excluded. Art. 8 DS-GVO contains special

Conditions for a child's consent in relation to the services

information society.

300

Appendix I - Privacy Materials

Special processing situations

There are also some special

regulations to be observed. You can see that in employee data protection

new BDSG based on the opening clause of Art. 88 GDPR

the requirement of the written form, unless due to special circumstances

another form is appropriate (§ 26 Para. 2 S. 3 BDSG; see also

the short paper no. 14, on employee data protection). specifics are

also when consenting to data processing for research purposes

to note.

A notice:

Note on the use of this short paper: This short paper may – without

Consultation with a supervisory authority – commercial and non-commercial

used, in particular duplicated, printed out, presented, modified,

processed and transmitted to third parties or with your own data and data

ths of others are merged and become independent new data sets

connected if the following source is mentioned:

"Conference of the independent data protection authorities of the federal and

countries (data protection conference). Data License Germany – Attribution

– Version 2.0 (www.govdata.de/dl-de/by-2-0)".

301

2. Activity Report on Freedom of Information

II

Second part

2. Activity Report on Freedom of Information

introduction

1. Introduction

introduction

The importance of freedom of information is still scarce among the population

been noticed. With the abundance of false and incomplete ones

Information disseminated in particular on social media,

meet the requirements for the seriousness of the press and the broadcasting

che basic service no longer for informational services of general interest.

Informational self-determination also requires correct information

by the state. People's sovereignty and information about it

Government actions are inseparable. This information requirement

must not be used exclusively to siphon off government information

degenerate for commercial purposes. The officer for information

heit has to check in each case whether a request for information of the informational

self-determination serves.

With regard to the basic constitutional requirements and dogma

refer to the technical principles of the Hessian Freedom of Information Act

I refer to my comprehensive statements in my first activity report

on Freedom of Information of 2018.

2. Freedom of information for Hessian municipalities and

ministries

Freedom of information in Hessian municipalities and ministries

Freedom of information is developing well in Hesse. This is shown, for example

at the municipal level, but the same also applies to the ministerial level

Area.

municipal level

In the case of complaints received here that were directed against municipalities,

was positively noticed that - unlike in the first months after the start of validity

of the Hessian Freedom of Information Act, i.e. the fourth part of the

HDSIG (sections 80 et seq. of which regulate freedom of information) – the municipalities,

for the lack of a corresponding resolution in the articles of incorporation

freedom of action does not apply, the rejection of the request for information correctly

substantiate the reference to Section 81 Paragraph 1 No. 7 HDSIG instead of, as is often the case, at the beginning

of the Hessian freedom of information in May 2018 not at all on the

to respond to requests for information.

§ 81 HDSIG

(1) In accordance with Article 2, Paragraphs 1 to 3, the provisions on the access to information

also go for…

7. the authorities and other public bodies of the communities and districts as well

their associations regardless of their legal form, as far as the application of the fourth

Partly expressly determined by the articles of association.

The city of Kassel and the rural districts of Darmstadt-Die-

burg and Groß-Gerau the validity of the Freedom of Information Act

decided. There are probably even more municipalities without that

this is known to me. For the relevant municipalities there is a case

of a statute resolution introducing freedom of information no this

relevant reporting obligation to the Ministry of the Interior or my authority. In

usually, the introduction is known via media or may particular

be researched on the internet.

Darmstadt case – scope of the statutory reservation

The statutory municipal statute reservation for the validity

of the freedom of information (§ 81 Abs. 1 Nr. 7 HDSIG) supports the

municipal self-government guarantee, but the reservation applies

not only on self-government tasks of the municipalities, but also on

Instruction tasks and order matters.

A citizen requested information from the city of Darmstadt about the number of

Traffic offenses reported by private individuals and about the

Number of violations punished as a result for the years 2017 and 2018. The

The City of Darmstadt rejected the application, citing as justification that

that they do not affect the applicability of the Hessian freedom of information law

determinative statutes within the meaning of Section 81 (1) No. 7 HDSIG

and therefore no access to information was given.

