Forty-seventh activity report

to data protection

and

First Freedom of Information Report

of

Hessian Commissioner for Data Protection

and freedom of information

professor dr Michael Ronellenfitsch

submitted as of December 31, 2018 pursuant to

§ 30 of the Hessian Data Protection Act (until May 24, 2018) and

Art. 59 of Regulation (EU) No. 2016/679 (from May 25, 2018) 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

47th activity report on data protection / 1st 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: www.datenschutz.hessen.de

(06 11) 14 08-0

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

poststelle@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

List of Abbreviations

List of Abbreviations

List of Abbreviations

a. a. O.

a. f

fig

Section.

Inc

AK technique

kind

ATDG

at the specified location

old version

Illustration

Unit volume

public company

Technology working group

Article

Law establishing a standardized

central anti-terror database of police authorities

and federal and state intelligence services

(Anti-Terrorism File Act)

BDSG

BDSG a. f

Civil Code

Federal Law Gazette

FCAG

BRPrints.

BTprints.

BVerfSchG

or.

approx.

ccTLD

CNIL

i.e. H.

DAkkS

DIN

DNS

DPIA

GDPR

DSK

Federal Data Protection Act

Federal Data Protection Act old version

Civil Code

Federal Law Gazette

Law on the Federal Criminal Police Office and the

Cooperation between the federal and state governments

in criminal matters

(Federal Criminal Police Office Act)

Federal Council printed matter

Bundestag printed matter

Federal Constitutional Protection Act

respectively

about

country code top-level domain

Commission Nationale de l'Informatique et des Libertés

That means

German Accreditation Body

German industry standard(s)

domain name system

Data Protection Impact Assessment

General Data Protection Regulation

Conference of Independent Data Protection Authorities

Federal and the states

XI

The Hessian Commissioner for Data Protection and Freedom of Information

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

registered association

European Data Protection Board

European Data Protection Supervisor

(European Data Protection Supervisor)

European Data Protection Board

European standard

recital

et cetera

European Union

Court of Justice of the European Union

constitution

in which case

Joint Control Authority

basically

Jurisdiction Act

Hessian representative for data protection and

Freedom of Information

Hessian data protection officer

Hessian Data Protection Act

Hessian Data Protection and Freedom of Information Act

Hessian Ministry of the Interior and Sport

Hessian law on public safety and

Order

Hessian Constitutional Protection Act

usually

in terms of

with the meaning of

combined with

Internet Corporation for Assigned Names and Numbers

International Electrotechnical Commission

in particular

Insolvency Code

International Organization for Standardization

(International Standardization Organization)

information technology

hospital information system

small and medium-sized companies

e. V

EDPB

EDPS

EDSA

EN

recital

Etc.

EU

ECJ

GG

possibly.

GKI

basically

GVG

HDBI

HDSB

HDSG

HDSIG

HMDIS

HSOG

HVSG

i. i.e. R

i. s.d.

i. S.v.

i. V. m.

ICANN

IEC

esp.

InsO

ISO

IT

CIS

SMEs

XII

List of Abbreviations

LfV

lit.

LKA

LKG Berlin

LKHG M-V

LTDprints.

State Office for the Protection of the Constitution

littera

State Criminal Police Office

Berlin State Hospital Act

Hospital law for the state of Mecklenburg-

Western Pomerania

State Parliament printed matter

m.e.

above

OH KIS

OWiG

PKK

in my opinion

above/named/named/named

Orientation guide for hospital information systems

Administrative Offenses Act

Parliamentary Control Commission

Source TKÜ online telecommunications surveillance

item no.

RED-G

S

s.

SDM

SGB

so-called.

StNumber

StPO

TOM

marginal number

Law establishing a standardized central

File from police authorities and intelligence services from

Federal and state governments to combat violence-related

Right-wing extremism (right-wing extremism file law)

page or sentence

please refer

Standard Privacy Model

social code

so-called/so-called/so-called

Official State Publisher for the Federal State of Hessen

Code of Criminal Procedure

Technical organizational measure

etc.

u. u.

UAG DPFA

UNITED STATES)

etc.

see.

among other things

in certain circumstances

Sub-working group on data protection impact assessment

United States of America

and so forth

compare

XIII

The Hessian Commissioner for Data Protection and Freedom of Information

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

very important person

Police and Police Access Act

law enforcement agencies and intelligence services

Visa Information System (VIS Access Act)

Virtual Private Network

working paper

for example

digit

Code of Civil Procedure

V.I.P

VISZG

VPN

WP

e.g. B.

item

ZPO

XIV

Register of Legislation

Register of Legislation*

Register of Legislation

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

law/regulation

site(s)

TFEU

ATDG

BDSG-old

BDSG-new

Civil Code

FCAG

BO

BRAOO

BVerfGG

BVerfSchG

Treaty on the Functioning of the European Union

26.10.2012 (OJ EU C 326/47)

Law establishing a standardized central

Anti-terror database of police authorities and intelligence services

The federal and state governments (anti-terrorist database law) i. i.e. F. from 22.12.2006

(Federal Law Gazette I p. 3409), last amended by law from 08/14/2017

(BGBl. I p. 3202)

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)

Federal Data Protection Act 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,

corrected p. 2909, 2003 p. 738), amended by Law of

December 18, 2018 (BGBl. I p. 2639)

Law on the Federal Criminal Police Office and the cooperation of the

federal and state in criminal matters

(Federal Criminal Police Office Act) i. i.e. F. from 01.06.2017 (Federal Law Gazette I p. 1345)

Professional regulations for doctors in Hesse from

September 2, 1998 (HÄBL 10/1998 p. I–VIII),), last changed on

November 27, 2018 (HÄBL 2/2019 p. 137)

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

Outline number 303-8, published revised version,

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

Law on the Federal Constitutional Court i. i.e. F. dated 08/11/1993

(Federal Law Gazette I p. 1473), last amended by law on October 8th, 2017

(BGBl. I p. 3546)

Law on cooperation between the federal and state governments

countries in matters of constitutional protection

and via the Federal Office for the Protection of the Constitution

(Federal Constitutional Protection Act) i. i.e. F. from 20.12.1990 (Federal Law Gazette I

p. 2954, 2970), last amended by the law of 06/30/2017

(BGBl. I p. 2097)

XV

The Hessian Commissioner for Data Protection and Freedom of Information

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

Charter of Fundamental Rights of the European Union from October 26, 2012

(OJ EU C 326 p. 391)

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)

Electronic Administration Promotion Act

(E-Government Act) i. i.e. F. from 25.07.2013 (Federal Law Gazette I p. 2749),

last amended by law from 05.07.2017 (Federal Law Gazette I p. 2206)

Judicial Constitution Act i. i.e. F. of 09.05.1975 (Federal Law Gazette I

p. 1077), last amended by law dated July 12, 2018 (Federal Law Gazette I

p. 1151)

Law Against Restraints of Competition i. i.e. F. from

06/26/2013 (Federal Law Gazette I p. 1750, 3245), last amended by law

from 12.07.2018 (Federal Law Gazette I p. 1151)

Hessian Data Protection Act i. i.e. F. from 07.01.1999 (GVBl. I

p. 98), repealed on 25.05.2018 by law dated

03.05.2018 (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

Hessian law to promote electronic administration

(Hessian e-government law) i. i.e. F. from 12.09.2018 (GVBl.

p. 570)

Law on professional representation, the exercise of the profession, the

Continuing education and the professional jurisdiction of doctors, dentists,

Veterinarians, pharmacists, psychological psychotherapists

and child and adolescent psychotherapists i. i.e. F. from

07.02.2003 (GVBl. I p. 66, 242), last amended by law

from 03.05.2018 (GVBl. p. 82)

Second law for the further development of the hospital system

in Hesse (Hessian Hospital Act 2011) i. i.e. F. from

December 21, 2010 (GVBl. I p. 587), last amended by law from

09/13/2018 (GVBl. p. 599)

Hessian school law i. i.e. F. from 30.06.2017 (GVBl. p. 150),

last changed by law from 03.05.2018 (GVBl. p. 82).

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)

GRCh

GDPR

EGovG

GVG

GWB

HDSG

HDSIG

HEGovG

Healthcare Professions Act

HKHG 2011

HSchG

HSOG

XVI

HVSG

HVwVfG

IHKG

InsO

JI Policy

Art Copyright Act (KUG)

LKG Berlin

LKHG M-V

OWiG

OZG

Register of Legislation

Hessian Constitutional Protection Act i. i.e. F. from 25.06.2018

(GVBl. p. 302)

Hessian Administrative Procedures Act i. i.e. F. from 01/15/2010

(GVBl. I p. 18), last amended by law from September 12th, 2018

(GVBl. p. 570)

Act for the Provisional Regulation of the Law of

Chambers of Industry and Commerce in the Federal Law Gazette Part III,

Outline number 701-1, published revised version,

last amended by law from 03/29/2017 (Federal Law Gazette I p. 626)

Insolvency Code of October 5th, 1994 (Federal Law Gazette I p. 2866), last

changed by law from 23.06.2017 (Federal Law Gazette I p. 1693)

Directive (EU) 2016/680 of the European Parliament and of

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

Processing of personal data by the competent

Authorities for the purpose of prevention, investigation, detection

or prosecution of criminal offenses or the execution of sentences

as well as for the free data traffic and the repeal of the

Council Framework Decision 2008/977/JHA (OJ EU L 119 p. 89)

Law on copyright in works of fine arts

arts and photography in the Federal Law Gazette Part III,

Outline number 440-3, published revised version,

last changed by law from 16.02.2001 (Federal Law Gazette I p. 266,

280)

State Hospitals Act of September 18, 2011 (GVBl. p. 483), last

changed by law from 02.02.2018 (GVBl. p. 160)

Hospital law for the state of Mecklenburg-Western Pomerania

May 20, 2011 (GVOBl. M-V 2011, p. 327), last changed by

Law of 05/16/2018 (GVOBl.

M-V p. 183, 185)

Law on Administrative Offenses i. i.e. F. dated 02/19/1987

(BGBl. I p. 602); last amended by law from 17.12.2018

(BGBl. I p. 2571)

Online Access Improvement Act

Administrative services (Online Access Act) i. i.e. F. from

14.08.2017 (Federal Law Gazette I p. 3122, 3138), came into force on

08/18/2017

Law establishing a standardized central file of

Federal and state police and intelligence services

to combat violent right-wing extremism

(Right-Wing Extremism File Act) i. i.e. F. from 20.08.2012 (Federal Law Gazette I

p. 1798), last amended by law dated August 14, 2017 (Federal Law Gazette I

p. 3202)

Social Code, Book One - General Part - i. i.e. F. from

December 11, 1975 (Federal Law Gazette I p. 3015), last amended by law dated

08/17/2017 (Federal Law Gazette I p. 3214)

Social Code Book Tenth Book - Social Administrative Procedures and

Social data protection – i. i.e. F. from 18.01.2001 (Federal Law Gazette I p. 130), last

changed by law of December 18, 2018 (GVBl. I p. 2639

penal code i. i.e. F. from 13.11.1998 (Federal Law Gazette I p. 3322), last

amended by law of December 18, 2018 (Federal Law Gazette I p. 2639)

Code of Criminal Procedure i. i.e. F. from 07.04.1987 (Federal Law Gazette I p. 1074, 1319),

last amended by law from 18.12.2018 (Federal Law Gazette I p. 2639)

Law on Donation, Removal and Transfer of Organs

and tissues (transplant law) i. i.e. F. from 04.09.2007

(Federal Law Gazette I p. 2206), last amended by law from 07/18/2017

(BGBl. I p. 2757)

Police and Police Access Act

Law enforcement authorities and intelligence services on visa

Information system (VIS Access Act) i. i.e. F. from 06.05.2009,

last amended by law from 26.07.2016 (Federal Law Gazette I p. 1818)

RED-G

Social Code I

SGB X

StGB

StPO

TPG

VISZG

XVIII

core items

core items

core items

1.

The focus of this activity report is on the data

protection reform and the creation of a right to freedom of information. He

is therefore divided into a data protection report for the first time (divided for the

Time before or after the General Data Protection Regulation came into force) and one

Freedom of Information Act report.

2. Data protection law developed in the EU in the reporting year, the

Member States and Germany differ (first part, no. 2.1

to 2.3). In Hesse, the Hessian Da-

Data Protection and Freedom of Information Act created and numerous

Changes made to specialist legislation (Part One, Section 2.4).

3. The Hessian Constitution Protection Act and the Hessian Law

on public safety and order were in part comprehensive

amended (First Part, Section 2.5 and Section 2.6). By EU regulations,

Federal laws and state law are additional audit obligations for the

HBDI (Part One, Section 2.7). A draft law that

The Hessian Hospital Act contains a regulation for the closure of a hospital

hospital is to be inserted, was introduced to me (first part,

Clause 5.3).

4. With the introduction of the “BAföGdirect” app, accompanied by data protection law

and the preparatory work on interoperable service accounts for deployment

Administrative services offered online were further building blocks

"Digital Hessen 2020" strategy implemented (first part, no. 3.5.2 and

Section 3.5.3). The implementation of the "Digital Model Authority" project

with the sub-project "recognition bonus" is up under data protection law

a good way (first part, no. 4.3.1 and no. 4.3.2).

5. The project "School without Racism - School with Courage" must

be improved under data protection law (first part, point 4.4.3). The

Digitization project "School diary for children of professional travelers"

(Digital learning on the go - DigLu) is progressing (first part, point 5.1).

The Hessen-wide introduction of the learning process diagnostics software "quop"

I accompanied data protection law and with regard to the new

Advice on the requirements of the GDPR (first part, point 4.4.2).

6. Since the General Data Protection Regulation came into force, inputs have dominated

in the public and non-public area on the rights of those affected

to. Typical complaints for both areas and

Questions regarding the right to information (Part One, Section 4.3.4, Section 4.5.2

and Section 4.7.2), for reporting by internal data protection officers, for

Information for those affected (first part, section 4.6.1), for recording

Telephone conversations, photo and video recordings (first part, no. 4.1
and Section 4.3.6) and for the publication of employee photos (first
part, clause 4.9.1).

7. With the change in Microsoft's business model, for which Microsoft
Cloud Germany with the trustee model no new customer contracts
to close more, the use of the product Microsoft 365 or
Azure questioned in schools (Part One, Section 5.2).

8. The Europeanization of the fine procedure leads to a collision with
national procedural law (first part, point 4.11.1). First experience
with the fine procedures according to DS-GVO were made (first part,
Clause 4.11.2). First experience reports on reports of data breaches
are presented (first part, clause 4.11.3 and clause 4.11.4).
In the healthcare sector, dealing with patient files was always a problem
Theme. The refusal of patients to provide information
Signing the information flyer according to Art. 13 DS-GVO led to the inadmissible
Refusal of medical treatment (Part One, Section 4.6.2).

9.

10. The protection under data protection law when transferring data to the
some states, the Privacy Shield, was again put to the test
(First part, Section 4.2.1). For the Europe-wide cooperation of the HBDI
with other European supervisory authorities according to DS-GVO
first structures created (first part, number 4.2.2).

11. Interesting developments are in the area around the automotive
stuff to track. The admissibility of accident data under data protection
Data storage can only be recorded with corresponding information obligations

(First part, Section 4.5.1). A wide-ranging testing campaign by car repair shops

sites showed data protection deficiencies in the handling of vehicle data

(First part, Section 4.5.3).

12. In the first activity report on the Freedom of Information Act, I present the

constitutional principles and first experiences from the

practice (part two, nos. 1 to 3).

XX

First part

47th activity report on data protection

1

47th activity report on data protection

The Hessian Commissioner for Data Protection

2

introduction

1. Introduction

introduction

1.1

upheaval

This 47th activity report is the last activity report of the 19th election

period of the Hessian state parliament from 01/18/2014 to 01/17/2019. In this

period there was a fundamental transformation of the European (EU),

German and Hessian data protection law. On 05/25/2018, the day on

when the General Data Protection Regulation (GDPR) came into force

according to Selmayr/Ehmann a new era (DS-GVO commentary, 2nd ed.

2018, introduction para. 1). Even if you think that's an exaggeration, it is

noteworthy that on this day the GDPR and the EU directive for

Justice and Home Affairs (JHA Directive; JHA Directive) by a broader public

only and mostly skeptical.

The skepticism is mainly based on the fact that not only individual provisions

of the GDPR, but generally the requirements of data protection law

were misunderstood. The JL-RL remained largely unknown.

1.2

Consequences for reporting

As a result, the tasks of the data protection supervisory authorities are also reduced

including annual reporting. Until 05/24/2018

were the tasks of the Hessian data protection officer (HDSB) in

§ 24 HDSG 1999 regulated.

§ 24 HDSG 1999

(1) The Hessian data protection officer monitors compliance with the provisions of this

Law and other regulations on data protection at the data processing

Place. For this purpose, he can make recommendations to improve data protection

give; in particular, he can represent the state government and individual ministers as well as the rest

advise data processing bodies on questions of data protection. The courts are subject

the control of the Hessian data protection officer, insofar as they are not in judicial

act independently. The Hessian data protection officer controls the

Compliance with data protection regulations also at the bodies that are and to the extent that they are

according to § 4 para. 3 sentence 1 have been subject to his control.

(2) The Hessian data protection officer monitors the effects of the automated

data processing on the way of working and the decision-making powers of data processing

working places. In particular, he must ensure that they lead to a shift in

the separation of powers between the constitutional organs of the country, between the organs

of local self-government and between the state and the local government

conduct self-government. He should suggest measures that seem appropriate to him,

to prevent such effects.

...

From May 25th, 2018, the tasks of the Hessian supervisor

contributed to data protection and freedom of information from § 13 HDSIG.

§ 13 HDSIG

(1) The Hessian data protection officer monitors the public and not

public bodies and their processors the application of this law, the

Regulation (EU) No. 2016/679 and other regulations on data protection, including

according to the legislation adopted to implement Directive (EU) No. 2016/680.

(2) In addition to the tasks under Article 57 of Regulation (EU) No. 2016/679, the

Hessian data protection officer the tasks,

1. the application of this law and other regulations on data protection,

including the legislation adopted to implement Directive (EU) No. 2016/680

regulations, to monitor and enforce,

2. the public for the risks, regulations, guarantees and rights related

to sensitize and inform them about the processing of personal data

educate, with specific measures for children and young people special

get attention

3. the state parliament, the parliamentary groups represented in the state parliament, the state government, the committee

munen and other institutions and bodies on legislative and administrative

Measures related to the protection of the rights and freedoms of natural persons

advise on the processing of personal data,

4. the persons responsible and the processors responsible for them under this law and
other data protection regulations, including those for the implementation of the
Directive (EU) No. 2016/680, resulting obligations
to raise awareness when processing personal data,
5. at the request of each data subject, information on the exercise of their rights
due to this law and other regulations on data protection,
Finally, the legal
regulations, and, if necessary, for this purpose with the
cooperation between supervisory authorities in other Member States,
6. dealing with complaints from a data subject or complaints from a body, a
Organization or association according to Art. 55 of Directive (EU) No. 2016/680
to investigate the subject matter of the complaint to a reasonable extent
and the complainant within a reasonable time of progress
and to inform the result of the investigation, especially if a further
investigation or coordination with another supervisory authority is necessary,
7. to cooperate with other supervisory authorities, including through information
exchange, and to provide them with administrative assistance to ensure the uniform application and enforcement
tion of this law and other regulations on data protection, including
the legislation adopted to implement Directive (EU) No. 2016/680,
to ensure,

8. Investigations into the application of this law and other regulations on
data protection, including the implementation of Directive (EU) No. 2016/680
enacted legislation, also on the basis of information
functions of another supervisory authority or another authority,

9. to follow relevant developments insofar as they relate to the protection of personal

related data, in particular the development of information and

communication technology and

10. To provide advice in relation to the preliminary processing operations referred to in Section 64.

Within the scope of Directive (EU) No. 2016/680, the Hessian

Data protection officers also carry out the tasks under Section 52 (7) also in connection with

§ 51 para. 4, § 53 para. 7 and § 55 true.