The person concerned then turned to me and submitted that the

reserves within the meaning of Section 81 (1) No. 7 HDSIG only refers to municipal

nal self-government tasks, but it does not affect the constellation as

here, namely if the mayor does not have a municipal self-government

performance task, but in the context of traffic monitoring

instead, tasks to fulfill instructions/order matters

have to do.

Legal Assessment

It is true that the Hessian municipal law between self-

administrative tasks and those to fulfill according to instructions and instructions

carrying matters differs. The legal influence

of the state to the municipalities are in the case of self-government to the

Legal supervision is limited, while in the case of instructions and orders

technical supervision possibilities exist, viz

in the form of general instructions and instructions for individual cases (§§ 4,

135 Hessian Municipal Code (HGO)).

For the freedom of information issue of access to official companies

In Hesse, however, it is irrelevant which municipal branch of responsibility

is affected. Because the wording of § 81 Para. 1 No. 7 HDSIG refers

clearly to municipal bodies as such and precisely not differentiated

according to which task division it is.

It is not only the wording of the regulation that does not see any task-related differences

cation, but also the justification of the draft law does not give any

Reason to take part in the position-related regulatory character of § 81 Para. 1 No.

7 HDSIG (cf. Landtagdrucks. 19/5728 p. 150 to § 81).

Therefore, the mayor and mayor are also subject to the

Regulation of § 81 Para. 1 No. 7 HDSIG if - for example within the framework of the

local traffic surveillance - tasks of the local regulatory authorities

Freedom of information in Hessian municipalities and ministries

and district regulatory authorities as a matter of commission (§ 4

Paragraph 2 sentence. 1 HGO).

Something else only applies if originally municipal organs

lich exceptionally assigned to the state administration, in this

context then not act as a municipal body and to that extent also

no longer subject to Section 81 Paragraph 1 No. 7 HDSIG relating to municipal authorities

fall under. An example can be found in the area of municipal supervision, if

the district administrator belonging to the municipal level specifically in his function

as a municipal supervisory authority over the municipalities here as a country

of the authority is legally qualified (§ 136 Para. 3 HGO).

§ 136 HGO

...

(3) The supervisory authority for the other municipalities is the district administrator as the authority of the state

administration.

This organizational legal assignment of the municipal administrative

organs district administrator for state administration in the context of municipal supervision

but is not made by law, insofar as it is in the area of

Traffic surveillance to prevent regulatory activities on the ground

position of the Hessian law on public safety and order

goes (HSOG) goes. This follows from Section 85 HSOG, to which the

had informed complaining citizens about the refusal to provide information.

§ 85 HSOG

(1) General regulatory authorities are...

3. the district administrators in the districts and the mayors in urban districts as

District regulatory authorities…

I have therefore informed the complainant that his

view, in matters of instructions and orders is the reservation of the articles of incorporation

of § 81 Para. 1 No. 7 HDSIG not affected because the regulatory administration

(HSOG) is not a self-governing task is incorrect. Because even

in this context, the scope of § 81 Section 1 No. 7

HDSIG given, insofar as originally municipal authorities are not exceptional

assigned by law to the state administration.

309

The Hessian Commissioner for Data Protection and Freedom of Information

2. Activity Report on Freedom of Information

ministerial level

As far as the ministerial level is concerned, I am not aware of any case where

Because of my advice, access to information was unlawfully granted.

Core area of will and decision-making

I supported the decision of the Hessian Ministry of the Interior

in 2018, the legislative process regarding the introduction

Preparatory/accompanying evaluation reports on freedom of information

Freedom of information in the federal and state governments initially depends on access to information

to exclude The Ministry of the Interior justified this by saying that the

publication of the expert report the core area of will and decision-making

formation of the state government (§ 84 Para. 2 No. 1 HDSIG).

§ 84 HDSIG

(2) The request for access to information is to be rejected,

1. if the disclosure of the information is the core area of the will and decision

Education of the state government concerns...

For a certain period of time, this had the denial of the access to information

initially justified, but which has now expired. Since 2019, therefore

the Hessian Ministry of the Interior information access in the matter

granted, which is also necessary because expert opinions are fundamentally

Access to information is open (§ 84 Para. 1HDSIG).

Section 84 (1) HDSIG

(1) The request for access to information can be rejected for draft decisions

ments as well as for work and resolutions for their immediate preparation, to the extent and

as long as by the early disclosure of the information the success of the decision

or pending official measures would be thwarted. Not the immediate

The preparation of the decision according to sentence 1 is regularly used for the results of the gathering of evidence

and opinions or opinions of third parties.

deadlines

Regarding the ministerial level, however, it should be criticized that the

the deadlines applicable to the processing of information requests are not always

are complied with and the intermediate

message often missing.

§ 87 HDSIG

(1) The body responsible for providing information shall immediately, at the latest within one month,

the cases of § 86 at the latest within three months after receipt of the sufficient

to decide on a specific application. In the cases of § 86, the decision is also dem

to disclose to third parties.

(...)

(4) Can the information not or not completely within the in paragraph 1 sentence 1

specified deadlines are made accessible or require scope or complexity

an intensive examination, the body responsible for information can extend the period by one month

extend. The applicant is informed about the extension of the deadline, stating the

relevant reasons in writing.

Of course, on the other hand, it is not positively noticed that applicants

even if their applications show third-party concern and/or where

the question might arise whether they might be due to disproportionate

Administrative expenses within the meaning of Section 85 (2) can be rejected,

sometimes already lodge a complaint with me if a month plus a

previous day has passed without access to information.

Type of Access Granted

The way in which access is granted is not precise in §§ 80 et seq. HDSIG

regulated.

One complainant complained that the Ministry responsible for information

him the information on a document only through on-site inspection

wanted to grant, instead of sending him a copy to his place of residence in Berlin

send what he asked for. Then I got the ministry

asked about the complainant's journey from Berlin to

To spare Wiesbaden, and the ministry then has this concern

also corresponded.

In general, it is up to the decision of the body responsible for information

determine how access to information is granted. §§ 80,

87 do not contain any further definition in this respect, and from the cost regulation

of § 88 it only follows that there are different types of information

currency there.

§ 88 HDSIG

(1) The provision of verbal and simple written information as well as inspection

in files and files on site are free of charge according to the fourth part of this law...

In another case, the ministry responsible for information referred the

complainant that the information requested by the ministry was yes

also available in a certain municipality and therefore should/can

he can also get the information there. I have the ministry on it

pointed out that such a procedure is not permissible, but the

Information is required from the body that has the requested information.

This is already clear from the information request

Regulation § 85 HDSIG.

§ 85 HDSIG

(1) Access to information will be granted upon application to the body that has the requested information

regulations (body subject to the obligation to provide information), granted.

Conversely, to be separated from this is the aspect that in the case of exclusion

of access to information to certain bodies of this exclusion

cannot be frustrated by the fact that information from these bodies is still available

are also available from other bodies, Section 81 (3) HDSIG.

§ 81 HDSIG

(3) Insofar as access to information is excluded according to paragraph 1 or 2, this also applies to

File and file components that are in files or files of other authorities.

312

Administrative offenses Frankfurt Airport

3. Administrative offenses at Frankfurt Airport (delayed

landings)

Administrative offenses Frankfurt Airport

In relation to authorities that are responsible for fines, there is in this respect

no right to access information.

A citizen requested access from the Darmstadt Regional Council regarding

fend documents of completed administrative offense proceedings

delayed landings at Frankfurt Airport. The responsible government

Presidium Darmstadt rejected this because the HDSIG was

offenses law (OWiG) and is therefore not applicable

may be. This led to a complaint to my authority.

Evaluation

The Darmstadt Regional Council is to be agreed insofar as that

Hessian freedom of information law is then not applicable, insofar as Aus-

future claims are regulated by special law. This subordination of

Hessian freedom of information law (the fourth part of the HDSIG, viz

the §§ 80 ff.) against special information claims is also in the HDSIG

expressly standardized, Section 80 (2) HDSIG.