(3) The Hessian data protection officer monitors the effects of the automatic

mated data processing on the way of working and the decision-making powers of the

public bodies, in particular whether these lead to a shift in the separation of powers

between the constitutional organs of the country, between the organs of the municipal

self-government or between state administration and local self-government

lead administration. She or he should suggest measures that appear appropriate, such

to prevent effects.

...

The existing awareness-raising and

clarification task is expressly designed as a legal obligation (§ 13 Para. 2

#2 HDSIG). Even under previous law, the HDSB had one per year

submit a written activity report. This resulted from § 30 HDSG.

§ 30 paragraph 1 HDSG 1999

On December 31 of each year, the Hessian data protection officer gave the state parliament and

a report to the state government on the result of its activities in accordance with Section 24 (1) to (3).

to submit. He also gives an overview of the technical and organizational aspects

Measures according to § 10 and suggests improvements in data protection. interim reports

are allowed. Simultaneously with the report according to sentence 1, the Hessian data protection

commissioned the state parliament to submit a report on its activities in accordance with Section 24 (4).

The reporting obligation of the HBDI is now regulated in § 15 HDSIG.

Section 15 (3) HDSIG

On December 31 of each year, the Hessian data protection officer

te the state parliament and the state government a report on the result of their or

of its activities and suggests improvements in data protection. the or

the Hessian data protection officer makes this report public, the EU

European Commission and the European Data Protection Board.

Interim reports for submission to the state parliament and the state government are permissible.

The addressees of the activity report have so far only been the state parliament and state

government. These continue to be the primary addressees of the reports. Reports

are now also the public, the European Commission

and "make available" to the European Data Protection Board.

Their explicit mention makes them secondary addressees who

not only to inform those who are not affected about legal relationships of third parties,

but are to be considered in terms of content and function. For the European

Data protection committee is the obvious. For fulfilling his duties

national reporting is indispensable due to the nature of the matter.

The European Commission can ensure the uniform implementation of the GDPR

Only monitor effectively if you have meaningful reports from the national

be submitted to supervisory authorities. The obligation of the HBDI, the

DS-GVO to bring the public closer also in the context of reporting

gen, ultimately results from the requirement of effective task fulfillment.

The functional expansion of the job area that occurred on May 25, 2018

court gives reason to review the legal situation before and after the validity of the GDPR
to be treated separately (items 3 and 4). In terms of content, the following is added: The
Task, in the activity report misunderstandings of data protection law
to counteract this was also possible without a simple statutory regulation
based on constitutional law, in particular on the rule of law
Special position of the independent state (data protection) supervisory
hear. The amended data protection law only contains specific statutory provisions
Specifications of this special position, so that the constitutional
Foundation remains a task of science and practice. Also the
Activity reports have to contribute to accomplishing this task. The
happens in the present activity report in such a way that the actual
Che report part of the activity report with general statements on
Understanding and interpretation of the GDPR is expanded. This matches with
the exercise started with the 35th activity report, the ones presented
specific supervisory activities, general preliminary remarks on the status of
data protection and data protection law. were treated
so far, for example, the function of data protection within the framework of the national
Constitutional order and Union law (35th activity report, p. 21 ff.;
36th activity report, p. 21 f.; 38th activity report, p. 21 ff.), the thrusts
of data protection and its relationship to freedom of information (37th activity
ness report, p. 23 f.), the conception of informational self-determination
(38th activity report, p. 21 f.; 45th activity report, p. 21 f.), the task
Position of the data protection officer according to national law and after
requirement of Union law (independence) (36th activity report, p. 20 ff.;
41. Activity report. p. 35 ff.; 43rd activity report, p. 23 ff.), the specific
Role of Hesse in the further development of data protection law (39th activity

performance report p. 23 ff.; 40th activity report, p. 29 ff.), the Europeanization of the Data protection law (41st activity report, p. 32 ff.; 43rd activity report, p. 27 ff.; 44th activity report, p. 21 ff.) and the international references of the data property rights (42nd activity report, p. 25 ff.; 43rd activity report, p. 23 ff.).

In the 46th activity report (p. 23 ff.), in anticipation of the expected Development of trading in personal data. The European data economy driven by the Commission (cf. Communication from the Commission to the European Parliament, the Council, European Economic and Social Committee and the Committee of gions "Building a common European data space" [SWD(2018) 125 final] of April 25, 2018 (BRdrucks. 156/18) and statement of European Economic and Social Committee on the "Communication from the Com-Mission to the EU Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building a European technical data economy" [COM(2017) 9 final] refers only to non-personal data and should not affect the GDPR (cf. the European Commission publication: Enter the data economy, EU policies for a thriving data ecosystem, Issue 21 / 01/11/2017). This limitation but in the age of ubiquitous computing and big data, it will be for a long time view is not possible and is also not desirable. The right must keep pace with technical developments (cf. already Ronellenfitsch, DVBl. 1989, 851 ff.). The reform of data protection law is therefore one permanent task. However, before embarking on further reform projects, should the DS-GVO be given the chance to use it in the overall complex of the

to develop the effectiveness due to data protection law. The scope of

The current upheaval will only become apparent when the norm is enforced. A legal

Correct implementation of the norm requires clarity about the scope of the regulation,

which is to be determined in a methodically comprehensible manner.

1.3

norm enforcement

1.3.1

Scope of regulation of the GDPR

Due to its regulatory character, the DS-GVO is considered to be direct

applicable legal act (Article 288 (2) TFEU) has a comprehensive

claim. Added to this is the concern of the addressees and users of the standard,

if possible, all data protection regulations in a uniform way

find law. Finally, were also related to this

simple and understandable regulations desired. The EU Commission

accordingly strived for full harmonization. This target

genes would have required an all-encompassing codification of Union law.

However, the GDPR does not correspond to this and could not

chen: Firstly, the definition of the competences of the Union applies to the

Principle of conferral (Article 5 (1) sentence 1 EU). The

However, data protection also extends to areas in which no

Competences of the EU exist. Here in Germany alone are the federal government

or the countries responsible. Second, Union law is governed by organs of the

Member States carried out, which alone have the competence to regulate the

national administrative organization and administrative procedure.

Thirdly, the living conditions in the globalized networked information

tion society is so complex that simple rules are out of the question.

For example, multi-pole legal relationships cause difficulties that only

are to be overcome by carefully considered solutions to problems. the

Legislators can then draft simple and “lean” regulations in terms of language

meet, but the differentiated problem solution is only shifted to

the enforcement of the norm. The standardization of vague legal terms and

However, the (federal)

Constitutional state only possible to a limited extent (keyword: "essentiality theory"),

albeit conceding that systematically structured codifications

facilitate coherent interpretations. The Age for Simple Laws, in

coherent and self-explanatory, simple codifica-

tion is irretrievably over (cf. Lepsius JuS 2019, 14 ff.).

The realities of data processing are so complicated

become and are changing so quickly that the legislature is constantly

repair is forced. All of this together explains why

the GDPR not only contains specification clauses, but also numerous ones

contains real opening clauses, the supplementary and deviating regulations

allow and require the Member States to carry out such measures (see Section 2). In the

Scope of the DS-RL applies anyway.

1.3.2

interpretation of Union law

Legislation is interpreted in all EU member states

according to subjective and objective criteria, the wording, regulatory

subject matter, the will to regulate and the purpose of the regulation. In connection

to Savigny (System of today's Roman law I, 1840, p. 213 f.).

grammatical, historical, systematic and teleological criteria of

interpretation differed. The criteria usually complement each other, but can

also collide. Above all, the weight of the respective

criteria in the individual legal systems of the EU member states.

8th

introduction

However, this must not lead to an inconsistent application of Union law

to lead. The ECJ therefore considered right from the start of its case work

the European union of states as an independent legal order and

practiced an autonomous interpretation of the

applicable law (ECJ ECR 1982, 12). For the interpretation of Union law

it then comes first to the wording of the disputed

determination. All language

versions (ECJ ECR 1983, 3781, para. 12), what the word interpretation

put into perspective. It is nevertheless the starting point of any interpretation, since Ge-

typesetting texts are only conceivable in verbal form (in the literal sense). With clear

The wording of the "acte clair" or "acte eclairé doctrine" applies, according to which the ECJ

a point of law is not to be submitted if the interpretation is reasonable

wise leaves no doubt (ECJ ECR 1982, 3415 para. 23 ff., cf.

also BVerfG, NJW 2018, 656 para. 43). Of historical interpretation comes

not of decisive importance in Union law. When primary law is

a meaningful investigation of the formation of the will of the contracting parties

hardly possible. In the case of secondary law, the decision-making process of the legislature

Exercise organs only to be considered as far as subjective ideas in the

have found their way into the legal text. The rationale for the statutory

Regulation can be found in the recitals that go directly to the

interpretation of the law can be used (ECJ ECR 1997, I-2549

item no. 21). The systematic interpretation is based on the context of the individual standard

within the overall regulation, clarifies the relationship between the individual articles

among themselves, draws conclusions from the positioning of the provision and

reveals regulatory gaps. In Union law is an important subcategory

the systematic interpretation, the interpretation of the primary law

secondary right. Finally, the teleological interpretation asks for meaning

or purpose of a regulation. When interpreting Union law,

Purpose in two respects to bear: On the one hand plays at the

Evaluation of a legal act its reasoned in the recitals

concrete purpose. The design should help

the legitimacy, competence and proportionality of the act

guarantee. On the other hand, the teleological method serves to

to promote the integration process in general, to keep it going and to preserve it

(integration-securing design).

9

10

legal development

2. Legal development

legal development

2.1

European Union

Efforts were concentrated at the EU level during the reporting period

to the most uniform possible validity and the uniform execution of the

GDPR. For this purpose, the commission already issued on January 24th, 2018

the Communication to the Parliament and the Council “Better protection and new ones Opportunities - Commission guidance on the immediate applicability of the General Data Protection Regulation from May 25, 2018 [COM(2018) 43 final]". Besides legal acts were issued that fill in specification and opening clauses or area-specific data protection law, to which data protection legal conception of the DS-GVO - in particular on the principles of Art. 5 ff. GDPR - but do not change anything. To mention are about

– Council Decision (EU) 2018/893 of 06/18/2018 on the Position taken on behalf of the European Union in the Common EEA Committee to Amend Annex XI (Electronic Communications cation, audiovisual services and information society) and the protokolls 37 with the list pursuant to Art. 101 of the EEA Agreement is (General Data Protection Regulation) (OJ L 159 of 22.06.2018 p. 31 et seq.);

– Regulation (EU) 2018/1725 of the European Parliament and of Council of October 23, 2018 for the protection of natural persons in the processing of personal data by the institutions, bodies and other bodies of the Union, to the free movement of data and to repeal of Regulation (EC) 45/2001 and Decision 1247/2002/EC (OJ L 295 of November 21, 2018, p. 39 ff.)

– as well as Regulation (EU) 2018/1862 of the European Parliament and of the Council of 11/28/2018 on the establishment, operation and the use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in Criminal cases, amending and repealing Decision 2007/533/JI of the Council and repealing Regulation (EC) 1986/2006 of European Parliament and Council and Decision 2010/261/

EU of the Commission (OJ L 312 of 07.12.2018, p. 56 et seq.).

2.2

Member States

The need to supplement the GDPR is determined by the Commission and

viewed differently in the Member States. As far as can be seen, found

the most intensive discussion of the legal competence requirements of the

Union law in the Federal Republic of Germany. Here, in the Bund and

in the countries, logically, the first supplementing the GDPR,

enact implementing laws (see Sections 2.3 and 2.4). Individual member

States, on the other hand, apparently consider implementing laws to be superfluous.

In most cases, implementing laws are in preparation. In the following

As in Germany, member states of the EU have also issued

management laws for the GDPR (overview in Pohle, Cri 2018, 97 ff., 133 ff.;

also GDPR implementation: Current legal status of the EU member states

der – ISiCO data protection https://www.isico-datenschutz.de/.../dsgv...: Die

GDPR in the EU member states: What is the status? - Schuermann

Rosenthal Dreyer Rechtsanwälte https://www.srd-rechtsanwaelte.de/.../...):

Belgium: Law of 03.12.2017 on the establishment of a supervisory authority

de "Loi du 03 December 2017 portant creation de l'Autorité de protection

des données"/"Wet tot oprichting van de Gegevensbeschermingsautoriteit"

(Moniteur Belge/Belgisch Staatblad of January 10, 2018 p. 989). The law

is limited to the establishment of the supervisory authority (Autorité de protection

des données" – APR), which takes the place of the Commission for the Protection of

Privacy ("Commission de la protection de la vie privée" - CPVP) came into force.

Denmark: Act on Supplementary Provisions for a Regulation on

the protection of individuals with regard to the processing of personal data

Data and on the free movement of such data – Personal Data Protection Act “Lov

In the event that the order is made for the order in which the physical person is assigned

i forbindelse med treatment af personoplysninger og om fri udveksling af

sådanne oplysninger – databeskyttelsesloven" of 05/17/2018 (Justitsmin.,

j.nr. 2017-7910-0004). The law contains more far-reaching regulations than

the GDPR for data processing by employees.

France: Personal data protection law “Loi n° 2018-

493 relative to the protection of personal data of 20.06.2018 (NOR:

JUSC1732261L). The law is declared retroactive to 25.05.2018,

repeats and substantiates numerous provisions of the GDPR and

determines the tasks and powers of the National Control Authority

France's CNIL (Commission Nationale de l'Informatique et des Libertés).

Ireland: Data Protection Bill 2018 of 18.05.2018

(Irish statute book07). The law contains a large number of differentiating ones

Regulations which, if Ireland is consistently enforced as a data subject,

ten protection refuge for international technology groups.

legal development

Croatia: Law on the Implementation of General Data Protection Agreements

Gen DS-GVO Implementation Act "ZAKONO PROVEDBI OPĆE UREDBE O

ZAŠTITI PODATAKA” of April 27, 2018 (Official Gazette NN24/2018). The law

contains extensive parallel regulations to the GDPR.

Latvia: The Personal Data Processing Act “Personas

datu apstrādes likums” of April 2nd, 2018 (12 Saeima, No. 1182/Lp 12)

largely takes the GDPR, which it expands with two legal definitions.

The Latvian Data Protection Inspectorate will also be established.

Netherlands: Decision of 05/16/2018 on the entry into force of the law

on general data protection "Besluit van 16 mei 2018 tot vaststelling

from het tijdstip van inwerkingtreding van de Uitvoeringswet Algemene ver-

ordening gegevensbescherming” (Staatsblad 2018, 145) Die Allgemeine

Data protection regulation "Uitvoeringswet Algemene verordening gegevens-

bescherming" expands the exceptions with reference to Art. 9 DS-GVO

from the fundamental ban on the use of personal data,

but at the same time, under certain conditions, data from third parties

To collect persons if this is necessary or a proportionate one

There is interest. The data protection authority is the Autoriteit Persoonsgegevens.

Austria: The federal law for the protection of natural persons in the

Processing of personal data (Data Protection Act - DSG; Federal Law Gazette I

No. 165/1999), which is substantiated by several amendment laws and

was heavily changed. The data

Tenant Protection Amendment Act 2018 (Federal Law Gazette I No. 120/2017). The title is

no longer "Data Protection Act 2000" (DSG 2000), but only "Da-

Tenant Protection Act (DSG). The changes are so extensive that almost

all references to provisions of the DSG 2000 are no longer valid. The

The DSG was revised after the end of the reporting period.

Romania: Law No. 190 amending and finalizing the law

No. 102/2005 on the establishment, organization and operation of the national

national supervisory authority for the processing of personal data and

for the repeal of Law No. 1 677/2001 (Proiect de Lege pentru

modificarea si completarea Legii nr. 102/2005 privind înființarea, organizarea şi funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum) from 31.07.2018. The opening clauses of DS-GVO were used to make exceptions for public authorities, political parties etc. to set.

Sweden: New Data Protection Act (Ny Dataskyddslag) of 18.04.2018 (Riksdagen's minutes 2017/18:100). The law makes of the possibility according to Art. 85 DS-GVO use, freedom of opinion and freedom of information in to give greater weight to the consideration of data protection.

Slovakia: The “New Data Protection Act”, i. H. the "Law on Protection personal data and the amendment of certain laws” (Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov) No. 18 of 01/01/2018 in amendment of the law no. 122/2013 over the Tenant Protection No. 18/2018.

Hungary: The Freedom of Information Act of 2011 was supplemented by two adapted to the GDPR. The first supplementary law concerns the Establishment of a data protection authority. The second supplementary law contains Deviations from the GDPR. The national data protection authority is called Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH).

2.3 Germany

The DSAnpUG-EU, which replaced the BDSG 2017, has already been pointed out in the 46th activity report (item 1.2.3). Through the draft of

2nd DSAnpUG-EU (Bundestag publication 19/4674) is to follow the 1st DSAnpUG-EU

be improved in order to meet the requirements of fundamental and European law.

The draft bill sees changes to the following standards of the

BDSG before:

- § 4 BDSG - video surveillance of publicly accessible rooms

- § 9 BDSG - jurisdiction

- § 16 BDSG - Powers

- § 22 BDSG - Processing of special categories of personal

Data

– § 86 BDSG (new introduction) – processing of personal data

for the purpose of state awards and honors

The countries also adapted their data protection laws to the GDPR:

Baden-Württemberg: Law to adapt the general data protection

law and other provisions of Regulation (EU) 2016/67 (Journal of Laws 2018,

p. 173)

Bavaria: Bavarian Data Protection Act (BayDSG) of May 15, 2018

(GVBl. 2018, p. 230)

Brandenburg: Law on the Protection of Personal Data in the State of Brandenburg

denburg (Brandenburg Data Protection Act - BbgDSG) from 08.05.2018

(GVBl. I/18, [No. 7])

legal development

Berlin: Law on the Protection of Personal Data in the Berlin Administration

(Berlin Data Protection Act - BlnDSG) of June 13, 2018 (GVBl. 2018,

p. 418)

Bremen: Bremen implementation law for the EU General Data Protection Regulation

Regulation (BremDSGVOAG) of 08.05.2018 (Bremen Law Gazette 2018, p. 131)

Hamburg: Hamburg Data Protection Act (HmbDSG) of May 18, 2018

(HmbGVBl. 2018, p. 145

Hesse: cf. item 2.4

Mecklenburg-Western Pomerania: Law to adapt the state data protection

law and other data protection regulations in the jurisdiction

Department of the Ministry of the Interior and Europe Mecklenburg-West Pomerania

to Regulation (EU) 2016/679 and to implement Directive (EU)

2016/680 from 22.05.2018 (GVBl. 2018, p. 194)

Lower Saxony: Lower Saxony Data Protection Act (NDSG) from

May 16, 2018 (Nds. GVBl. 2018, p. 66)

North Rhine-Westphalia: North Rhine-Westphalia Data Protection Act of May 17, 2018

(GV. NRW. 2018, p. 244, calculated p. 278 and p. 404)

Rhineland-Palatinate: State Data Protection Act (LDSG) of May 8th, 2018

(GVBl. 2018, p. 53)

Saarland: Saarland Data Protection Act of May 16, 2018 (Official Gazette 2018 I,

p. 254)

Saxony: Saxon Data Protection Act of 25.08.2003 (Saxon GVBl.

p. 330), last amended by Art. 46 of the law of 04/26/2018

(Saxony GVBl. 2018, p. 198)

Saxony-Anhalt: Law on the protection of personal data of citizens

(Saxony-Anhalt Data Protection Act – DSG LSA) i. i.e. F. the Notice

from January 13, 2016 (GVBl. LSA 2016, p. 24), last amended by Art. 1 of the

Law of February 21, 2018 (GVBl. LSA 2018, p. 10)

Schleswig-Holstein: Schleswig-Holstein Law on the Protection of Personal

personal data (State Data Protection Act - LDSG) from 02.05.2018

(GVOBl. 2018, p. 162)

Thuringia: Thuringian Data Protection Act (ThürDSG), promulgated as Art. 1

of the Thuringian law for the adaptation of the general data protection law

to Regulation (EU) 2016/679 and to implement Directive (EU)

2016/680 from 06.06.2018 (GVBl. 2018, p. 229)

2.4

Hesse

In Hesse, the state data protection law was amended by the

Act to adapt the Hessian data protection law to the Ordinance

Regulation (EU) 2016/679 and implementing Directive (EU) 2016/680 and

on freedom of information from May 3rd, 2018 (GVBl. 2018, p. 82). The law is

divided into articles; it is thus an article law. In the article laws

A distinction must be made between "Omnibus Laws" in which different regulations

areas of development combined in a single law and within the

be differentiated from one another by articles of the law (cf. Lachner, Das

Omnibus Act, 2007, pass.), and amending subsequent laws in which a

agreed on the newly regulated topic of changes in numerous specialist laws

leads. Omnibus laws are interpreted individually. change sequence

laws, on the other hand, make it necessary to use the common denominator

to work out. Title, structure and history of the origin of the HDSIG

give the impression of an omnibus law. The full title of

HDSIG lists three separate areas of regulation that do not necessarily have to be one

require control unit. Also the draft law of the parliamentary groups of the CDU

and BÜNDNIS 90/DIE GRÜNEN for a Hessian adaptation law

of the Hessian data protection law to the regulation (EU) 2016/679 and

to implement Directive (EU) 2016/680 and freedom of information

deals with the adaptation of the Hessian state law to the VO 2016/79,

the implementation of Directive 2016/79 and freedom of information as different

material. But even with the subsequent changes affecting the specialist laws

changes, the law assumes the uniformity of data protection law

out of. In contrast, different objectives were set for data protection

and freedom of information accepted (LTDrucks. 19/5728); more accurate:

Data protection law was only used as a barrier to freedom of information

understood. The draft justification states:

“The citizens of Hesse have a legal right

for access to the official

information. It is not only the protection of operational or

Business secrets guaranteed, but also in particular by

personal data. Because of the close connection between

the information access right on the one hand and data protection

on the other hand, the regulations on access to information as

further part in the Hessian Data Protection and Freedom of Information Act

inserted."