§ 80 HDSIG

(2) Insofar as special legal provisions regulate the provision of information, they go to the

provisions of Part Four.

However, the Administrative Offenses Act does not contain any provisions on the

Information regarding completed procedures. In addition, the HDSIG

with a view to two provisions, it is clear that regulatory

adversarial proceedings as a subject matter of the regulation. On the one hand, this should be done

the right of access to information cannot be effected by the expiration of

administrative offense proceedings are impaired. Below the description

"Protection of special public interests" is u. a. the administrative offense

data protection against specific disadvantages of access to information,

§ 82 No. 2. d) HDSIG.

313

The Hessian Commissioner for Data Protection and Freedom of Information

2. Activity Report on Freedom of Information

§ 82 HDSIG

There is no access to information...

2. for information, the disclosure of which could have adverse effects on ...

d) the success of ... administrative offense or disciplinary proceedings ...

In the case of completed administrative offense proceedings, this success can

but no longer affected.

In addition to this factual regulation, there are other, namely

regulations that these bodies are responsible for implementing

of administrative offense proceedings and are therefore responsible for fines,

exempt from access to information, namely § 81 Para. 1 No. 4 HDSIG

Reference to Section 40 (2) i. V. m.

Section 40 (1) HDSIG. And this exclusion also applies to authorities

which are not police authorities per se, but function as administrative offense

authority to become active (cf. on administrative offense proceedings also

Justification of the draft law, Drucks. 19/5728, p. 136 to § 40).

§ 81 HDSIG

(1) In accordance with Article 2, Paragraphs 1 to 3, the provisions on the access to information

go for too

...

4. the courts, criminal prosecution and enforcement authorities and others in Section 40

Section 2 and disciplinary authorities, but only insofar as they are public

perform lich-legal administrative tasks, and not insofar as they are within the framework

act in their judicial activity.

§ 40 HDSIG

(1) The provisions of this part apply to the processing of personal data by

for the prevention, investigation, detection, prosecution or punishment of criminal offences

or administrative offenses ... competent authorities.

(2) Paragraph 1 also applies to those public bodies responsible for the enforcement

are responsible for the enforcement and enforcement of penalties ... and fines.

I have therefore informed the inquiring citizen that he

about the Darmstadt Regional Council with regard to procedures

the imposition of fines does not entitle you to access information

owns, so here files on completed administrative offense proceedings

due to delayed landings at Frankfurt Airport.

314

The Law on the Protection of Trade Secrets

4. The Law on the Protection of Trade Secrets

The Law on the Protection of Trade Secrets

The law on the protection of trade secrets allows the information

freedom untouched. However, it defines the term "trade secret"

which is also important for access to information.

At the federal level is the Trade Secrets Protection Act

(GeschGehG) came into force on April 18, 2019. It also contains regulations

relating to freedom of information:

On the one hand, the stipulation made in Section 1 (3) No. 2. GeschGehG is important.

tion to the scope of the law, according to which freedom of information

remains untouched.

§ 1 GeschGehG

...

(3) The following remain unaffected: ...

2. Exercising the right to freedom of expression and information

according to the Charter of Fundamental Rights of the European Union (OJ C 202 of 07/06/2016,

p. 389), including respect for freedom and pluralism of the media, …

In addition to this provision, the regulations in § 4 GeschGehG,

of the prohibition to act, and the exceptions standardized in § 5 GeschGehG

men of the prohibitions on action of importance. This clarifies that

legitimate requests for freedom of information are not covered by the prohibitions on action

of § 4 GeschGehG are recorded.

§ 5 GeschGehG

Obtaining, using or disclosing a trade secret does not fall

under the prohibitions of § 4 if this is done to protect a legitimate interest,

in particular

1.

to exercise the right to freedom of expression and information,

including respect for media freedom and pluralism…

The law on the protection of trade secrets is now decisive,

as far as the freedom of information right to the legal concept of business

mystery. So it is regulated in § 82 No. 4 HDSIG that a claim

access to information does not exist for the personal area of life

related secrets or trade or business secrets,

unless the data subject has consented.