In the course of the legislative process, however, the opinion prevails

by the fact that data protection and freedom of information are not opposites, but

Elements of a comprehensively understood informational self-determination

are. Data protection and freedom of information were therefore not in several

Articles, but housed in one article. Hesse thus has
the most modern data protection law of the German implementing laws. The
Understanding of freedom of information as corresponding to data protection
the element of informational self-determination is not yet in
penetrated the general consciousness. Therefore, still on the youngest
Development of informational self-determination in connection with
of freedom of information. In connection with that
conventional data protection it is sufficient to point out that the HDSIG from the Hes-
was passed in the third reading on April 26th, 2018. With
Art. 5 of the law of September 12, 2018 added two provisions to the HDSIG
supplemented, relating to data processing at public honors and
obtain clemency proceedings.

2.5
Amendment of the Hessian law on the public
security and order

The Hessian law on public safety and order
undergone some changes this year. In addition to the necessary
Implementation due to the European data protection reform was the occasion
the case law of the BVerfG on the BKA law and the concerns of the
Government factions, further authorization bases for the police
create. It has not been possible in all points to establish the proportionate
to maintain idleness.

On the course of the legislative process

The partly comprehensive changes in the Hessian law on the
public safety and order (HSOG) - insofar as these also include data protection
are legally relevant – were based on three circumstances:

– In the HSOG, the specifications of the JI guideline (guideline 2016/680
of April 27, 2016 to protect natural persons during processing
personal data by the competent authorities for the purpose
the prevention, investigation, detection or prosecution of criminal offenses)
be implemented.

– In 2016, in its decision on the BKA law (1 BvR
966/09, 1 BvR 1140/09; BVerfGE 141, 220-378) framework conditions
formulated, which are also relevant for the state police laws.

– The government factions had decided to grant additional
legal basis, in particular for combating terrorism
create the police.

Some of the individual changes were difficult to understand during the process.
pull because they are in two legislative projects to be discussed at the same time
were included. On the one hand, this was Art. 18 of the Hessian law
to adapt the Hessian data protection law to the regulation (EU)
No. 2016/679 and for the implementation of Directive (EU) No. 2016/680 and for
Freedom of information, which was drafted by the governing parties on December 5th, 2017
was brought into the state parliament (LTDrucks. 19/5728). More – not un-
essential changes were contained in the draft law of the government factions
on the new regulation of the protection of the constitution in Hesse (LTdrucks. 19/4512
from November 2017).

Implementation of the BKA law decision of the BVerfG

In the decision mentioned, the BVerfG 2016 redefined, under

what conditions the police authorized data for a purpose

were allowed to be collected and processed, also for other purposes

may. To this end, it coined the term hypothetical reassessment.

This would meet the proportionality requirements for a change of purpose

concretize. However, the prerequisite for a change of purpose is that

the new use of the data the protection of legal interests or disclosure

of criminal offenses of such weight that constitutionally

justify their reassessment with comparably serious means

could. The preconditions for one are not identical in every case

Change of purpose with those of data collection, however, with regard to

required degree of specificity of the risk situation or the crime

thought. The relevant requirements determined under

ness aspects primarily the reason for the data acquisition

collection itself, but not also for the further use of the collected data.

As a new intervention to be justified, however, the authorization to

a use for other purposes of their own, sufficiently specific

occasion. Constitutionally required, but regularly accordingly

also sufficient to the extent that the data - be it from them

itself, be it in connection with further knowledge of the authority - a

specific investigative approach result.

The legislator can then fundamentally change the purpose of data

Lich then allow when it comes to information from which

in individual cases, concrete investigative approaches to uncover comparable

serious criminal offenses or to ward off at least in the medium term

threatening dangers for comparably important legal interests

whose protection the corresponding data collection is permitted.

The now revised regulations for data collection in the HSOG

allow the further processing of personal data to fulfill the

Tasks of security and police authorities for other purposes

than those to which they have been raised, only if at least

tens comparably serious crimes or administrative offenses prevented

or at least comparably important legal interests or other rights

are to be protected and concrete investigative approaches in individual cases

to prevent such criminal offenses arising or to ward off in a

foreseeable period of imminent danger to such legal interests or

reveal other rights, for the protection of which the corresponding data

collection would be constitutionally permissible. So are also after mine

Assessment in this context meets the criteria set by the BVerfG.

The other changes in the HSOG associated with the implementation of the decision

to the BKA law, cannot be detailed here

being represented. However, I also see no reason to

to formulate.

Extended powers of collection – QuellenTKÜ and online

search

The requirements for the online TKÜ in § 15a HSOG have been expanded.

In addition, the so-called online search was also added.

These changes were originally in the HSOG bill

not provided. However, appropriate powers for the

provided for constitutional protection. These arrangements were made as part of the

Parliament hearing and also in the public debate on a large scale

criticized.

In response to this, the government factions of appropriate

Apart from powers for the protection of the constitution and insofar their

draft law withdrawn. As part of this action was then

However, at short notice the corresponding change for the HSOG in the country

brought in day. A real argument as to whether and why this is considered

police powers is required and to what extent this is in the interests of the

to create framework conditions for the right to informational self-determination

were, could not be done.

In the contentious debate on the HVSG, a fundamental

additional security issue pointed out. To get the necessary tools

to develop or to adapt to a specific application and on which to

to implement the monitoring computer, it is necessary to

to know security gap. These should - as soon as recognized - actually the

be communicated to the respective software developer so that they can

lich be closed by appropriate updates to avoid damage

be avoided by all users. Exploiting such gaps and thus

the necessary concealment by the state is problematic. With it

does he tolerate the possibility that others - with the intention of causing harm - use these

also use the gap.

Whether and how these instruments will be used in the future and to what extent

far thereby the constitutional framework for lawful

encroachments on the right to informational self-determination are preserved,

will require careful monitoring. This is also the subject of the new

Inspection obligation according to § 29a HSOG (see also section 2.7)

The implementation of the European data protection reform

Not for all areas in which the police take preventive action is the

scope of application of the JI Directive. According to Art. 1 Para. 1 is dated

Scope of protection and defense against threats to the public

security included. This is not congruent with the scope

according to § 3 paragraph 1 HSOG.

Art. 1 para. 1 JI Directive

This policy contains provisions to protect individuals with regard to processing

personal data by the competent authorities for the purpose of prevention,

Investigation, detection or prosecution of criminal offenses or the execution of sentences,

and finally protection against and averting of threats to public safety.

§ 3 para. 1 HSOG

The provisions of this law apply to the performance of the tasks of the

Averting danger and other tasks according to § 1. Federal or state regulations

desrechts, in which the prevention of danger and other tasks are specifically regulated

are, take precedence over this law. Insofar as the special legal provisions do not

contain the relevant regulations, this law is to be applied additionally.

Therefore, a differentiation must be made for a large number of control complexes,

whether regulations of the GDPR or the HDSIG in addition to the area-specific

HSOG regulations apply. The law itself

does not define which specific tasks are not within the scope of

JI guideline are included, but refers abstractly to the application

area of application of § 40 HDSIG, which, however, only contains the wording of

Art. 1 JI Directive. In the following, reference is therefore made to the HDSIG

legal development

or the GDPR. With that, the regulations for the

Much more difficult for users as well as for citizens

accessible than the previous regulations of the HSOG. That becomes part

even covers that in the end there is no impact on practice

arise because the material content of the regulation has not changed. If this

overall can still be considered a standard-clear regulation - and thus one

essential prerequisite for permissible interference with the right to information

functional self-determination fulfilled – future practice must also show.

background checks

As part of the possibilities to carry out background checks,

several changes have been made. On the one hand, you can now

the Office for the Protection of the Constitution to be involved in these procedures. Additionally

on the authority for the protection of the constitution, data in this context

to be allowed to transmit, a new reason was also defined when a

such an examination is permissible (on the problem with this regulation, see Section 2.6).

Participation of the Office for the Protection of the Constitution in background checks

13a and b should take place, insofar as this is the case in individual cases

is required. In practice, there is still a considerable need here, criteria

to develop for when such an individual case exists. Always has to

be justified in the person of the person concerned or this can also be done by

the type of activity of the persons to be checked or their place of work

be dependent. This plays a role in particular in the future new regulation

Role. According to § 13b paragraph 1 sentence 3, the police can now also suggest

that in the context of a private event a background check

function can take place.

A real conception or even specifications from the state police

zeipräsidium according to which criteria both the event and a

Selection of the group of people to be checked can be made is

not known to me until now.

video surveillance

The regulations for video surveillance in the context of security

have found a fundamental reorganization. This is also in context

to see with the newly created § 4 HDSIG, which is now expressly

allows public bodies, under certain conditions - such as for

Safeguarding house rights – using video cameras. This is at the same time

clarified that the regulations of the HSOG in § 14 paragraphs 3 and 4 only apply in

can be applied in the context of classic hazard prevention.

Section 14 (3) and (4) HSOG

(3) The danger prevention and the police authorities can to avert a danger or if

factual evidence justifying the assumption that criminal offenses are imminent, public

openly observe and record accessible places by means of image transmission. The fact

of monitoring and the name and contact details of the person responsible

to be made recognizable by suitable measures at the earliest possible point in time. Firmly

installed systems must be checked every two years to ensure that they meet the requirements

are still available for your operation. Paragraph 1 sentence 2 and 3 applies accordingly.

(4) The danger prevention and the police authorities can open by means of image transmission

observe and record

1.

2. to control systems for directing or regulating road traffic, insofar as

to protect particularly endangered public facilities or premises,

Provisions of road traffic law do not conflict.

Insofar as the owner of the domiciliary rights is not a danger prevention or police authority, the following applies

he in the case of sentence 1 No. 1 as security authority. Paragraph 1 sentence 2 and 3 and Paragraph 3

Sentence 2 and 3 apply accordingly.

According to the will of the legislature, there is now no distinction

more, whether the police or the danger prevention authority - the municipality -

want to operate such systems. This is the previous distinction

repealed the establishment for the security authorities to a

higher hurdle, because there had to be corresponding ones

Criminal offenses have occurred and continue to do so within the framework of the risk forecast

to be expected. However, the current regulation reflects reality. In the

Most of the cases I know of were prompted to be monitored

from the political bodies of the municipality, but is enforced by the police

led and in this constellation by the state government also by not

insignificant grants funded. In fact, this is therefore after my

Assessment does not lead to any significant changes, whether in individual cases

a video surveillance system is planned or implemented or not.

The redesign of Section 14 (4) addresses questions from practice. Again-

holt shouldn't be a particularly vulnerable entity altogether, but rather

only individual rooms within a building can be secured.

The storage room for evidence such as weapons and/or

or intoxicants at the public prosecutor's office or access to cash

or vaults. From my point of view, this is a useful clarification.

As a total of the system of video surveillance for public bodies in

Hesse significant changes were made, I also had

excited to take up two further points that I find misleading or

even clearly disproportionate.

22

legal development

This refers first to Section 14 Paragraph 3 Sentence 4, which to Section 14 Paragraph 1 Sentence 2 and

3 and thus a storage period of up to two for all recordings

months possible. This is disproportionate and does not correspond either

of general practice. Even the LKA recommends this in a handout

for the municipalities only a storage period of up to ten days. This

Period is quite sufficient to decide whether an evaluation and

if necessary, a backup of the corresponding recorded sequences for

further measures or criminal proceedings to be initiated are necessary.

The general storage

regulations for the respective procedure. With that is a retention

of all records for such a long period of time is not required.

The wording in paragraph 3 sentence 3 has led to misunderstandings. she was

been created to ensure regular verification of legality

of the operation of a plant. In doing so, it should be ensured

that a system can also be operated until this inspection

test leads to a negative result. Should, however, in the course of

2-year period clearly shows that the requirements at this

place no longer exist, the legality of a

Video surveillance will not be stipulated. This comes about in cases in

Consider where the redesign or development of a square changes the local

changed in such a way that the original risk situation no longer exists

can be accepted. This must be especially true when

it can be foreseen from the outset that the prerequisites for video surveillance

are only given for a certain period of time. This is how it can be used

of video technology for a specific event - e.g. B. Major events such as

the Hessentag – does not justify video surveillance for two years.

That's why I suggested to formulate:

Permanently installed systems must be checked every two years to ensure that they

the conditions for their operation are still met."

Unfortunately, the legislature only followed the latter suggestion.

Framework for the use of new technical processes

Section 25a takes up new material. This is a response to considerations

new systems for data analysis for the fulfillment of police tasks

to use. The use of such systems by the police is suitable

elementary principles of data protection and the right to information

functional self-determination into question. Such procedures can

enormous amounts of heterogeneous – structured as well as unstructured –

Evaluate data at high speed. That's why the conference

the data protection officers of the federal and state governments already in their

89th Conference in March 2015 in a resolution pointed out that

that the existing legal regulations in the federal and state governments do not

explicit specifications for the use of extensive analysis systems

included (cf. 44th activity report, point 7.9).

The linking of data from different police databases

as well as, if necessary, the extension to include generally accessible data from the

Internet constitute encroachments on the right to informational self-determination

with a considerable depth of intervention. However, this is only permissible to the extent that

there is a clear legal basis.

§ 25a HSOG

(1) In justified individual cases, the police authorities may

process generated data using an automated application for data analysis

for preventive combating of those mentioned in Section 100a (2) of the Code of Criminal Procedure

criminal offenses or to avert a threat to the existence or security of the Confederation or

of a country or body, life or liberty of a person or things of importance

Value whose preservation is required in the public interest, or if of equal importance

damage to the environment is to be expected.

(2) Within the framework of further processing according to paragraph 1, relationships

or connections between people, groups of people, institutions, organizations

ations, objects and things produced, insignificant information and knowledge

excluded, the incoming findings assigned to known facts

and stored data are statistically evaluated.

(3) The establishment and significant modification of an automated application for

Data analysis is carried out by order of the authority management or one of

these authorized officers. The Hessian data protection officer is in front

to hear the establishment or significant change pursuant to sentence 1; in the event of imminent danger

the hearing must be made up for.

With the definition of the possible areas of application to the preventive

Combating particularly serious criminal offenses and restricting them

the regulation tries to ward off serious dangers

limit the scope. This seems to me considering the

interests of those affected are fundamentally proportionate. An additional

The moment of security results from the reservation of the head of the authority and in particular

special also my involvement in the context of the establishment or essential

Changes to Automated Applications.

The monitoring and control of corresponding projects will be a

important aspect of my activities in the field of police data processing

be work

legal development

2.6

Amendment of the Hessian Constitutional Protection Act

In June 2018, the Hessian state parliament passed extensive changes

ments of the legal regulations for the protection of the constitution. Next to

organizational questions, these also concern fundamental aspects in the

Context of the right to informational self-determination.

In November 2017, as part of a draft law by the Government

factions (LTdrucks. 19/5412) the long-awaited reform of the Hessian language

Constitutional Protection Act (HVSG) brought into the state parliament and then

in December as part of a change request (LTdrucks. 19/5782)

expanded.

A major change concerns the reorganization of the powers of the

protection of the constitution for information collection. A significant impact

on the rights of citizens, which also has the transformation of

information regulation. At the same time, parliamentary control became partial

restructured and regulated in a separate law, however

will not come into force until the beginning of the new legislative period in January 2019.

Before the regulations were introduced in the state parliament, I had no opportunity

to comment on the planned changes. Only during the hearing

in the state parliament I was able to comment on the extent to which it was intended

Regulations and the associated interference with the right to information

self-determination respects the constitutional requirements

became. This includes, on the one hand, that the regulations according to the

jurisprudence of the Federal Constitutional Court must be clear in terms of norms

as well as that the essential decisions by the legislature itself

are meeting These requirements must be observed in particular

if detailed regulations can only be made through service regulations, also

as far as this is not from the state office, but from the responsible ministry

are to be enacted.

A special focus of my statement was therefore on the regulations

genes that serve to safeguard the rights of those affected. That applies above all

for the possibilities of checking the handling of personal data

data and, in particular, the right of citizens to information.

Here are, in my estimation, limitations of the informational

self-determination that does not do justice to the protection of fundamental rights

the. Clear regulations are also necessary because the general

Data protection regulations for public bodies for the protection of the constitution

do not apply or only apply to a very limited extent.

The hearing in the state parliament has considerable criticism of some points of the amendment

make it clear. This applied in particular to the planned new authorization

such as online telecommunications surveillance (source TKÜ) and

the online search and the involvement of the Office for the Protection of the Constitution

in background checks. As part of a further amendment

trages (LTdrucks. 19/6502) was then im by these new powers

HVSG apart, but this in the Hessian law on the public

Security and Order (HSOG) included. Furthermore, an adjustment

adaptation to the new regulation of data protection law that has taken place in the meantime

in the context of the European data protection reform and its adoption

of the Hessian Data Protection and Freedom of Information Act (HDSIG).

Criticisms of the new legal regulation

I will single out a few points for which I believe

there is still a need for improvement.

Design of data collection

In contrast to the old regulation, the possibilities for data collection are included

intelligence means are now standardized in law and no more

left to a service regulation of the Ministry of the Interior. The regulations

for the further handling of this data should then continue

only result from a service regulation. The "dealing" with the raised

Information is not a term under data protection law and therefore opens one

wide scope for interpretation. Everything you need to know about encroaching on the law

however, the legislature itself is entitled to informational self-determination

rules. This wording makes it unclear which regulatory areas

are left to such a service regulation, but also to what extent

tere legal requirements for handling the data by such

Service regulations must be observed or even modified.

information of those concerned

The requirements and the procedure for obtaining information about

Storage by the Office for the Protection of the Constitution was made considerably more difficult,

if not limited in practical application. The

The right to information is an essential basis for those affected to exercise their fundamental rights

te to perceive and thus to enable them, if necessary, against

to defend unauthorized data storage or transmissions.

26

legal development

§ 26 HVSG

(1) The State Office provides the person concerned with information about his or her person

stored data free of charge upon request, as far as the person concerned

points to a specific fact and a special interest in information

sets out. If the data subject does not show a particular interest when requested to do so

the State Office decides at its due discretion. The information extends

not up

1. the origin of the data and the recipients of transmissions and

2. Data that is not stored in a structured manner in automated files, unless

the data subject provides information enabling the data to be located, and

the effort required to provide the information is not disproportionate

on the interest in information expressed by the data subject.

The state office determines the procedure, in particular the form in which information is provided,

at due discretion.

(2) The provision of information is omitted, insofar as this is done by you

1. there is a concern that the fulfillment of the tasks will be jeopardized,

2. Message access can be endangered or the exploration of the epistemological

status or the working methods of the state office is to be feared,

3. jeopardizes public safety or otherwise the welfare of the Federation or one

country would be disadvantaged or

4. Data or the fact of their storage are disclosed after a

Legislation or its essence, in particular because of the overriding

legitimate interests of a third party must be kept secret.

The decision is made by the management of the authorities or a member of staff specially commissioned by them.

worker or an employee specially commissioned by her.

(3) The refusal to provide information does not require any justification. It contains one

Indication of the legal basis for the lack of justification and that

the data subject to the Hessian data protection officer or the Hessian

data protection officer. Notifications from the Hessian data

protection officers to the data subject without the consent of the state office

do not allow any conclusions to be drawn about the state of knowledge of the state office.

Pursuant to Section 26 (1) HVSG, it is necessary for the person concerned to

indicates a specific fact as well as a special information

expresses interest. Comparable restrictions existed before the new regulation

not. The reason given was essentially the prevention of an

proportionate administrative expenses as well as the existing ones

regulations in federal law. In respect of fundamental rights

protection, the effort can only play a subordinate role.

The reference to the regulation of the BVerfSchG is also convincing as justification

not. For this question it is not necessary that the

legal regulations are identical nationwide. If anything, can

only have an impact on the question of to what extent

or in which cases the provision of information is restricted or rejected

can be. The possibilities for restricting the information or the

Refusal - as they are now contained in the law - has also existed

in the old rule.

The presentation of the special interest in information should also serve to

to prevent attempts to investigate. I have doubts whether this is a suitable

net means for it is. Who really to research his right of access

want to abuse will be able to increase his interest accordingly

formulate. On the other hand, everyone else is forced to explain why

he wants to exercise a fundamental right. As far as there is evidence of such

procedure, the refusal to provide information was also previously permissible.

It has not become known to me that under the old legal situation the information

has been misused on a fairly large scale for research purposes.

Participate in background checks

What was newly created was the express authority to

to include the protection of sockets in reliability checks. In the

However, the law itself will not do this within the scope of the powers, but

only regulated in the context of the permissible data transmissions in § 20.

§ 20 HVSG

(1) The State Office may provide information including personal data, even if

they were collected by means of intelligence services, to domestic public authorities

transmit if the recipient needs the information

1.

to protect the free democratic basic order or for other purposes

public security or criminal prosecution, insofar as the transmission is not

is limited according to paragraph 2, or

2. to fulfill other tasks assigned to him, provided that he also does so for protection

to contribute to the free democratic basic order or aspects of

has to appreciate public security or foreign interests, in particular

...

c) verifying the compliance of persons applying for employment in

apply for public service, with their consent,

...

g) checking the reliability of persons according to the security and

commercial regulations, in particular

aa) the admission of persons for the access-protected security area

of events,

bb) from the Hessian initial reception center for refugees and their

security personnel employed at branch offices,

cc) by security guards employed at communal refugee shelters,

h) the verification of the reliability of at the Hessian initial reception center

Department for Refugees and its branch offices

and interpreters,

the event-related review of the reliability of people and organizations

organizations with which the state government works

aa) in justified individual cases,

bb) on the occasion of the first funding of organizations with state funds,

provided these in work areas to combat anti-constitutional

efforts should be made

with their consent and the opportunity to comment,

...

However, some of the defined cases seem to me to be very broad.

A prerequisite for such checks would also have to be for the individual person

always be that there are indications that it is the case in a specific case

is required. A blanket inclusion of entire organizations or

Groups of people is not compatible with the principle of proportionality.

Admittedly, it was also obtained here as part of the legislative process

on the promotion of organizations with state funds or also the

Cooperation of people in state government projects

improving, but the framework is still very broad. After my

Assessment will be given to organizations upon initial funding

a general suspicion, without any indication of the individual

Necessity of such a review, with the concrete to be checked

Persons are related, must be present.

Also the possibility of reviewing applicants for the public

Service reminds of the rule review as part of the Radical Decree

from the 1970s.

Data protection control of the activities of the state office

for protection of the constitution

Due to the new regulations in data protection law and because of the constitutional

protection is expressly excluded from the application of the DS-GVO acc.

Art. 2 Para. 2 lit. a DS-GVO, it is determined in § 15 which regulations of the

HDSIG apply in addition to the provisions of the HVSG.

Unlike most administrations, this rule is mine

Area of competence still very limited. Because it can also in the future

I only make complaints. From the new powers that i

e.g. B. to the police, I can only warn that

a planned data processing against data protection regulations

violates. With that, I still have limited options, in the interest

of those affected to ensure that their rights are respected.

In the context of the tightening of the above-mentioned requirements for the information

From my point of view, this represents a significant limitation for the granting of

which was not given a viable justification in the legislative process.

Parliamentary control of the state office

The regulations for parliamentary control of the protection of the constitution

can now be found in a separate law, the Constitutional

protection control law. The regulations differ only slightly from the

current regulations. After the justification, changes should be in

to a large extent based on the Federal Control Body Act. Not

in all respects, however, succeeded, the new and the existing

to reconcile regulations in a meaningful way.

Among other things, it is new that the Parliamentary Control

Commission (PKK) a branch is clearly assigned. One

However, there is no assignment of tasks for this office. The

Minutes of the meetings will continue to be taken by the chancellery of the state parliament

transfer. There are still no specifications for the meeting rhythm; only

Deadlines are given for the reports to be submitted. A real boost

of parliamentary responsibility this is not.

Also the regulation that the members of the PKK with named employees

discuss matters of the control commission

may, but there is no clarification that this also includes documents for the

Being allowed to see consultations does not seem successful to me. A sensible one

Advice can often not be given in the abstract without documents. As it often

will deal with documents that require special confidentiality,

and personal information may also be the subject,

an express permission in the law would have made sense.

Therefore, whether these rather marginal changes in content compared to the

old regulation for a more effective control of the protection of the constitution

by the PKK, future practice must show.

2.7

Increased statutory inspection requirements

The legislator has specifically strengthened the data protection officers

undertakes regular checks of individual data processing procedures

to perform. In some cases, a specific test cycle is explicitly stated

predetermined. This ties up considerable personnel capacities, also at the expense of

Fulfillment of other tasks of my office.

There are already a large number of statutory provisions in place at the present time

inspection requirements. State, federal and EU laws are constantly introducing new ones

added. For the first time in his decision on the Anti-Terrorism Database Act (ATDG)

in 2013, the Federal Constitutional Court (BVerfG) explicitly one

specific test frequency required for data protection officers (1 BvR
1215/07, BVerfGE 133, 277-377). The court had stated: “Because a
Transparency of data processing and enabling individual
Legal protection by the Anti-Terrorism Database Act is only very limited
can be ensured comes ensuring effective
supervisory control all the more important. The relative
The principle of quality therefore requires an effective design of this control
increased both at the level of the law and of administrative practice
requirements” (paragraph 214). From this, the court then has corresponding
Requirements for the control by the data protection officer formulated:
“Given the compensatory function of supervisory control for the
Weakly designed individual legal protection comes more regularly
implementation and are such controls appropriate
measured distances – the duration of which is a certain maximum, about two
years, shall not exceed – to be carried out” (paragraph 217).
As a reaction to this decision, at the end of 2014 the novel
The regulation of the ATDG stipulates the obligation to check every two years.
§ 10 ATDG
(1) According to § 24 paragraph 1 of the
Federal Data Protection Act to the Federal Commissioner for Data Protection and
freedom of formation. The records entered by the countries in the anti-terror database
can also be used jointly by the respective state representative for data protection
be controlled in connection with the performance of their examination tasks in the federal states,
as far as the federal states are responsible according to § 8 paragraph 1. The Federal Commissioner for the
Data protection and freedom of information works in this respect with the state representatives for
data protection together.

(2) Within the scope of their respective responsibilities, the bodies named in paragraph 1 are

is obliged to check the implementation of data protection at least every two years.

It didn't stop with this commitment. In addition to other federal

legal regulations, there is now also a corresponding one in the HSOG

contain obligation. Further obligations arise in the context

of data processing within the European Union. The single ones

Obligations differ partly in frequency, but also in

the number of positions to be checked. In particular

further procedures are currently being planned by the EU, which will

create obligations.

An overview of the current status results from the following

Tabel. Other obligations that are due to

the distribution of responsibilities within the Federal Republic of the BfDI

are incumbent, but for which support is provided by the state representatives

must take place, because only they are entitled to verify the legality of the

underlying data storage by state authorities in the

respective files to be checked.

to be checked

Place)

test cycle

LKA and LfV

LKA and LfV

every 2 years

every 2 years

LKA

LKA and PPs

possibly more

authorities

data processing

Events in N.SIS II:

every 4 years (under

support for BKA)

otherwise (especially

data retrieval and

-further processing):

regularly

Querying the security

health authorities

VIS access

decide everyone

4 years otherwise:

regularly

yearly

all

closed

authorities

(Police;

Foreigner-

offices)

Subject of the examination	Legal basis
a) Federal Audit Obligations	
Anti-Terrorism File (ATD)	
Right-wing extremism file (RED)	
b) EU legal instruments	
Schengen information system (SIS II) – processing	
processing of SIS II data (including their transmission and exchange and further processing of additional information.	
Visa Information System (VIS) – Processing of	
VIS data (incl Transmission to the and from VIS)	
	Section 10 (2) ATDG
	Section 11 (2) RED-G
	Art. 44 para. 1 VO 1987/2006/EC i. V. m. Article 60 paragraph 1 Resolution 2007/533/

JI Council

Art. 41 para. 1 VO

767/2008/EC

i. V. m.

Article 8 paragraphs 5 and 6

Resolution 2008/633/

JI Council

i. V. m.

§ 4 VISZG

(VIS access law)

Art. 32 para. 2, 33

Para. 2 VO

603/2013/EU

European dactyloscopy

System (Eurodac) –

Processing of the Eurodac

data (including their

Transmission to and from

Eurodac)

32

c) State law inspection obligations

HSOG

Section 29a

all police

hear

legal development

at least all

2 years;

according to § 28 paragraph 2

logged ver-

covered measures

as well as transmission

international

nal area

In addition to checking whether the individual data in the respective databases

are rightly stored, for example, a check is then carried out

considering whether the procedures and conditions for the query have been complied with

became.

Such tests cause a considerable personnel expenditure. One

Control of access rights initially includes an evaluation of existing ones

loggings. Tools are not available for this in all cases

facilitate meaningful evaluation of the respective log files. so can

the log files generated as part of the use of the ATD

be evaluated according to assigned parameters, but the result is common

nevertheless a presentation in the form of a pdf file that has several 100 pages

may include. Whether the respective accesses were authorized can only be determined by

a parallel insight into the underlying files/administrative processes

be assessed.

The consequence of this is that even with a very small sample

rehearse such a review with all the pre- and post-processing several

days and binds at least two to three employees. Included

If the checks of the technical conditions are not yet included

considers.

In its decision, the BVerfG also expressly referred to the framework

conditions for adequate control by the data protection officer

pointed out: “Given the compensating function of the supervisory

Control for the weakly designed individual legal protection comes

their regular implementation is of particular importance. This is at

their endowment” (paragraph 217).

With the current body of staff, all these obligations cannot

be adequately met. This is also not due to another

punktbildung achievable, as well as the processing of complaints and

the fulfillment of my other tasks according to the DS-GVO and § 7

HDSIG must not be neglected in favor of the compulsory examinations.

33

34

Data protection report until 05/24/2018

3rd data protection report until 05/24/2018

(according to HDSG and BDSG)

Data protection report until 05/24/2018

3.1

General administration, municipalities, social affairs

3.1.1

Data transmission to religious communities to determine the

local church tax

The municipalities are not authorized to collect the data of all those subject to property tax A

to transmit to the church tax office, so that this the local church tax

can set for the evangelical parishioners.

Two municipalities have contacted my office and asked whether

it is permissible to send the data of all those subject to property tax A to the Evangelical

sche church tax office. The church tax office uses

of the tax data of the municipalities the local church tax for their

members.

Basically, the financial authorities are according to § 31 paragraph 1 sentence 1 tax

ordinance (AO) obliges tax bases, tax base amounts and

Tax amounts to corporations under public law, including

Religious communities that are corporations under public law,

to notify the determination of such taxes, which are due to this taxation

bases, tax base amounts or tax amounts. However

this obligation does not apply if the compilation of the desired

databases would mean a disproportionate amount of effort

(Section 31 paragraph 1 sentence 2 AO). This can e.g. e.g. if the com-

Don't mune the requested information by church membership at all

separately available.

§ 31 paragraph 1 sentence 1 and 2 AO

The tax authorities are obliged to provide tax bases, tax base amounts and

Tax amounts to corporations under public law, including religious

communities, which are corporations under public law, for the determination of

to notify such taxes, which are based on these tax bases, tax base amounts

or attach tax amounts. The obligation to notify does not exist insofar as its fulfillment

would involve a disproportionate amount of effort.

This is how it was with the requesting municipalities. Both municipalities

commented that they did not have the necessary staff to process the data

evangelical parishioners from the data of all taxpayers

to sort out. They have this from the evangelical church tax office

communicated. The church tax office replied that other municipalities

under these circumstances, the data of all those subject to property tax A

would have made available to the church tax office. This then have the

Evaluation of the records taken and the data of the evangelical

Community members extracted.

With this procedure, the church tax office also receives tax

data of taxpayers of other denominations and beliefs

as well as non-denominational. The church tax office is for this group of people

but not authorized to set taxes. In other words: the data

are not necessary for the fulfillment of the tasks of the church tax office and

their transmission is in no way derogated from the legislation cited above

covered.

I have therefore informed the municipalities that I will no longer transfer the data

of the tax data of all those subject to property tax A to the church tax

office to be inadmissible. Only the data of the taxpayers who

belong to the Evangelical Church, would have permissibly belonged to the Church

may be transmitted to the tax office.

A consultation with the Hessian Ministry of Finance put me in

confirmed this view. The Ministry also referred to Section 8

of the Church Tax Act, according to which the state and municipal authorities

the churches (congregations) on request for taxation

transmit the necessary data, insofar as these have already been provided by the authorities

are collected for other purposes and to the extent that the administration of the

tax is not the responsibility of the tax offices.

3.1.2

Administrative assistance from the social administration at the request of a tax office

The transfer of personal data by a social authority to

the tax office cannot be based on the administrative assistance principle, but

requires a data protection law authorization standard.

A job center asked me for a data protection assessment with regard to

a request for information from a tax office. Specifically, it was about personal

data from a beneficiary of the job center. was propped up

the request from the tax office to § 111 Para. 1 AO and § 3 SGB X.

The § 3 SGB X mentioned by the tax office concerns the "administrative assistance".

cooperation of authorities.

§ 3 paragraph 1 SGB X

Each authority provides additional assistance (administrative assistance) to other authorities upon request.

This regulation placed in the first chapter of the tenth book of the SGB

is, however, regulated by that in the second chapter of the Tenth Book

Social data protection law is superseded insofar as it is

behavior is about personal data (social data). This arises

from § 37 S. 3 SGB I.

§ 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.

The consequence of this is that in this respect the social data protection law

must be given priority. Regarding the concrete

context, i.e. the request from the tax office (and securing the tax

arising), is there also a regulation that addresses this topic

subject (§ 71 Para. 1 No. 3 SGB X).

§ 71 paragraph 1 SGB X

A transmission of social data is permitted insofar as it is necessary for the fulfillment

the statutory notification requirements

...

3. to secure tax revenue according to ... Section 111 (1) of the Fiscal Code ...,

to the extent that these provisions are directly applicable, ...

§ 111 para. 1 AO stipulates that all authorities responsible for carrying out the

have to provide administrative assistance required for taxation.

This provision is also in the present case, so the request of a

Tax office, directly applicable, as well as § 71 Abs. 1 Nr. 3 SGB X

required. Direct applicability within the meaning of this provision is only

then not given if not the financial administration of the country, but

Municipalities levy taxes (cf. Rombach in Hauck/Noftz, SGB X,

§ 71 para. 6, 35).

Accordingly, I informed the job center that it was not with

Look at the justification of the tax office, but nevertheless in the result data

is permissible under intellectual property law to comply with the request of the tax office.

37

3.1.3

The use of free text fields in e-meld21 is not permitted

The use of free text fields at e-meld21 is not permitted; existing

Content is to be deleted.

The one offered by ekom21 and at the Hessian registration offices

The data processing program used, e-meld21, has a free text

field, which is commonly referred to as "clerk information".

That such a field can undoubtedly be helpful in processing

for example processing statuses or other processing-relevant

to store information that other users are also aware of

long, seems understandable.

However, this design is problematic against the background of the legal

stipulations in the Federal Registration Act and the fact that the

Free text field, with or without content, part of the data record under reporting law

according to § 3 BMG. There are the possible and legally permissible contents

enumerated catalog-wise and conclusively. It follows that here

no further data may be stored, for which, however, a free text

field opens up an actual possibility. Use of the free text field

must therefore be regarded as inadmissible.

Insofar as a free text field in the data record under reporting law is actually

holds, of course, the right to information also extends according to § 10

BMG on this content, i. H., what is noted there is unreservedly to the

to inform those affected.

3.1.4

Video surveillance in Schwalbach am Taunus

It is not the number of cameras that decides whether a video

Monitoring system according to § 14 paragraph 3 HSOG.

Since the summer of 2017, the construction of a video surveillance system in

Schwalbach am Taunus (market place/centre area) in an advisory capacity

accompanied.

Video surveillance should be used because in the mentioned

rich to register an increased crime rate again and again

was. In addition to damage to commercial properties, there was also a

Arson attack on a pizzeria and attacks on police officers. the

Minality development could be based on data collected by the police from the

police crime statistics can be traced and left the area

appear qualitatively and quantitatively as a crime focus.

First, a temporary police video surveillance system was set up there

installed on the roof of the town hall. By the will of the magistrate

the city of Schwalbach am Taunus and the responsible police headquarters

West Hesse was to replace the temporary police facility with a permanently installed

system must be replaced. This should now no longer alone from the

police, but also by the public order office as a danger prevention authority

of the city of Schwalbach am Taunus. This was possible

since the legal requirements according to § 14 paragraph 3 of the Hessian

Public Order and Safety Act (HSOG) for both

authorities are identical.