315

The Hessian Commissioner for Data Protection and Freedom of Information

2. Activity Report on Freedom of Information

§ 82 HDSIG

There is no right to access information...

4. in the case of secrets belonging to the personal sphere of life or business or

Trade secrets, unless the data subject has consented.

What is to be considered a trade secret (the term trade secret is

merged into the concept of trade secrets), now regulates § 2 GeschGehG.

§ 2 GeschGehG

For the purposes of this law

1. trade secret a piece of information

a) neither in total nor in the exact arrangement and composition of their

components of the people in the circles who are usually familiar with this type of information

bypass information, is generally known or readily accessible and therefore

is of economic value and

b) the subject of the circumstances after reasonable confidentiality measures

by its rightful owner and

c) who have a legitimate interest in confidentiality ...

It is obvious that regulation c) in particular will lead to debates

can; in the previous entries according to the Freedom of Information Act

for me, however, the topic of trade secrets has not yet been addressed

played a bigger role.

316

ANNEX II

Freedom of Information Materials

Appendix II – Freedom of Information Materials

Appendix II – Freedom of Information Materials

1. Resolution of the 37th Conference of

Freedom of Information Officer in Germany

on June 12, 2019 in Saarbrucken

Transparency in political decision-making processes –

Introduce mandatory lobby register

Parliamentary democracy thrives on the open and therefore public

chen discussion of different, often different interests, which in the

framework of legislation by Members of Parliament against each other

have to be weighed. Given the complexity of the social and

economic reality and the regulatory matters, it can

tical decision-making process can often be helpful, relying on the expertise of

different people, groups and stakeholders from society

and economy to fall back on. The way of such

However, exerting influence must be transparent. The citizens

should know who is involved in the formulation during the development process

involved in a bill and who, on whose behalf and with whom

attempts to influence political decisions by means of means. entanglements

in particular between politics and business, it must be made clear

thus making hidden influence more difficult and public control

is made possible.

For this reason, some states already have regulations on the management of

lobby registers. From the point of view of the freedom of information officers in Germany

it is required for a democratic community, mandatory register

to introduce, into the information about advocacy groups and their

activities are to be entered. It contains at least the names of the natural

chen and legal entities, stating their organizational form, the

Focus of the content or professional activity and at least the

essential contents of the contribution to the respective legislative procedure

publish. The resulting transparency strengthens the trust of the

People in politics, enables democratic control and increases the

Acceptance of political – especially legislative – decisions.

The Conference of Freedom of Information Officers calls on the Federal

and the state legislators therefore to do so, for example based on that

Thuringian Stakeholder Transparency Documentation Act of February 7th

2019 legal framework to introduce a mandatory

to adopt the lobby register.

2. Position Paper of the 37th Conference of

Freedom of Information Officer in Germany (IFK)

on June 12, 2019 in Saarbrucken

Facilitate access to information in the authorities

"Freedom of Information by Design"

The digital transformation is one of the major challenges facing the

public administration stands today. Currently, e-government

Laws and the regulations in the Online Access Act are implemented.

At the same time, there is an increased interest in the transparency of the administrative

actions that are increasingly being taken up by legislators. The

public administration is obliged to respect the right to access information

implement freedom. Confidence in the fulfillment of government tasks

strengthened by processing requests for information quickly and efficiently.

Against this background, the Conference of the Freedom of Information

commissioned in Germany (IFK) the public authorities of the federal government and the

Countries that have freedom of information requirements from the start

flow into the design of their IT systems and organizational processes

to allow: "Freedom of information by design". The legislators are

call to create the legal basis and necessary resources

to provide.

definition

"Freedom of information by design" includes the entirety of technical and

organizational instruments, taking into account the state of the art,

the perception and fulfillment of the rights under the information

health and information access laws, environmental information laws and

serve federal and state transparency laws. With that supported

"Freedom of information by design" on the one hand with bodies subject to information requirements

the fulfillment of a requested information access as well as in the implementation

of publication obligations, on the other hand, for applicants

easier access to information.

general conditions

For the processing of personal data, the EU

European legislators the principle of data protection through technology

technical design – i.e. “data protection by design” – standardized. In the area

of freedom of information are also regulations, from which for

Bodies subject to information technical and organizational obligations

result. Depending on the content of the regulation, this includes the state and

federal regulations, for example

– proactive disclosure requirements,

- working towards the storage of information in electronic

databases,

- the designation of contact persons or other information-

term positions,

– the provision of registers of available information,

– the establishment of publicly accessible information networks and

-portals,

– the consideration of labeling of information by third parties

as “vulnerable” and

- the enabling of limited access to information with only partial

wise conflicting public or private interests.

Furthermore, the observance of the principles of proper filing

management serve to limit the time required for provision

and reduce the cost of accessing information.

Measures

"Freedom of information by design" measures can be taken when fulfilling these

provide assistance with technical and organizational obligations.

So should the findability of information in the information subject

places e.g. B. through efficient filing systems and electronic search functions

be guaranteed. In filing systems, when new information is recorded,

information, sensitive sections or parts of files are marked,

which facilitates a separate check for confidential parts.

Information should be categorized in the filing systems whenever possible

be what in certain administrative areas such as through the leadership of

Part files is conceivable that are part of a main file. Publishable

Information should be proactively provided by the information authority, such as via

an information portal to be made available to the general public.

With the “Freedom of Information by Design” approach, standardized solutions can

Solutions for recurring issues are developed, whereby the

Effort on the administration side is reduced. This system design is incumbent

not only those responsible for public administration, but also

the developers of software solutions for public

Administrations facing freedom of information requirements from the start

should be included in the concepts and implementations.

subject index

I 5.3

I 11.2, I 12.1

I 11.2

I 12.1

II 2

4.3

I 14.1

323

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection / 2nd activity report on freedom of information

survey

– design

– citizen survey

– Midwife survey

- anonymous

medical malpractice

User identification

user interface

employee data

removal order

operating system

motion profiles

application documents

Binding Corporate Rules (BCR)