Section 14 (3) HSOG

The danger prevention and the police authorities can to avert a danger or if

factual evidence justifying the assumption that criminal offenses are imminent, public

openly observe and record accessible places by means of image transmission. The fact

of monitoring and the name and contact details of the person responsible

to be made recognizable by suitable measures at the earliest possible point in time. Firmly
installed systems must be checked every two years to ensure that they meet the requirements
are still available for your operation. Paragraph 1 sentence 2 and 3 applies accordingly.
The design of the monitoring system was viewed critically. In
In this context, with my participation in April 2018, an in-
training event in the town hall of Schwalbach am Taunus
interested citizens also questions about data protection law
aspects of the video surveillance system.
In particular, it could be clarified that alone the quite high
number of 17 cameras does not mean that video transmission is inadmissible
guard led. The number of cameras used is not of itself
legal relevance and does not provide a parameter for the depth of intervention
The decisive factor is rather the necessity of the individual cameras
with a view to defusing a crime hotspot.
In the present case, the number of cameras was the special building
of the monitored area. It was necessary to avoid that due
areas that cannot be seen due to the somewhat confusing constellation of buildings
develop. Operation and access authorizations could also be clarified.
The now permanently installed system is used by the police and the public order office
operated by the city. Both authorities have access to the video sequences.
Before the final commissioning I have all the camera settings
reviewed and, where necessary, adjustments made. Through

Using appropriate pixelation techniques, I was able to achieve that

Cameras do not output any data even when panning and focusing

so-called private protection zones. A peek into private homes,

on balconies, in gastronomy areas and shops becomes technical

prevented. The collected data (video recordings) are allowed for ten days

stored and can, if necessary, be used as evidence in

averaging procedures are used.

3.2

schools, colleges

3.2.1

Without certificate of good conduct and health information for school attendance

The requirement to present a police clearance certificate and/

or information on the state of health of an applicant is within the scope

of a school's admissions process is not permitted under data protection law.

Through the information of a person concerned, I became aware that

that state adult education schools as part of the admission

a police leadership

request a certificate. A student had gone through an admissions process and

should be used as documents e.g. present a police clearance certificate. Also

Questions about the state of health of the

prospective student. The person concerned regarded the procedure as

disproportionate and not appropriate for the purpose.

The school managements concerned guided the legality of their actions

from a decree as an appendix to the ordinance on the design of the schools

for adults (SfEAusgV). It says:

"An application for admission to a school for adults includes the following

Attach the following documents: 1. Birth certificate, alternatively a copy

of personal documents; a police clearance certificate may be required

become; 2. [...]”.

I consider the specification in the decree referred to to be data protection law

inadmissible because not necessary. I have therefore written to

cash to the issuer, the Hessian Ministry of Education (HKM).

In my letter I found that neither the Hessian

School Act nor the regulation on the processing of personal data

Data at schools contain a norm related to a

Admission procedure for any type of school, the template

requires or provides for information from the Federal Central Register.

Rather, schools are only authorized to collect data from students and

Parents as well as teachers to raise the lawful fulfillment

of the school's upbringing and educational mandate and the associated

related purpose, to carry out school organizational measures

or to fulfill the tasks assigned to them by legal regulations

are required (§ 83 Para. 1 HSchG and § 1 Para. 1 of the Ordinance on

processing of personal data in schools). This includes the template

a certificate of good conduct.

Section 83 (1) HSchG

Schools may collect personal information from students, their parents

and teachers process, insofar as this is necessary for the lawful fulfillment of the

Educational and educational mandate of the school and a purpose associated with it

or to carry out school organizational measures.

Section 11 (1) HDSG

The processing of personal data is permitted if it is for lawful purposes

Fulfillment of the tasks for which the data processing office is responsible and

is required for the respective purpose.

The requirement of a police

Certificate of good conduct inadmissible. The data processing must be

gene purpose may be required. A requirement for the collection of data from

a register, in particular a police clearance certificate

I can not recognize. Even within the framework of the employment relationship

knowledge of employees is the demand of the employer for a

to be interpreted restrictively. The Federal Labor Court in

a judgment of November 17, 2016 on this subject:

"The intervention in the general personal

The employee's right to privacy must also be within the scope of Section 32 (1).

Federal Data Protection Act of weighing up the interests of both parties

stand up to the principle of proportionality."

In my letter I had also insisted that the Minister

rium, already received and usually in the student file

to remove filed certificates of good conduct from it and to deny the documents

returned to those affected or, if this is not possible, destroyed.

After all, I had drawn the attention of the Ministry of Education to

makes that the collection of health-related data

the admission procedure also lacks a legal basis.

The Ministry of Education shares my legal opinion

unrestricted

The Hessian Ministry of Education has criticized my legal position in all

ten points and informed me that remedial measures had been initiated

have. Thus, by decree, all schools were asked to use the

standing "can formulation" in relation to the submission of police

Certificates of good conduct prohibited. In the same context, a

Amendment of the ordinance on the organization of schools for adults

(SfEAusgV) announced. Until they become law, the decree includes a

Application of the "can formulation".

In addition, at a meeting of schools for adult

education verbally explained the future procedure to the school management.

Schools have been instructed to keep all notices and pronouncements

in relation to the submission of police clearance certificates from the

School publications, promotional materials and/or other media

and remove it from all recording documents. Also became

prompts all student files to already submitted certificates of good conduct

scour and return them to those affected, as far as possible

is. Otherwise, there is an obligation to delete the document

or to destroy.

They also agreed on the collection of health data

in my opinion. The Hessian Ministry of Education has towards the

School administrators also clarified that the collection of health data

or questions about the state of health in the course of admission procedures

are inadmissible. Corresponding documents, insofar as these are in student files

are also to be removed and destroyed.

3.2.2

Data protection-compliant design of the tendering process

for the transport of students with health impairments

Hesse

The previous design of the tendering process will not be used in Hesse

uniformly practiced and partially contradicts data protection law

principles. It must therefore be adjusted accordingly.

A petitioner complained to my authority about the publication of

98 student address data as part of a tender process

for student transport. Among other things, he presented the address data

are personal and can therefore be assigned to individual students.

42

Data protection report until 05/24/2018

This complaint was based on the following facts:

In February 2018, a school authority in Hesse published a

open procedure on the Hessian tender database

Call for tenders for school transport for children who are unable to go to school

of the city and suburbs concerned to a school within that city.

The Hessian Tender Database (HAD) describes itself on their

home page as follows:

"The Hessian Tender Database (HAD) is an internet-based,

generally available database for the publication of notices

genes in the context of public procurement procedures. You will be interested

of commercial economy, crafts and freelancers in Hesse

operated in order to make procurement processes in the public sector more competitive

competition, transparency and efficiency.

Due to the close cooperation between ministries, business and

Procurement agencies, the HAD is constantly being further developed in a practical manner. The HAD is not only an announcement platform, but also a free Contact person for all technical, content and legal questions procurement procedure.

The HAD was founded at the end of the 1990s by the Hessen e. V. (ABSt) from participation in the EC project 'Simap-Vergabe-platform' developed. The EC project was discontinued by the European Commission from ABSt Hessen e. V. as a project for the country Hesse continued. HAD has been a free service since 2007 for all Hessian contracting authorities and companies in Europe. Since per Hessian Public Procurement and Tariff Loyalty Act the obligation to publish all national and EU-wide announcements on the HAD, all Hessian announcements can be found in full on the HAD. Furthermore, important procurement regulations, whether guidelines or laws or decrees and other circulars on public procurement law in particular published daily on the HAD for the Hessian administration."

Accordingly, in the context of this call for tenders, in addition to the Name of the school including the school classes attended in the respective students also published their home addresses (district, street, house number). Also was the tender documents to infer the fact that it was impaired health children acted (inability to go to school).

True, the names of the children of the published address list were not can be seen, but at least two of the 98 published were Address data with regard to the surnames of the children concerned

essentially personal. This resulted in a - based on this address list
carried out extensive research. After these two names
could each be assigned to an object (single-family house) and
it had thus become obvious that the fundamental possibility of
If there was a personal reference, the facts were clear.

Due to the legal changes in public procurement law
Orders must include the tender documents both national
as well as Europe-wide in the context of the publication anyone without technical
be made accessible ("accessibility"). any
Access restrictions to the tenders have been lifted. A
a group of addressees selected from the outset, e.g. B. in the present case
Transport company, does not exist (anymore).

Thus, the knowledge of the following personal data was also
possible for third parties not involved in the tendering process: addresses
of the affected children, existence of a health impairment
for these children and the name of the school attended including the
school class of the respective child.

Due to the barrier-free access to this data,
enables companies that do not operate a transport business to
to process the data for your purposes. It would be conceivable here, for example
the offering of product offers by medical supply stores or others
towards the parents of the children concerned, for example by throwing in
Advertising brochures in the mailboxes of the parents' houses.

At the time of the announcement/publication, the Hessian language was still valid

Data Protection Act (HDSG). Since May 25th, 2018 the situation has been resolved

to assess the GDPR.

Both under the old law (§ 7 Para. 4 HDSG) and under the new law (Art. 9

Para. 1 DS-GVO) health data are subject to special protection.

§ 7 paragraph 4 HDSG

Unless a legal provision prohibits the processing of personal data via the

racial and ethnic origin, political opinions, religious or philosophical

beliefs, union membership, health or sex life

provides for or requires as a mandatory requirement, processing may only be carried out in accordance with Sections 33 to 35

and 39

take place. Otherwise, processing based on this law is only permitted if

it is exclusively in the interest of the person concerned and the Hessian data protection

commissioned has been heard in advance.

Art. 9 Para. 1 GDPR

The processing of personal data revealing racial and ethnic

Origin, political opinions, religious or philosophical beliefs or

union membership, as well as the processing of genetic

data, biometric data for the unique identification of a natural person,

Health data or data on sex life or sexual orientation

natural person is prohibited.

The term "health data" does not only include specific medical data

to subsume diagnoses, but rather the fact that

a person has a health impairment, in this

Case of the inability to go to school of the affected children.

Because the personal reference could be produced, this form of

writing is not permitted from a data protection point of view, provided that the

restricted release

1. Both the full address details of the children concerned and

2. the fact that it is a question of health impairments

children acts,

concerned.

I reported this to the school board. Then he informed me

to proceed as follows in the future:

For tenders for transport contracts, it is from the school year

2019/2020 a two-stage tendering procedure according to § 41 of the

delivery guideline notified. The first step is to create a list as an attachment to the

Bill of quantities published, exclusively the street names

(without house numbers) and the number of people expected to be transported

students included. This serves to orient the

essence of the tender. After submitting a confidentiality agreement

the publication then takes place in the second step for the basis of calculation

of the address lists, stating the house numbers, separately to the respective

interested parties in the tender.

I think this procedure is acceptable if there is a need

the students because of their respective health conditions

Impairment to have to pick up immediately at their home address.

traffic, services of general interest

3.3.1

Transmission of consumption values by the network supplier or

network operator to the landlord

The landlord has no claim for surrender against the gas network operator

driver regarding the gas consumption values in the rented supply object.

This year I received a complaint from a landlord who was at

the gas network operator responsible for the area of the rented property

Information under data protection law about the consumption values of the gas meter

coveted for several years. The landlord was the owner of a rented

dead object. Gas consumption was not billed via the

landlord, but was dealt with directly by the gas supplier with the tenant

settled. The gas network operator refused due to data protection law

Reasons for the release, unless the tenant has consented to the transfer

averaging the gas consumption values could be presented.

The gas network operator is responsible for the operation of the gas network

Gas suppliers, on the other hand, for the delivery of the gas. The basic rule is: Den

You can change gas suppliers, but not network operators. The gas supplier

pays the grid operator a fee for grid usage and meters.

The respective gas suppliers transmit the individual gas consumption values

the gas network operator. These are used to calculate the grid usage

fees that the gas supplier has to pay to the gas network operator,

needed. This means that the gas network operator has all the consumption values

for a measuring point. The property owner/landlord is responsible for

the gas network operator responsible for the area is known. The gas company could

- depending on the contractual conditions - by the tenant without the participation of the

be selected by the landlord.

The right to information under data protection law depends on the existence of the personal

personal data of the claimant. According to § 3

Para. 1 BDSG are personal data individual details about personal

or factual circumstances of a specific or identifiable natural

Person. Consumption data can be used to draw conclusions about the heating behavior of the

residents, the periods of their presence and absence and use

of certain rooms, which is why they are personal data

ten are to be considered (also in the judgment of 28.10.2014 of the LG Dortmund,

Az: 9 S 1/14, ZMR 2015, p. 330). The consumption values are personal

Data of the gas consumer and thus of the tenant. Eligible

is therefore the tenant. The landlord cannot provide information from § 34 BDSG

demand because it is not about his personal data.

However, the landlord could demand the consumption values if he is

Request can be based on a data protection law basis. The

Collection, processing and use of personal data according to § 4

Para. 1 BDSG only permissible insofar as this is permitted by law or

orders or the person concerned has consented.

The tenant's consent was not present in this case. Another

legal basis e.g. B. as part of a rental agreement (§ 28 Para. 1 No. 1

BDSG) or due to his legitimate interest of the lessor (§ 28

Para. 1 No. 2 BDSG) was not substantiated by the landlord.

Therefore I did not support the landlord's request and

shared that he has no right to information under data protection law

can make and otherwise no permission for the transmission of the

data was presented.

3.3.2

Modification of the procedure for issuing a so-called

drone license

For the issuance of a certificate as proof of sufficient knowledge

abilities and skills according to § 21a Para. 4 Air Traffic Regulations (so-called

drone license) it is not necessary for the applicant to have a

Sign a statement certifying that for the past five years

neither an investigation by the public prosecutor's office nor a judicial

criminal proceedings against her which did not result in a conviction

was completed.

I received a notice that a competent body for the issuance of

Drone driving licenses from the applicants a "Declaration of

ment procedure" which must be used to confirm that

– you have not had a criminal record,

– there are currently no criminal proceedings against oneself or

preliminary proceedings of the public prosecutor's office are pending and

– against a in the last five years neither a preliminary investigation

the public prosecutor's office nor a judicial criminal procedure, which is not

resulted in punishment has been completed.

Since April 7th, 2017, the ordinance regulating the

Operation of unmanned aerial vehicles from 03/30/2017. She was dated

Federal Ministry of Transport and Digital Infrastructure issued and has

the amendment to the Air Traffic Regulations (LuftVO) and the Air Traffic

Licensing Regulations (LuftVZO) on the subject. Since this year it is

therefore necessary for operators to have a drone license beforehand

they are allowed to control certain types of aircraft. The drone license

is issued after passing an exam. In advance of the exam

provide certain documents. As part of the submission of these documents

Among other things, the present declaration on investigative

procedure required.

According to data protection regulations, the collection of personal

Generic data is only permitted if a legal provision provides for this or

the person concerned has consented. Since the possibility of consent

met was not granted, the collection of those listed above

Data is only permitted if a law or regulation

collection allows.

As such a provision, the competent authority has defined § 21d para. 3

submitted to the Air Regulation.

§ 21d para. 3 LuftVO

The applicant must have reached the age of 16 and have a recognized position

submit the following documents before the examination:

1. a valid identity document,

2. in the case of minors, the consent of the legal representative,

3. a declaration of ongoing investigations or criminal proceedings and

4. a certificate of good conduct according to § 30 paragraph 1 of the Federal Central Register Act, if

he is applying for a certificate for the first time.

The Air Traffic Regulations, which regulate the requirement for a drone license

regulation is a federal regulation and can therefore be used as a data protection

act as a legal basis. However, I pointed this out to the competent authority

out that on § 21d Abs. 3 LuftVO only the submission of a declaration of

ongoing investigations or criminal proceedings and a certificate of good conduct,

which contains the applicant's criminal record, can be supported.

The submission of a self-certification that the applicant has been

five years, neither an investigation by the public prosecutor's office nor

a judicial criminal proceeding that has not resulted in a punishment,

has been completed is not required by the standard.

Further legal bases could not be named, so I

Collection of self-disclosure about completed investigation and criminal

proceeding without a conviction as inadmissible.

The body responsible for issuing drone licenses has changed

then the statement on investigations accordingly, so that the

Self-disclosure on completed investigations and criminal proceedings without

Conviction removed from Investigation Statement. Further

were all applicants from whom the data was unlawfully collected

informed about the legal situation. All declarations already submitted as well as

the associated documents have been deleted.

3.4

healthcare

3.4.1

Access to files at the Hessen Chamber of Psychotherapists (LPPKJP

Hesse)

A member of the LPPKJP Hessen was granted access to a

closed procedure of the Complaints and Arbitration Committee

failed. I took this as an opportunity to take a closer look at the specifications

of the LPPKJP Hessen in this area. As a result, could

be achieved that the member concerned the desired inspection of files

is granted and that the requirements of the LPPKJP Hessen regarding the

File inspection to be revised.

The occasion

A member of the LPPKJP Hessen described to me that there was a complaint

of her patient in 2014, the subject of a proceeding in committee

for complaints and arbitration of the Chamber. The complaint was

finally rejected in 2015 without giving any reason. The

Member asked for access to files the following year for answers to

their open questions - especially with regard to the justification of the

divorce – to obtain. This request was made by the LPPKJP Hessen under

Appeal to the Rules of Procedure of the Board of Appeal of the Chamber

rejected. The rules of procedure do not provide a legal basis for this. The

File was closed and archived. Since I have the attitude of the Chamber

not legally compliant, I am in a dialogue with the Chamber

kicked. The member was then granted partial access. The from

The part of the

File in which the reasons for the decision were recorded

but denied to the member. In particular, it was stated that

that record is not part of the file as it is physically separate from

of the file is attached to the file in a sealed envelope.

In addition, such logs would sometimes contain sensitive third-party data

contain. After all, some of these are verbatim reports

which reference is also made to other similar cases.

Legal Acknowledgment

I have the chamber on the regulations of § 29 HVwVfG and § 18 paragraph 5

HDSG advised.

Section 18 (5) HDSG

Are personal data stored in files that lead to the person concerned

then he can inspect the files designated by him at the storing location

demand. ... Inspection is not permitted if the data of the person concerned with data

Third parties ... are connected in such a way that their separation is not or only disproportionately

great effort is possible. ... Incidentally, information can be granted to him instead of inspection.

Section 29 (1) HVwVfG

The authority must allow those involved to inspect the files relating to the procedure

allow, as far as their knowledge to assert or defend their legal

interests is required. ...

As part of a formal administrative procedure, the regulation on

Right of inspection of § 29 HVwVfG takes precedence over § 18 HDSG (see Dem-

bowski in: Schild/Ronellenfitsch/Arlt/Dembowski/Wellbrock/Müller/Piendl/

Topp/Wehrmann: HDSG, § 18, para. 20, 11/2015). That means that until

Completion of the procedure the parties under the conditions of

§ 29 HVwVfG can assert a right to inspect the files. After

At the end of the procedure, the right to information under § 18 HDSG applies

(Dembowski, loc.cit.). According to this, all those affected whose personal

gene data were processed in the process, for information or inspection

entitled under the conditions of § 18 HDSG.

Since the state regulations are higher-ranking law

acts, I informed the chamber that the very narrow provisions of the articles of incorporation

of the chamber for inspection of files were unlawful and therefore not applicable.

file term

Also the position of the chamber, the "non-public protocol of results"

was not part of the file, was not justifiable in my view.

The complaint file is a personal file of the chamber member

(§ 49 Para. 3 Health Care Professions Act). The data protection term "file"

is legally defined in § 2 Para. 7 HDSG:

§ 2 para. 7 HDSG

A file is any document used to fulfill the task that is not part of the automatic

ted data processing.

The legislature assumes a comprehensive concept of files. The

"Result protocol" gives the content and the result of the consultation of the

shot back to the case in the file. It is used for assessment

of the case and will also be used in the event of any subsequent complaints

kept against the chamber member. It therefore serves the purpose of

performance of the Committee's duties, namely the possible misconduct

of the chamber member to be able to pursue. Should this not be the case,

the record of results would have to be destroyed. The physical separation

of the result log from the file (e.g. through a folder or

a stapler) can be selected from the above reasons not cause this

does not become part of the file in terms of data protection law. Much more

would such a consideration arise from informational self-determination

circumvent the rights to inspect files and information resulting from this right.

Protection of third party data

The Chamber's argument that the "protocols of results" were partially

contain valuable data from third parties, I objected that the legislature

in § 18 para. 5 sentence 3 HDSG I have taken into account exactly such constellations:

§ 18 paragraph 5 sentence 3 HDSG

Inspection is inadmissible if the data of the data subject is combined with data from third parties...

are connected in such a way that their separation is not possible or only with a disproportionately large amount

effort is possible.

A case-by-case examination must always take place here. Allow individual data

cover before inspection or through individual documents for inspection

replace the exchange with partially blackened copies, the

effort are not classified as disproportionate. For that in the case

of the "result protocols" a separation or blackening is out of the question

would come because this involves a disproportionate amount of effort

would be, I saw no clues.

Result

The LPPKJP Hessen also granted the member access to the files

"non-public record of results". The data of uninvolved third parties were

blackened.

In the amended Rules of Procedure of the Complaints Committee and

Arbitration the following change was included:

Section 5 (5) Rules of Procedure of the Complaints and Arbitration Committee

After the procedure before the committee has been completed, it must be ensured that all case-related

gene documents are brought together in the case file maintained by the GS.

The GS secures the file with a seal and keeps the process under lock and key.

File inspection and information rights of those affected or third parties remain unaffected.

3.4.2

Presentation of a new role and authorization concept for

Hospital information system of Klinikum Höchst

A hospital is not a legal entity within which personal

Genetic patient data may be disclosed at will. Also within the

hospital is medical confidentiality within the meaning of the professional code

and the penal code to be observed. The hospital information system

(HIS) is to be designed in such a way that employees in the hospital can only access

on the patient data they actually have for the performance of their duties

require.

The starting point was a data protection incident at Klinikum Höchst in

2016. At that time there was an incident on a ward where a patient

shot around with a pistol and several clinic employees

had hurt. This prompted the clinic management to carry out a precautionary check

of internal access to the electronic patient files of the

affected clinic staff. It turned out that

a whole range of employees – both medical

as well as nursing staff - from different departments

had accessed the medical records of the injured clinic staff.

In response to the incident and to prevent further similar ones

The management of the clinic assured me of events, an extensive one

to adapt the role and authorization concept and

introduce trial controls of access to medical records. this one

I have continued to accompany the process over the past year.

52

Data protection report until 05/24/2018

For handling the patient data of their own hospital employees

There are no special legal regulations for them. For those affected

fenen, however, it is of particular importance that their patient data

remain protected and do not become known to unauthorized persons. Neither

the human resources department may have personally interested colleagues

gins or colleagues should be informed of the treatment data.

In principle, patient data may only be used in the hospital for the purpose

are further processed for which they were collected or stored,

i.e. H. specifically for the implementation of the treatment contract.

In Hesse, the Hessian Hospital Act 2011 (HKHG 2011)

expressly stipulated that in § 12 para. 2 HKHG 2011 specified

legal requirements for the transmission of data accordingly

also for the transfer of patient data within the hospital

apply between specialist departments (§ 12 Para. 3 HKHG 2011).

Access to a patient's data may therefore only be granted to those

house workers who are involved in the treatment

or administer the treatment.

A hospital is not a legal entity within which personal

Genetic patient data may be disclosed at will. Also within the

hospital is medical confidentiality within the meaning of the professional code

and the Criminal Code (“island concept”). So may in particular
a specialist department that does not treat a patient, its detailed
medical data will not be acknowledged unless it accepts
in agreement with the patient, the concomitant or follow-up treatment. The
Administrative staff may only have access to patient data to the extent
this for the fulfillment of his tasks and for the respective purpose within the framework
the implementation of the treatment contract is required. This right
Common specifications are in the design of the access authorizations
of the hospital information system. However, it has to
corresponding role and authorization concept for a hospital
still allow sufficient flexibility due to the complex tasks
(e.g. for emergencies, overcrowding, night shift, relocation, consultation) so as not to
jeopardizing patient safety.

Implementation of the guidance for
Hospital Information Systems (OH HIS)

As an orientation framework for the data protection-compliant design and the
data protection-compliant operation of the HIS, the data protection officer
guidelines prepared by the federal and state governments for health

home information systems (OH KIS) (see also https:// data protection.
hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Orientie-
ungshilfe%20Krankenhausinformationssysteme.pdf). After that it has to
ensure the role and authorization concept and its implementation,
that employees in the clinic only have access to patient data,

that they actually need to fulfill their tasks.

According to the OH KIS, it should be possible in a HIS system for Fallak

ten can be marked if necessary to the effect that the

patient is an employee of the treating hospital and that for

the case file requires special protection. The structure of the role and

Authorization concept should make it possible to access this identification

special access regulations can be linked.

According to the information provided by Klinikum Höchst, the HIS software used

was not previously a software solution that the patient data from

special protection for employees. Thus, as long as the used

Accordingly, KIS does not offer sufficient technical possibilities

appropriate organizational measures are taken to ensure patient

to protect employee data. In addition to raising awareness of

Employees is the logging of the accesses in the HIS and their

regular evaluation of central importance for data protection

right design of the HIS. The log data ultimately serves as well

to prove error-free and proper data processing

and to detect abusive access or access attempts

chen. According to the requirements in the OH KIS, a procedure must be carried out

for regular, suspicion-independent checks as well as in cases of

suspicion of unauthorized access. There are case files

of employees to an appropriate extent.

In the interest of transparency for everyone involved, this is appropriate

Logging and evaluation concept known to the employees

close. In the meantime, a corresponding concept has been developed in the hospital

created and implemented.

As there has been repeated unauthorized access in the past

Patient data came from employees in the clinic, was also

to assume that it is individual employees at the appropriate

There is a lack of sensitivity to data protection. I asked the clinic

to take appropriate measures to raise data protection awareness

to improve employees. The clinic reacted to this and

informative information and circulars sent out. Furthermore are

employees are obliged to attend data protection training regularly

to participate. In addition, department-specific training courses are held

Privacy issues in order to specifics in each work unit

enter into.

In the meantime, the clinic has sent me the first parts of a revised access

concept presented, in which the possibilities of unauthorized access

can be further reduced to patient data:

– To be used in future emergencies despite the restricted access rights

on patient data outside of the actual area of responsibility

to be able to access, an emergency access is set up. Any access

about this function is to be justified by the user and is documented.

A random test and evaluation of the

made accesses.

– Furthermore, the hitherto hospital-wide patient search function was

restricts.

– In order to prevent unauthorized use of the HIS by third parties,

an automatic logoff of the employee from the HIS in the future

prolonged inactivity.

The discussion on some areas is currently not yet over.

So I was promised to continue working on a technically satisfactory one

Implementation of a concept to protect VIPs or employees who

are being treated to work. I will do the related

follow developments.

3.4.3

Inspection of the patient file by heirs and relatives

after the patient's death

In the event of the death of the patient, heirs and relatives have

patients have a right to inspect the patient file of the deceased

under the conditions of § 630g Para. 3 BGB. Again and again

shows, however, that the medical profession and hospitals are not legally secure

deal with the claim.

In the first half of the year, my authority received several complaints

agree that relatives of deceased patients

Access to the patient documentation was denied. In one case

was the sister of a deceased patient, in a

further about the daughter of the deceased. Both appealed to each other

the hospitals on their right from § 630g Abs. 3 BGB as relatives.

An immaterial interest was presented in each case.

§ 630g BGB

(1) Upon request, the patient may immediately inspect the complete information concerning him/her

grant patient records. ...

...

(3) In the event of the patient's death, the rights under paragraphs 1 and 2 apply

Protection of the property interests to his heirs. The same goes for the

next of kin of the patient, insofar as they assert immaterial interests.

The rights are excluded insofar as the inspection of the express or

contrary to the will of the patient.

Access was denied for a variety of reasons.

The hospital made opposite to the sister u. a. claims she is

no "nearest relatives", there would probably be children and the husband

of the deceased sister who would come before her in the order of precedence. Should-

If they had died, the sister would have a right of inspection.

A certificate of inheritance was initially required from the daughter of the deceased.

Should this be submitted to the hospital as proof of inheritance

den, the copy of the file would be sent without further inquiry.

When the daughter, in the absence of a certificate of inheritance, relied on her right as a relative

appealed, she was retorted that the documents could only be suspected

informed consent of the deceased patient.

Such must be proven by her.

The patient's right, standardized in Section 630g of the German Civil Code, to inspect the

According to the explanatory memorandum to the law, the resulting patient file serves to achieve this

his right to informational self-determination (Bundestag printed paper 17/10488,

p. 26). Despite the character of the standard under civil law, it is also

legally relevant.

Regarding the concept of "close relatives", I have taken the position that

by a ranking of the relatives named in the explanatory memorandum

(Spouses, life partners, children, parents, siblings and grandchildren).

to go out. The absence of an express provision as to the order of precedence

speaks for the fact that such is not provided and thus all the next

Relatives equally in the presence of an immaterial interest

are entitled to inspect. This differs from the provision of

§ 630g para. 3 BGB, for example, from the provisions of the Transplantation Act

(TPG), which expressly determines a ranking in § 1a No. 5 and in the

following provisions only speaks of a next of kin

(cf. § 3 para. 3 TPG, § 4 para. 1 and 2 TPG) or § 77 para. 2 StGB, the

also specifies a ranking of the relatives who are entitled to apply. The

The wording of § 630g Para. 3 BGB determines "the next of kin" as

eligible. If the legislature had assumed a ranking,

would have designated "the next of kin" as the beneficiary.

In addition, I pointed out in the second case that the burden of proof for

the treating person bears an opposing will. Not the

Relatives or the heirs must therefore explain and prove that

who or the deceased would have agreed to an insight,

but the treating person must outline and describe

indicate that the inspection of the express or presumed will

opposed to the or of the deceased. This follows from the

Wording of § 630g paragraph 3 sentence 3 BGB and should - taking into account

the protection of the patient in relation to that contained in the patient file

Information also after his death - the principle into account

bear that it normally corresponds to the will of the patient that

after his death, heirs and relatives keep the patient file in accordance with the law

see the defined scope.

The two relatives were then informed by the hospitals

granted. Due to the numerous uncertainties that have come to light in dealing with

with § 630g Abs. 3 BGB I have the questions relevant in the cases

summarized and created an information paper for my homepage

(https://datenschutz.hessen.de/datenschutz/gesundheits-und- sozialwesen/

healthcare/inheritance-inspection-of-patient-files).

3.5

technology, organization

3.5.1

Attack Scenarios Specter and Meltdown:

What do they mean for virtualized environments?

For several years, there has been a sustained trend towards

Virtualization of IT infrastructures and for the relocation of services and

Monitoring applications in the cloud. On January 3rd, 2018, among the

Names Specter and Meltdown two types of attack scenarios on serious

Vulnerabilities in modern processor architectures published. of this

Large scale virtualized environments are affected, so from perspective

of data protection an analysis of possible effects and resulting

risks is essential as a basis for an appropriate risk assessment.

virtualization and cloud computing

Virtualization and cloud computing are two closely related

widespread and popular trends in the context of today's IT landscapes.

Virtualization is often used as the basis for cloud computing
for use. An essential concept of virtualization is the shared
me use of hardware resources while delimiting the
software systems using each other. A software system will
a virtual environment is exclusively made available. Several vir-
ual environments can be based on one and the same hardware platform
be operated in parallel and separately from each other. Through the separation
virtual environments are isolated in such a way that unwanted changes
effects, such as mutual access to data, are prevented.
Such measures will, among other things, the goal of client separation
tracked. From the point of view of the operator of virtualization platforms
hardware resources are used efficiently, especially when
several virtual environments are used on them at the same time.
In addition to economic aspects, this also creates demands
a Green IT fulfills.
The basis of virtualization is a separation into the essential
components host and guest. Above all, an innkeeper takes on the core task of the
management of resources. He provides guests with virtual guest environments
available and takes over the allocation of the available resources
to these guest environments. Guests use the virtual one assigned to them
environment to carry out their tasks. The figure below shows this
Structure schematic.

Guest

Guest

Guest

Guest

Guest-

vicinity

Guest-

vicinity

Guest-

vicinity

Guest-

vicinity

host

resources

Figure: Basic structure of virtualized environments

In practice, there are different types of virtualization. celebrities

Hardware and operating system virtualization are representatives. In the

Hardware virtualization, the host presents the guest with a virtual machine

available as a guest environment, which of these i. i.e. R. initially as Ba-

sis used for installing and configuring an operating system.

Further activities are then carried out according to the intended

intended purpose, such as installation, configuration and commissioning

of services. Operating system virtualization follows the approach of

sharing an operating system between guests. during that

Base operating system or its core is shared, can

components based on it, e.g. B. Libraries, available to guests

are provided and used exclusively by them. The provision of

The guest environment takes the form of a so-called container.

An essential requirement when using virtualization platforms

is, from the point of view of data protection, an unrestricted isolation of the virtual

ell environments among each other. Such isolation is fundamental to

a client separation, which in turn is a prerequisite for data protection

compliant processing of personal data. This applies all the more

more if environments of different users are one and the same

Share hardware platform, for example in the context of the platform of a cloud service

leisters (public cloud). Otherwise there could be potentially incalculable

Risks for guarantee goals, such as availability, integrity, confidentiality

and non-linkability.

roll

In the context of virtualized environments, different roles with

speaking responsibilities into account. These can be

which subdivide the two groups manufacturer and system operator.

The manufacturer group includes those roles that

Provide hardware or software as the basis of virtual architectures.

Accordingly, the group of manufacturers can be further divided into hardware and

Operating system manufacturers and manufacturers of virtualization software

subdivide.

The group of system operators includes platform operators and

Guest-operators summarized. The former put out a combination

hardware and software to provide a virtualization platform

and to operate permanently. The latter use one from the platform operator

virtual environment provided on the basis of its virtualization platform,

to build on this the applications and services desired by him

to provide.

It should be emphasized that quite a few roles of one and the same

actors can be perceived. For example, a company

operate their own virtualization platform (private cloud) and on the basis

provide these services. In this scenario, the company would

both the role of the platform operator and that of the guest operator

take the evening.

Complex IT landscapes

In the previous two chapters, virtual environments and

roles shown. It was focused on a single physical environment and

their hardware resources. Platform operators have in

their respective platform landscape, however, usually over several physical

sic environments. They assign guest environments to these. The amount

the virtual environments made available to a guest and the

Correspondingly, connections between these form a guest landscape.

So far, exactly one guest operator and exactly one

Platform operators assumed. However, this is often the case

not given:

A company can create virtual environments at different corporate

external platform operators, for example in a public cloud.

At the same time, the company itself can operate internally as a platform

appear with their own data center. In the context of public virtualization

tion platforms, there are often situations in which

virtual environments of different guests on the same physical one

be operated in the environment of a cloud service provider.

The result is often complex IT landscapes in practical use

with a multitude of actors in different roles. This

applies in particular to public clouds.

Effects

If an unrestricted client separation of the individual virtual

Environments among themselves as well as in relation to connections between

From the guest's point of view, ensuring these is a focus on one's own

virtual guest landscape sufficient. This is from a safety point of

ten possible because in such a scenario a complete delineation of the

guest environments and landscapes is ensured.

The vulnerabilities exploited by Specter and Meltdown in

modern processor architectures, unauthorized reading of memory

cher areas and thus data on the hardware level is possible. in

refer to the previous explanations of virtualization and

Cloud computing means that the lowest level of the outlined

architectures is affected. At this level, resources are provided

assigned to guest environments on higher levels.

Accordingly, provided that the underlying hardware of the

Weaknesses is affected, basically the danger of spying

of data across the boundaries of guest environments. This applies to

Guest environments provisioned from the same physical environment

be provided. In such a case, the key requirement is isolation

virtual environments among themselves are no longer guaranteed. Additionally

can also be the demarcation between the physical environment on the

on the one hand and the virtual environments on the other.

Conclusions

The risk potential for individual, based on virtual environments

driven method depends on several factors. Basically, to

Exploiting the vulnerabilities the possibility of program code execution

necessary. It should be noted here that the execution is not necessarily

would have to take place within the considered virtual environment. Much more

could, due to the broken isolation, a corresponding one

Program code to be executed in a virtual environment

different virtual environment within the same physical environment

to spy on Virtual environments can therefore be used in risk analysis

and evaluation cannot be viewed in isolation.

In a privately operated or dedicated physical environment

information about their virtual environments is available. For all

these virtual environments must run the risk of program code execution

be viewed and evaluated for spying purposes. Here must from the

assumption that the most vulnerable virtual environment

determines the risk assessment of the remaining environments. In addition,

sen actions are taken to account for relevant changes over time

to be identified and taken into account. This also includes in particular

Changes in the mapping of virtual environments to the underlying

lying physical environments. In the previous scenarios

was implicitly assumed that an attacker could gain access to a

virtual environment to provide the necessary for the spying

execute program code. It should be noted here that such a

Access does not necessarily require an attack on a virtual machine.

A conceivable scenario would also be renting a virtual environment

in a public cloud with the aim of attacking neighboring ones

environments of the same physical environment. a data

A requirement under property law can therefore also include exclusive use

be of dedicated hardware for certain procedures.

In summary, it can be stated that through the publication

vulnerabilities uncovered by Specter and Meltdown are profound

Effects on risk assessments of virtualized environments and

have landscapes. A central requirement of data protection is therefore

the comprehensive and effective isolation of virtual guest environments and

Connections between these are no longer fully met. con

sequences from this arise on all levels of the underlying

architectures and for all actors involved. The Hessian data protection

commissioned issued a press release on January 11, 2018, in which

he has called on all stakeholders to take the necessary measures.

The press release can be downloaded from the website of the Hessian Commissioner

for data protection and freedom of information at https://datenschutz.hessen.

en/press releases/spectre-und-meltdown.

3.5.2

Introduction of the “BAföGdirect” app

Already in the 41st activity report (item 3.3.3.2) and in the 44th activity report

(Section 3.2.1) I have dealt with the Hessian BAföG-/AFBG-Ver-

driving busy. It was one of the most modern processes right from the start

in Germany. However, with the introduction of the “BAföGdirect” app, Hessen

times pioneer. From May 2018, services related to the application for

Services optimized for smartphones and tablets possible.

The company Datagroup IT Solutions GmbH, as a service provider of the HMWK for

the IT specialist procedure (BAföG and AFBG software including operation) as another

Expansion stage of the existing contract since May 2012 at https://www.

bafög-hessen.de existing online application offer an app for BAföG

(students and pupils) and ascent BAföG (AFBG).

The development was accompanied by the HMWK and my employees.

The "BAföGdirekt" app supports the previous features of the online

Application for BAföG and AFBG on smartphone and tablet and was

introduced in Hesse on January 25, 2018.

The mobile app enables the following services:

– The responsible office and its contact details can be determined,

contact can be made directly from the app (through

phone call or email).

– The app contains a “navigation function”. This allows users to

after determining the responsible office directly the route to the visitor

Address depending on the end device used in Google Maps or

Calculate and display Apple Maps.

– The status query on the status of application processing can be carried out passively

gene, in which a status change in the application processing - after

explicit consent by the user during the installation of the

Data protection report until 05/24/2018

App - a push notification is automatically transmitted. this function

can be activated or deactivated by the user at any time.

– Major innovation: Documents can be sent with the

Smartphone or tablet photographed and sent directly and securely to the responsible

tive office to be transmitted. This allows the previously required

Scanning and uploading for a submission in the document upload

portal can be dispensed with. The documents are transferred to the specialist

wear, an important further step on the way to digitization

of administrative services and the electronic file.