Blockchain

Letter box

Brute force attack

fine

- Procedure

– Employee excess

– net income

- Concept

– health data

chat

– Applications

- Group

– partners

cloud

data transfer

324

5.4

5.4

5.4

5.4

I 9.1

4.3

I 13.4

I 4.4, Appendix I 1.1

I 10.1

I 14.1

Appendix I 1.8

I 4.4, I 9.6

subject index

– internal

– operational

- An order

– conflict of interest

– duty of naming

– Risk of sanctions

Data Protection Impact Assessment

data protection management

level of privacy

data economy/

data minimization

data storage

– Duration of storage

– storage period

– credit bureaus

service provider

service provider

digital platform

direct survey

third country

I 9.2, I 15.1, I 7.2, I 4.4

I 11.2

I 15.3

I 16.2, I 16.3, I 16.4

I 5.1

I 5.3

I 7.5

I 11.1

I 4.1

I 15.1

I 4.1, I 15.1

I 15.1

Appendix I 1.3

Appendix I 1.3

I 17.2

I 14.2

I 3.1

I 8.1, I 9.5, I 14.2, Appendix I 2.4

I 7.5

I 12.1

I 12.1

I 12.2

I 8.2, I 11.2, I 13.4, I 14.2,

Appendix I 1.7

I 13.1, I 13.2

I 7.3

I 6.3

I 3.1

I 2.2

consent

- Survey

- voluntarily

– video surveillance

– data transmission

- Children

- Advertising

– Chat functionality

– health data

– customer data

– research project

e-mail

- Account

– communication

– Acknowledgment of receipt

– addresses

– encrypted

disposal

– of documents

– of glass waste

– of application documents

– video surveillance

Survey, register-based

discretionary decision

fan page

remote inspection

wireless smoke detector

research project

security

326

I 5.4,

I 8.1

I 10.1

I 12.1

I 13.1

I 13.2

I 13.3

Appendix I 1.7

Appendix I 2.3

Appendix I 2.5

4.3

I 4.3, I 8.3

I 8.3

I 11.2

I 11.5

I 7.2

I 9.2

I 9.6

I 10.2

I 7.6

I 6.3

Appendix I 2.6

I 8.2

I 8.2

Appendix I 2.5

Appendix I 1.8

subject index

fine

– metering

– determination

– harmonization

trade secrets

reference file

Hessenbox

whistleblower

home page

principle of homogeneity

hyperlink

I 15.1

I 15.2

I 15.2

II 4

I 11.4

I 17.1

I 6.3

I 8.3

I 7.1

– informational

self-determination

health insurance

crime fighting

crime focus

cryptocurrency

Teacher Education Act

learning aids, digital

lobby register

deletion

I 6.1, I 13.1

I 13.2

I 8.3

I 6.1

I 11.2, Appendix I 2.3

Introduction, I 1, I 13.1

Appendix I 1.2

Appendix I 1.5

I 9.1

I 6.2

I 10.2

I 14.5

I 7.1

I 7.3

Appendix II 1.1

I 11.4, I 11.2, I 14.2

- Link

administrative offences

- Procedure

– Freedom of information right

patient records

patient data

patient record

password

identity card copy

number of people

ID number

identity check

I 3.1

I 3.2

I 7.5, Appendix I 1.4

I 11.3

I 13.2

I 13.3

I 13.3

I 16.3

II 3

I 9.1, I 9.3, I 9.4

I 9.2, I 15.3, Appendix I 1.6

I 9.3,

I 4.3, I 11.3

I 8.1

I 4.1

Appendix I 1.4

I 6.2

329

The Hessian Commissioner for Data Protection and Freedom of Information

48th activity report on data protection / 2nd activity report on freedom of information

association of persons

phishing

POLAS

police department

press term

Privacy Shield

profile management

Qualified Electronic

signature

accountability

rehab process

re-identification

– re-identification factor

– re-identification

risk

- Judgement

– points of view

broadcasting fee

I 11.1

I 4.3, I 11.2

I 6.2

I 6.2, II 3

I 5.1

I 3.1

I 11.3

4.2

4.3

I 6.4

I 5.3

I 5.3

4.3

4.3

I 11.3

Appendix I 2.4

Key Authorization

written form

written form requirement

student transportation

school portal

protection level

scoring

self-government, municipal

I 7.2

4.2

4.2

I 7.5

Appendix I 2.1

Appendix I 2.2

I 13.2, Appendix I 1.7

I 10.2, I 13.1, I 13.2, I 14.4,

Appendix I 1.2, Appendix I 1.4,

Annex II 1.1, Annex II 2.1

I 8.3, I 17.1

I 5.3

I 15.2, Appendix I 1.1

vandalism prevention

responsibility, common

behaviour rules

– voluntary

processing,

cross border

Directory of

processing activities

Infringement notification in accordance with

Art. 33 GDPR

video surveillance

– in business premises

- Garbage

– Forest parking lot

– residential complex

– private

- Gastronomy

– swimming pools

water damage

Web

- Access

- Page

– Analysis

– -based IT system

– Servers

– health pages

2021 census

Access Permission

access

- -protection

– -code

– grant

332

I 10.3

Appendix I 2.6

I 12.2

I 3.2, I 11.2

I 4.2, I 14.4

I 4.3,

I 10.1

I 10.2

I 10.2

I 10.2

I 10.3

I 10.4

I 10.5

I 9.3

4.3

I 13.2

I 13.2

I 14.1

I 14.1

Appendix I 1.7

I 7.6

I 5.3, I 11.3

I 9.4

I 14.1

II 2

subject index

cooperation of

regulators

earmarking

- private purposes

Two-factor authentication

72 hour period

I 3.2

I 14.2, I 15.1

I 15.1

I 11.2

I 4.3, I 15.3

333