The app supports the operating systems iOS (Apple) and Android (google).

This means that 97% of all smartphone owners in Germany can currently do this

use service.

The app is another important contribution to the “Digital Hessen

2020”. The "Hessian BAföG and AFBG procedure (HeBAV)" is in it

Part II named under 3.10.

On the one hand, the existing online offer is expanded to include the

App the further expansion of services for citizens (e-services) and

It contributes to the optimization of administrative processes (e-administration)

because the documents transmitted by the Office directly into the are under construction

existing electronic files can be taken over. It is expected,

that through this contemporary feature the BAföG and AFBG applicants

increasingly addressed and in particular by the mobile function of the

Document transmission will make use of.

Hesse is the first federal state to offer BAföG applicants and

AFBG (students, pupils and participants at

training measures) offers such a service.

3.5.3

Citizens and Business Service Hesse

The Online Access Act stipulates that all administrative services

to be offered over the Internet. An infrastructure building block for

the offers of both the municipalities and the state is the offer

of interoperable user accounts. Here, Hessen builds on the preparatory work of the

Citizens and Business Service Hessen (BUS Hessen).

The requirements of the Online Access Act

The Online Access Act (OZG) of August 14, 2017 came into force on August 18, 2017.

In § 1 Para. 1 OZG, all federal and state authorities are obliged to

their administrative services also electronically within five years (by 2022).

and to make them available via administration portals. According to § 1 paragraph 2 OZG

The federal and state governments must provide their administrative services in a portal network

link together.

§ 3 para. 2 OZG obliges the federal and state governments to provide user accounts in the portal

to provide federal. According to § 7 OZG, the federal and state governments determine public

Bodies that set up and register user accounts.

This shows that an essential goal of the OZG is the provision

of interoperable user accounts for a uniform, convenient and

secure access to administrative services offered online. That's true

for the local, state or federal level.

An OZG implementation catalog is used as the starting point for recording/

Mapping of administrative services to use:

– 575 service bundles to be implemented

divided into 55 life situations and business situation package (each

of these packages contains an average of ten administrative services)

and 1981 services currently to be implemented in Hesse.

The catalog should be continuously updated and updated.

About the Hessian law for the promotion of electronic administration

(Hessian E-Government Act - HEGovG) are also the municipalities

obliged to provide access for the transmission of electronic documents

(§ 1 Para. 1 No. 1 in conjunction with § 3 Para. 1 HEGovG).

§ 3 paragraph 1 HEGovG

Every authority is obliged to provide access for the transmission of electronic documents,

even if they are provided with a qualified electronic signature.

The implementation of the OZG in Hesse

In order to meet the above requirements, the Hessian

state administration etc. the project "Implementation OZG" was launched.

The project is part of the HMDIS as a preliminary project.

In the "Implementation OZG" project, the necessary organizational,

substantive, temporal and financial specifications are drawn up.

These form the basis of a strategy for implementing the OZG by the end

of the year 2022. Main goals and framework conditions of the project

are i.a. The following points:

– Processing of the legal, political and organizational framework

conditions at EU, federal and state level (includes the com-

munen),

– Answering legal questions and questions regarding the data

ten protection in the state and municipalities, e.g. for legal anchoring

of the OZG activities within the framework of the HEGovG.

– The implementation of the individual specialist procedures should be decentralized and

managed by the departments.

– All administrative services i. s.d. OZG are already available and

are based on legal norms, d. H. to a wide range of

Federal laws, state laws, directives and regulations up to

towards municipal statutes and subsidy guidelines in the sense of

administrative regulations.

– Some of the services are already accessible online. In Hessen

this currently applies to 13% of municipal services.

– Responsible for the obligation to comply with data protection regulations

GDPR and the HDSIG when processing personal data

Data is the controller.

– In the public sector, the person responsible for processing the respective data

tending public body within the meaning of Section 2 (1) HDSIG, i.e. as before

e.g. B. the municipality or the ministry. Ultimate responsibility

remains with the authority management or the management according to the DS-GVO

the public body.

The respective responsible persons and processors have a central one

responsibility, especially for

– the lawfulness of the processing of personal data,

– the observance of the procedural rules, d. H. keeping records

Details of the processing activities, reporting and notification obligations

and conducting data protection impact assessments as well

– the technical and organizational measures to protect the

processed data.

When analyzing the initial situation, not least the legal framework

conditions and questions regarding data protection in the state and municipalities

to include Since just providing interoperable user accounts

will be an important component of the system, it was decided

sen, on the preparatory work for the development of the civil and corporate

service (BUS) Hessen.

Development of the Citizens and Business Service (BUS) Hessen

As early as mid-2015, the IT planning council decided in favor of a nationwide

proliferation of service accounts for citizens and businesses

chen. After a thorough examination of the legal framework,

such as the federal EGovG, the HMDIS had in mid-2016

Principles formulated, from which it resulted in particular which data

may be processed for this purpose.

The Hessian state administration then developed the "Digital Hessen" strategy

developed in which i.a. services for citizens and businesses

(e-Services) were examined. The EU regulation on the

direction of a central digital access gate (single digital gateway) and

the draft of the OZG is taken into account. Among the indispensable components

belonged to the identity module "Service account with post box", which as a service

account in BUS-Hessen. At the beginning of 2018, the situation was as follows

represents:

– Interoperable service accounts are held at the country level

and are described as user accounts in the OZG.

– Interoperable service accounts exist in the form: citizen accounts

for individuals or corporate accounts for legal entities.

- Interoperable service accounts have interoperable mailboxes.

– Interoperable service accounts can be transferred to a payment service provider

to be connected.

– Interoperability has been successfully tested.

– The interoperable service account Hessen uses the technology developed by

provided to the data center AKDB of the Bavarian municipalities

and will be installed on the ekom21.

– A cooperation agreement with the federal government/Bavaria/Hesse has been concluded.

Below is a sample pre-check for the service account

carried out and a model list of procedures drawn up. These were mine

presented. Following my comments, prior checking has been revised.

Potential users, namely citizens (currently in Hesse approx.

5 million) and companies (currently around 260,000 in Hesse), according to § 3

OZG and § 3 Abs. 4 HEGovG user accounts (formerly called service account)

can set up. A core data record is stored – once – which

when using the administrative services

(once-only principle).

The various public bodies should be able to access the

access the user account and the data required for a specialized procedure

access if they are authorized to do so.

According to § 7 paragraph 1 OZG, the federal and state governments each determine a public one

Place that allows users to set up a user account in the portal network

offers. After determining the BMI, this is not the only responsibility

for the technical setup and provision of the user account

meant, but also the data protection responsibility for this

Account.

§ 7 paragraph 1 OZG says, among other things: assumes that the federal and state

agreed bodies are responsible for compliance with data protection

bear as far as the user account is concerned. From this determination can

the EGovG of the countries do not deviate effectively, since the OZG in this regard

is also binding for the countries. In Hesse, the ekom21 was called this

position determined.

Technical integration of the user account/service account

in BUS Hessen

Management service providers authorized to retrieve data are provided by the

ekom21 – KGRZ Hessen, each stating from

– EntityID,

– return address,

– X509 certificate

checked, registered and set up.

Depending on the data required for the service, only the data required for this

required attributes for data retrieval provided.

The technical process of data retrieval is as follows:

Legend:

FC:

FS:

NKC:

NCS:

FSID:

Specialist Procedures Client

Specialist Procedures Server

User Account Client

User Account Server

ID of the specialized procedure/service

Communication channels:

1 Access to the website of the service by an external party (e.g. a citizen)

2a Retrieval of the page from the specialist procedure server

2b Return of the necessary information about the specialist procedure

(administrative service) necessary attributes from user account and transfer

aktionsID/procedureID and transmission of the necessary authentication

ornament level

3 Calling up the login page of the user account (call up in a popup or in

a separate page) and transfer of the transaction ID/procedure ID

and the necessary attributes

4 Validation of the login data against the user account

5 Return of the transaction ID/procedure ID and the necessary attributes

6 Calling up the specialist procedure server with transfer of transaction ID/procedure

rensID and the requested attributes

The processes mean that every citizen can choose to

decide whether he would like to use the user account.

Data protection report until 05/24/2018

Conclusion

This creates the conditions for portals with a

to use data protection-compliant proof of identity.

3.6

Labor statistics (until May 24, 2018)

3.6.1

submissions and consultations

The activities of practically all of my employees (Ge-

office, IT department and legal departments) was widely

from the preparations started in 2017 to meet the requirements of the

European data protection reform.

In-house, individual working groups examined more than 35 sub-projects

specific topics of the GDPR for their effects in the administrative

execution. The task of the individual working groups was, in particular, to

work, which legal, technical and/or organizational

Measures had to be taken to prepare for the new law. On

In this way, initial application and understanding questions from

responsible data processors, internal data protection officers,

citizens as well as inquiries from politicians and the media

be answered reliably.

In many working sessions, not only within the authorities, but also on

State, federal and EU level, interpretation, coordination and organizational

tion issues are discussed and clarified if possible, opinion-forming processes

initiated and orientation aids or guidelines laid down by the deadline

of the DS-GVO first results for a uniform application of the DS-GVO

to be able to present. The necessary organizational requirements,

such as B. Introduction of a deadline system, renewal of the homepage with

Providing electronic access for privacy complaints

and data protection glitches, could be implemented on time. On the

Numerous articles and application notes (e.g. from

the school sector or health care) in order to use

to offer an initial orientation. These preparatory measures

took place alongside the day-to-day specialist work. As for the latter, it was

the number of complaints and requests for advice received in the

similar to last year for the first few months. Until the key date 05/25/2018

the statistics did not deviate significantly, despite initial inquiries about the GDPR

from 2017 onwards.

The following table contains information on the number of inputs and

Consultation requests are presented, which, in addition to the processing of fundamental

gen, statements on legislative projects and market observation in the

area of IT products make up a significant part of my work.

The statistics are largely automated with the help of the deployed

created a document management system. The number of phone calls

gave and deliberations that took more than 10 minutes to complete, however

were not reflected in files, were derived from the average data

of November 2017, as there are no significant deviations

could be determined.

The slightly increased number of written docu-

deliberations in the first half of the year showed the first signs that

that already some data controllers in the public

and non-public areas, the explosiveness of the forthcoming changes in the law

recognized.

However, the actual extent was underestimated by many. suddenly

attention changed on May 25, 2018, the day on which the

GDPR came into effect.

70

(E= submission/complaint, B = advice)

Data protection report until 05/24/2018

Area of Expertise

Housing, rent, neighborhood

Credit bureaus and collection agencies

take

Schools, colleges, archives

electronic communication,

Internet

Employee data protection

municipalities

address trading, advertising

health, care

credit industry

social

police, criminal proceedings, judiciary,

defense of Constitution

Traffic

Trade, crafts, trade

IT security, data processing technology and

Manufacturer Inquiries

Company/official DPO

utilities

Associations and associations

insurances

Data protection outside DE/EU

Radio, television, press

research, statistics

taxation

Aliens Law

Other topics < 10

(e.g. religions and beliefs

communities, agriculture and

forests, geodata)

Total documented

submissions and consultations

of which total documented

ten inputs (excluding taxes)

of which total documented

ten consultations

including submissions and consultations

Regarding video surveillance

plus sum of telephone

consultations

Total inputs and

consultations

Number 2017

in total

(E+B)

328

number to

05/24/2018

(E+B)

148

number from

05/25/2018

(E+B)

248

Number 2018

in total

(E+B)

396

205

189

168

163

148

130

112

102

95

92

71

67

51

34

32

32

27

23

18

14

10

10

68

2.189

2,001

188

260

5,808

7,997

118

78

120

59

52

71

142

54

40

104

39

30

30

4

48

16

17

0

4

10

4

0

33

1.221

881

340

113

2,420

3,641

533

296

414

197

172

161

397

178

62

153

134

275

54

468

76

323

35

5

21

4

7

2

141

4,356

2.171

2.185

71

only June

1,703

July to Dec

3,036

9,095

651

374

534

256

224

232

539

232

102

257

173

305

84

472

124

339

52

5

24

14

11

2

174

5,577

3,052

2,525

184

7.159

12,736

71

In some areas, the number of submissions (complaints) rose sharply

to multiples (credit agencies, electronic communication, trade, etc.). In

other areas (internal data protection officers, schools, municipalities

organizations, clubs) my advice was in greater demand. In retrospect

I have to get the impression that only a few companies, associations

ne, retailers and traders etc. - but also public authorities and

facilities – were even remotely aware of the requirements

the DS-GVO would place on them.

The above overview shows the quantities up to May 24th, 2018.

3.6.2

sanctions

In the reporting period, a total of 53 administrative offense proceedings,

where violations of the BDSG a. F. underlying, completed.

This was despite the associated with the entry into force of the DS-GVO

significant workload much of the backlog from previous years

finally processed.

A total of eleven procedures resulted in a fine or

Warning (§ 56 OWiG) ended and fines or warning money

set at EUR 17,100. Four old cases were able to

reasons before 05/25/2018 can no longer be processed conclusively.

The infringements were subject to the fines of the

BDSG a. F., under the regime of the DS-GVO these are no longer

threatened with a fine. In the cases concerned, the change in

The legal situation means that the law on the time of the crime (BDSG a. F.) due to the in

Section 4(3) OWiG no longer standardized the principle of most-favoured-nation treatment

could be applied. These administrative offense proceedings had to

therefore be discontinued.

Apart from that, the completed proceedings mainly related to violations

against the facts of § 43 paragraph 1 and paragraph 2 BDSG a. F. perish. It

were violations of the obligation to provide information to those affected or

the supervisory authority and against the obligation to order a data

protection officer punished. Furthermore, numerous procedures related

to incidents related to unauthorized data collection or

-processing. There were no exceptional cases.

3.6.3

Information obligation according to § 42a BDSG

From January 1st, 2018 to May 24th, 2018 there were 51 reports according to § 42a

BDSG old version. Of these, 19 were so-called suspected cases after the

were not to be reported under the legal situation at the time, and 32 justified reports.

Facts of unlawful acquisition of knowledge

Theft of account records/customer records

Incorrect transmission of account data to third parties

Wrong delivery of mail with account data

Wrong sending of an e-mail with personal data of various customers

Theft of laptops with customer data

Theft Electronic Cash Terminal

Wrong dispatch of post with personal data according to § 3 Abs. 9 BDSG

Transmission of personal data to unauthorized third parties

Wrong mailing of letters with health data

Total number of justified reports

Number

3

2

6

1

1

11

3

3

2

32

For comparison: From May 25, 2018 to December 31, 2018, 630 data protection

reported violations according to Art. 33 DS-GVO; see also Section 4.11.3

and 4.11.4.

73

74

Data protection report from 05/25/2018

4. Data protection report from 05/25/2018

(according to DS-GVO, BDSG new, HDSIG)

Data protection report from 05/25/2018

4.1

Cross-cutting issues of the GDPR

4.1.1

On the scope of the right to information under Article 15 GDPR

A claim to the release of individual copies - e.g. B. in the sense of a

Photocopy of certain documents - contains Art. 15 Para. 3 DS-GVO in all

Rule not: the obligation to provide a copy is not included

a general right of access to information or a file

equate right of access.

Nevertheless, in individual cases, those responsible can also send a

be required to photocopy a specific document. Then he can do this

be the case if the right of the person concerned, the legality of the data

checking processing independently is inextricably linked to this.

Art. 15 GDPR

(1) The data subject has the right to receive confirmation from the person responsible

to request whether personal data concerning them is being processed;

if this is the case, you have the right to information about this personal data

and the following information:

a) the processing purposes;

b) the categories of personal data being processed;

c) the recipients or categories of recipients to whom the personal

related data have been disclosed or will be disclosed, in particular

especially for recipients in third countries or international organizations;

if possible, the planned duration for which the personal data will be stored

or, if that is not possible, the criteria for determining them

Duration;

d)

e) the existence of a right to rectification or erasure of data concerning them

personal data or restriction of processing by the

controller or a right to object to this processing;

the existence of a right of appeal to a supervisory authority;

f)

g) if the personal data were not collected from the data subject

all available information about the origin of the data;

h) the existence of automated decision-making including profiling

according to Article 22 paragraphs 1 and 4 and - at least in these cases - meaningful

Information about the logic involved as well as the scope and the desired ones

Effects of such processing on the data subject.

(2) If personal data is sent to a third country or to an international organization

sation, the data subject has the right to be informed of the appropriate guarantees

to be informed in accordance with Article 46 in relation to the transfer.

(3) The person responsible shall provide a copy of the personal data that is the subject
processing are available. For all further copies made by the data subject
requested, the person responsible can charge an appropriate fee on the basis of
require administration costs. If the data subject submits the application electronically,
the information must be made available in a common electronic format,
unless otherwise stated.
(4) The right to obtain a copy under paragraph 3 shall not prejudice the rights and freedoms of others
not affect people.
In recent months, my authority has received an increasing number of inquiries that
with the right to information according to Art. 15 DS-GVO and in particular
deal with the scope of the regulation of Art. 15 Para. 3 DS-GVO.
If those affected assert their right to information under Art. 15 DS-GVO, they are
According to Art. 15 Para. 3 DS-GVO, those responsible are also obliged to
“Copy of the personal data that is the subject of the processing
are” to make available. It must therefore be clarified on the one hand whether Art. 15
Para. 3 DS-GVO in synopsis with Art. 15 Para. 4 DS-GVO an own
permanent right of the persons concerned in addition to Art. 15 Para. 1 DS-GVO
person justified. On the other hand, there is the question of interpretation – and
ultimately the range – the copy concept.
Importance of the right to information
The right to information of Art. 15 DS-GVO pursues in data protection
different objectives: It follows from recital 63 that data subjects
by exercising the right of access, awareness of the processing
obtain and be enabled to access their personal data
should be able to check the legality of the data processing.
In addition, Art. 15 DS-GVO can pave the way for the exercise of further

data protection design rights, such as B. Right to Rectification

according to Art. 16 DS-GVO or right to deletion according to Art. 17 DS-GVO,

prepare or serve to assert claims for damages.

The right to information comes into play when enforcing the right to information

functional self-determination is therefore of crucial importance.

76

Data protection report from 05/25/2018

Scope of the right to information according to Art. 15 Para. 1 DS-GVO

According to the importance of the right to information, Art. 15 Para. 1 DS-GVO

states that the data subject has the right to obtain a

To request confirmation as to whether personal data relating to you

data are processed. If those responsible agree to the processing of personal

personal data, the data subject is entitled to the rights specified in Art. 15 Para

lit. a to h DS-GVO and paragraph 2 DS-GVO more detailed information

to provide.

No extension of the right to information according to Art. 15 Para. 3 DS-GVO

Art. 15 Para. 3 DS-GVO obliges those responsible to “make a copy

of the personal data that are the subject of the processing".

To make available. In addition, Art. 15 Para. 4 DS-GVO speaks of

"Right to obtain a copy". Therefore it is represented that it is a

content expansion in the sense of an independent publication right

against the right to information contained in Art. 15 Para. 1 DS-GVO.

I am of the opinion that Art. 15 Para. 3 and 4 DS-GVO does not depend on Art. 15

Para. 1 DS-GVO is a separate right. Those responsible must be the person specified in Art. 15

Para. 3 DS-GVO therefore also without a corresponding obligation

Comply with the notice of those affected. The wording of Art. 15 speaks for this

Para. 3 GDPR. According to this, the person concerned is given a copy of the personal

to provide gene data that are the subject of the processing

are. Art. 15 (3) GDPR specifies the wording of Art. 15 in this respect

Paragraph 1 lit. b GDPR: The data subjects are not only aware of the categories of personal

personal data being processed, but theirs

provide specific personal information. Art. 15 Para. 3 GDPR

thus clarifies the regulation contained in Art. 15 (1) lit. b GDPR

Scope of the right to information and determines the manner (copy) of

Provision of information.

Furthermore, it should be noted that the European legislator

Those affected not only have the right to information contained in Art. 15 DS-GVO

granted, but with the right to data portability in Art. 20 DS-

GMO has its own claim for surrender in favor of those affected

founds. While the right to information gives those affected the opportunity

to check the lawfulness of the data processing, and this with it

if necessary, only enabled to exercise further data protection rights

(e.g. rectification or erasure), it shall be the right

to data portability make it easier for those affected to know about their data

available (e.g. by moving to another IT environment or by

transmission/provision of a copy of an existing dataset).

It is therefore not apparent why Art. 15 Para. 3, 4 DS-GVO is a

Art. 20 DS-GVO should justify the right of surrender.

The general standards of the

Art. 12 GDPR. The information must be precise, transparent, understandable and

be easily accessible in clear and simple language. The

"Fed off" by providing copies without comment is fundamental

not permitted. It follows that Art. 15 Para. 3 DS-GVO is not an additional

Right to receive a copy of the personal data means,

but requires that the right to information according to Art. 15 Para. 1 DS-

GVO the provision of a copy is sufficient. The right from Art. 15 Para. 4

DS-GVO does not go further than the required rights under Art. 15

Para. 1 and Para. 3 GDPR.

No general right of access to information/

right to inspect files

Due to the wording of Art. 15 Para. 3 DS-GVO "Copy of personal

data that are the subject of the processing", arises for responsible

verbatim and those affected raise the question of the scope of the right to information.

If one deals with the meaning of the term "copy", one finds

e.g. B. the following definitions of terms: "Copy, duplicate of a document,

photocopy, imitation". The understanding of what is stated in Art. 15 is therefore decisive

Para. 3 DS-GVO used copy term.

If in the "Copy of personal data that is the subject of the

processing", the duplication of a document or a photocopy is understood

den (hereinafter referred to as "copy"), this would result in

Affected persons according to Art. 15 Para. 3 DS-GVO e.g. B. a general claim

the transmission of all e-mail correspondence conducted, provided that

personal data contained therein.

I understand the copy concept of Art. 15 Para. 3 DS-GVO in the sense of a

meaningfully structured summary. The person concerned must therefore

copies of all documents relating to them have not been made available

become.

Art. 15 Para. 3 DS-GVO only regulates the type of information

Issuance and has a serving function in relation to Art. 15 Para. 1 DS-GVO:

The person concerned is once again - by providing a structured

Summary of your personal data – recognizable in context

made, which personal data is processed by the person responsible

become.

78

Data protection report from 05/25/2018

This also corresponds to the assessment of Art. 12 Para. 1 DS-GVO, according to which the

Responsible through appropriate measures all communications relating to

refer to the processing, in a more precise, transparent, understandable and easy

accessible form in clear and plain language.

Art. 12 GDPR

(1) The person responsible shall take appropriate measures to provide the data subject with all information

ments pursuant to Articles 13 and 14 and all communications pursuant to Articles 15 to 22 and

Article 34, related to the processing, in more precise, transparent, understandable

and in an easily accessible form, using clear and plain language; this applies

especially for information specifically aimed at children. The transmission of

Information is provided in writing or in another form, possibly also electronically.

If requested by the data subject, the information can be given orally,

if the identity of the data subject has been proven in some other way.

(2) The controller makes it easier for the data subject to exercise their rights

in accordance with Articles 15 to 22. In the cases referred to in Article 11(2),

the controller will only refuse based on the request of the data subject

exercise their rights under Articles 15 to 22 to take action if credible

makes it impossible to identify the data subject.

(3) The person responsible shall provide the data subject with information on the request

measures taken in accordance with Articles 15 to 22 without undue delay, but in any event

available within one month of receipt of the application. This deadline can

Another two months can be extended if this takes into account the complexity

and the number of applications required. The person responsible informs the person concerned

Person within one month of receipt of the request for an extension of time,

along with the reasons for the delay. The data subject submits the request

electronically, it should be informed electronically if possible

she says nothing else.

(4) If the person responsible does not act upon the request of the data subject,

he shall inform the data subject without delay, but at the latest within one

month after receipt of the application about the reasons for this and about the possibility of

to lodge a complaint with a supervisory authority or a judicial remedy

to insert

(5) Information pursuant to Articles 13 and 14 and all notifications and actions

according to Articles 15 to 22 and Article 34 are provided free of charge.

In the case of manifestly unfounded or - especially in the case of frequent repetition -

excessive requests from a data subject, the controller may either

a) demand a reasonable fee, in which the administrative costs for the company

establishment or notification or implementation of the requested action

be taken into account, or

b) refuse to act on the application.

The controller has evidence of the manifestly unfounded or excessive

character of the application.

...

The importance of the right to information is also fully taken into account

carried. Because those affected are thereby put in a position to

to become aware of the processing of their personal data and

to check the lawfulness of the data processing. You can theirs

exercise design rights under data protection law and - if they are

see hurt in this – e.g. B. assert claims for damages or

exercise their right to lodge a complaint with a supervisory authority.

Providing a structured summary is also consistent

the aim of the DS-GVO, natural persons in the processing of their personal

to protect personal data, see Article 1 (1) GDPR. Will he

The copy term of Art. 15 Para. 3 DS-GVO is generally interpreted broadly, see above

there is a risk that the right to information of Art. 15 DS-GVO as all

common right of access to information or as a right to inspect files

is understood, with the result that the assertion of Art. 15 DS-

GVO not to pursue data protection goals within the meaning of the DS-GVO,

but is misused to achieve other goals.

Finally, understanding the term as a structured

Summary also of the assessment contained in Art. 15 Para. 4 DS-GVO.

According to this, the right to receive a copy pursuant to paragraph 3 shall entitle the rights and

Do not interfere with the freedoms of other people. Become those affected

Copies of papers or documents made available, so can

If care is not taken, the risk increases that the person concerned will too

information is made available that may

affect third parties. On the other hand, those responsible produce a structured one

Summary and carry the personal data of

If those affected work together independently, this risk is significantly reduced.

4.1.2

Handling of the right to information according to Art. 15 DS-GVO in the area

of employee data protection

Scope and manner of providing information in the employment

ratio are defined by the person responsible in a synopsis of Art. 15

Para. 1 and Para. 3 DS-GVO to be determined in individual cases. Depending on the circumstances

the information can be provided through a structured summary of the data,

which are the subject of the processing, or a copy. Go

Responsible from the existence of the conditions of a restriction

of the right to information, those affected must be informed of this.

An employment relationship involves a large number of personal

related data processing justified. Therefore,

Data protection officers and those responsible contact me if on the part of

Employed requests for information have been asserted. As examples per-

Son-related data processing comes to the management of the personnel file

or the use of a personnel information system, the implementation of

Personnel development measures, time recording or video surveillance

under consideration. In addition, employees emit under consideration

their work, personal data, for example when using the

provided IT infrastructure (PC, laptop, mobile phone, tablet)

or business communication (creation of documents or

communication via e-mail). Since the employment relationship naturally

a certain duration is created, this data may overflow

for years and decades.

With a view to Art. 15 GDPR, I recommend those responsible and data

protection officer the following:

If those affected assert their right to information under Art. 15 DS-GVO,

is fundamentally detached from the exercise of the right to receive a

Copy according to Art. 15 Para. 3 DS-GVO also a structured summary

to provide the personal data that is the subject

of processing. Art. 15 para. 3 GDPR supplements and modifies this

Right to information of Art. 15 Para. 1 DS-GVO and is in particular before the

Background of the transparency anchored in Art. 5 Para. 1 lit. a, 12 DS-GVO

to implement the principle (see also the article, Section 4.1.1).

Which approach seems particularly suitable depends on

of the data processing to be assessed, and therefore of the circumstances of the

on a case-by-case basis.

In the following constellations I have assumed that the requirement

requirements of Art. 15 Para. 3 DS-GVO are met:

– Provision of an excerpt of the profile of those affected when used

of a personnel information system by responsible persons

– List of documents or file numbers stored for a person

when using a document management or filing system

If, with reference to Art. 15 Para. 3 DS-GVO, the copy of individual written

pieces or e-mail correspondence is requested, this claim

then exist if the right of those concerned, the legality of

to check data processing independently, inseparably linked to this

the is. In a synopsis of Art. 15 Para. 1 and 3 DS-GVO and

against the background of the importance of the right to information, it is likely to

my understanding usually suffice if the persons concerned have the in

personal data contained in a document are communicated.

81

The Hessian Commissioner for Data Protection

47th activity report on data protection

However, the copy of a document/e-mail is usually not required

to provide.

Art. 15 para. 4 DS-GVO and recital 63 provide that the right

on receipt of a copy the rights and freedoms of other persons, such as

trade secrets or intellectual property rights and in particular

which may not interfere with the copyright of software. This may

according to recital 63, however, does not lead to the affected

person is denied any information. Art. 23 GDPR also enables this

Restrictions on the right of access by Member States. In German-

Land was informed of this possibility in Sections 27 (2), 28 (2), 29 (1).

Clause 2 and 34 BDSG used.

Art. 23 GDPR

(1) By legal provisions of the Union or the Member States to which the responsible

liche or the processor is subject to, the obligations and rights under the

Articles 12 to 22 and Article 34 and Article 5, insofar as the provisions of

comply with the rights and obligations provided for in Articles 12 to 22, by way of

Legislative measures are limited, provided that such a limitation

respects the essence of fundamental rights and freedoms and in a democratic

society constitutes a necessary and proportionate measure that:

ensures:

a) national security;

b) national defence;

c) public security;

d) the prevention, investigation, detection or prosecution of criminal offenses or criminal

enforcement, including protection against and defense against threats to the

public safety;

e) the protection of other important objectives of general public interest

Union or a Member State, in particular an important economic or

financial interests of the Union or a Member State, for example in monetary,

budget and taxation, as well as in the field of public health and

social security;

the protection of the independence of the judiciary and the protection of judicial processes;

f)

g) the prevention, detection, investigation and prosecution of violations of the

professional rules of regulated professions;

h) Control, monitoring and regulatory functions that are permanently or temporarily associated with

the exercise of public authority for those under letters a, b, c, d, e and g

mentioned purposes;

the protection of the data subject or the rights and freedoms of others;

the enforcement of civil claims.

i)

j)

(2) Any legislative measure within the meaning of paragraph 1 must in particular

also contain specific provisions at least in relation to

a) the purposes of the processing or the processing categories,

b) the categories of personal data,

c) the extent of the restrictions imposed,

d) the guarantees against abuse or unlawful access or unlawful

Transmission,

e) information about the person responsible or the categories of person responsible,

f)

the respective storage periods and the applicable guarantees, taking into account

the type, scope and purposes of the processing or the processing categories,

g) the risks to the rights and freedoms of data subjects and

h) the right of data subjects to be informed of the restriction, where

this is not detrimental to the purpose of the restriction.

§ 34 BDSG

(1) The right of access of the data subject pursuant to Article 15 of Regulation (EU)

2016/679 exists in addition to those in § 27 paragraph 2, § 28 paragraph 2 and § 29 paragraph 1

Sentence 2 mentioned exceptions not if

1. the data subject pursuant to Section 33 subsection 1 number 1, number 2 letter b or

Paragraph 3 is not to be informed, or

2. the data

a) are only stored because they are required by law or by the articles of association

Retention rules must not be deleted, or

b) are used exclusively for data backup or data protection control purposes

and the provision of information would require a disproportionate effort

as well as processing for other purposes through appropriate technical and

organizational measures are excluded.

(2) The reasons for the refusal to provide information must be documented. The rejection of

The provision of information must be justified to the person concerned, unless by

the notification of the factual and legal grounds on which the decision is based

the purpose pursued by the refusal to provide information would be endangered. The for the purpose

the provision of information to the data subject and for their preparation

Data may only be processed for this purpose and for data protection control purposes

become; for other purposes, processing is permitted in accordance with Article 18 of the Ordinance

Regulation (EU) 2016/679.

(3) If the data subject is not informed by a public agency of the Federation

issued, it shall be issued to the Federal Commissioner upon request, to the extent that

the competent supreme federal authority does not determine in the individual case that this

federal or state security would be jeopardized. The notification of the

Federal Commissioner to the person concerned about the result of the data protection law

The examination must not allow any conclusions to be drawn about the level of knowledge of the person responsible,

unless the latter agrees to further information.

(4) The data subject's right to information about personal data collected by

a public body neither processed automatically nor processed automatically

and stored in a file system only exists to the extent that the data subject

provides information that enables the data to be located and for the issuance of the

Information required effort not disproportionate to that of the data subject

asserted interest in information.

If responsible persons of the existence of the conditions of a restriction

effect of the right to information, the data subjects are also entitled to do so
inform. This is both Art. 12 Para. 4 GDPR and Section 34 Para. 2
BDSG. Because only on the basis of appropriate information
the data subject has the opportunity to challenge the lawfulness of the refusal
to check the right to information. Corresponding explanations are missing
of the person responsible is not the right of access of the data subject
enough done.

According to Art. 12 Para. 5 GDPR, the information to be provided is free of charge
to provide. However, if requests for information are obvious
are unfounded (very rare) or – especially in the case of more frequent
Repetition - a data subject in an excessive manner disclosure
submits applications to those responsible, they can charge an appropriate fee
request, taking into account the administrative costs of the notification
become. Alternatively, those responsible can refuse to
to take action on future applications.

Do those responsible assume that the requirements of Art. 12
Para. 5 DS-GVO are fulfilled, the data subjects have to do so in accordance with Art. 12
Para. 4 DS-GVO to be informed.

It should also be noted that according to Art. 12 Para. 5 DS-GVO, responsibility
liche evidence of the manifestly unfounded or excessive
character of the application have to be provided. Carry those responsible
hence the burden of proof.

Pursuant to recital 63 sentence 7 of the GDPR, those responsible can
demand that those affected specify their request for information if a
large amount of information about the data subjects is stored. This
is to be assumed for data processing in the employment relationship, since

here, as mentioned at the beginning, on a large scale and over a long period of

room personal data accrue.

Against the background of the factually varied personal

Son-related data in the employment relationship, the principle of

Transparency (which in Art. 12 Para. 1 DS-GVO in particular also includes a precise,

understandable form and clear and simple language), protection

of the rights of third parties, the gratuitousness of the request for information, the

Art. 12 Para. 5 DS-GVO provides for the possibility of preventing abuse

by those responsible and the clarification idea of the recital

84

Data protection report from 05/25/2018

reason 63 DS-GVO should when asserting requests for information

The following aspects must be taken into account in the employment relationship:

– The data subjects are provided with the information in accordance with Article 15 (1) lit. a bis

h GDPR made available.

– The person concerned will (at the discretion of the person responsible and in particular

especially against the background of creating transparency according to Art. 12

DS-GVO) structured summaries (e.g. extract from the registry) or

Copies are provided for all data processing operations that

be processed to your person.

– Are structured summaries or copies with reference to

existing rights of third parties are rejected, this is the person concerned

communicate transparently. This also applies to other restrictions

the right to information.

- If personal data of the persons concerned in data processing

are stored that are not used for the processing of employee data

n, but other purposes (e.g. processing of customer data) and

are therefore not processed in relation to the claimant is sufficient

it if those responsible have the information according to Article 15 Paragraph 1 lit. a bis

h DS-GVO and give those affected the opportunity

allow you to clarify your request for information.

4.1.3

Obligation to report data protection officers according to Art. 37

Para. 7 GDPR

Due to the European data protection reform, Hessian responsible

lic and processors since May 25, 2018 in accordance with Art. 37 Para. 7 DS-GVO

obliged to provide the contact details of the data protection officer

Notify the Hessian Commissioner for Data Protection and Freedom of Information.

Violations of the obligation to notify the competent supervisory authority

can be punished with a fine.

The Hessian Commissioner for Data Protection is responsible for processing the reporting obligation

and Freedom of Information (HBDI) introduced an online reporting process that

at https://datenschutz.hessen.de/service/benannenung-eines-datenschutzbe-

is to be reached. The implementation of the online reporting form

took place on May 14, 2018. Since then, around 15,000 reports have

13,470 positions were received.

In addition to all public bodies that, according to Art. 37 Para. 1a, 4 DS-GVO i. V. m.

§ 5 para. 1 HDSIG the office of the data protection officer and the deputy

treters must fill and the named persons via the registration portal

have to report, are also other responsible persons and processors
to appoint and report a data protection officer
obligated. In addition to the requirements of Art. 37 Para. 1 DS-GVO
Responsible persons and processors the regulations of § 38 paragraph 1
BDSG to take into account. After that, those responsible and commissioned
processor to appoint a data protection officer if
at least ten people regularly with the automated processing
personal data are engaged.
Despite the high number of reports already received,
of that a variety of controllers, processors and
public authorities in Hessen of their obligation to report
has not complied. This omission must be rectified immediately.
The HBDI regularly checks as part of the processing of transactions
also whether the obligation to report has been complied with. If not, will
this circumstance in the context of the decision on necessary measures
taken into account and can therefore also lead to the imposition of fines
lead (see also Section 4.11.2).

4.1.4

Acknowledgment of information according to Art. 13 and Art. 14 GDPR

The duty of the controller to inform the data subject about the data processing
to inform does not lead to an obligation of the person concerned to receive it
to acknowledge the information with a signature.
A citizen contacted my office and complained that
that a municipality asked him to receive the information
Art. 13 DS-GVO to be confirmed by his signature. Neither Art. 13 nor
Art. 14 DS-GVO see such a confirmation by the recipient

of the information. The municipality took the position that

only through the signature of the recipient according to their accountability

Art. 5 Para. 2 DS-GVO can comply.

Art. 5 Para. 2 GDPR

The person responsible is responsible for compliance with paragraph 1 and must

Demonstrate compliance (“accountability”).

In my opinion, the information obligation under Art. 13/Art. 14 DS-GVO not under the

according to Art. 5 Para. 1 DS-GVO, the obligations of the person responsible to be proven.

It is therefore sufficient if the person responsible documents that

the data subjects have been informed in accordance with Art. 13 and 14 GDPR. Furthermore

The information that is often made available on the Internet is also used

prove this.

I have a comparable question in the area of patient information

I rated accordingly (see Section 4.6.1 and 4.6.2).

4.1.5

Recording of telephone conversations (call recording).

the GDPR

The recording of telephone conversations (so-called call recording) is permitted,

if the data subjects have given effective consent, unless

there are statutory recording and retention requirements.

I received a notice that an energy service provider for heating and

Utility bills Standard telephone calls to the hotline

be included. An express consent (opt-in) on the part of

interlocutor was not caught. There was only a note

that the interlocutor at the beginning of the conversation of a recording

could object.

By resolution of March 23, 2018 (resolution of the DSK of March 23, 2018

drawing of telephone calls; s.a. Materials, Section 2.3) have the

independent federal and state data protection authorities (data

protection conference - DSK) stipulated that a recording of telephone

In terms of data protection law, we usually only talk with your consent

of the external caller is permitted. A privacy law

Effective consent within the meaning of Art. 4 No. 11 DS-GVO is therefore required

requires that the person concerned before the start of the intended recording

asked if he agrees to the recording. The record

requires the express consent of the person concerned, e.g

saying "yes" or by taking an active affirmative action

(e.g. by pressing a telephone button). Likewise, the consent

be given "in an informed manner". That means dem

Interlocutor before giving consent voluntarily, information

how the purposes, the storage period etc. are to be communicated.

In its decision, the data protection conference emphasizes that the mere

elimination of an objection option and the subsequent continuation

of the telephone call does not constitute effective consent under data protection law

the GDPR represents.

The energy service provider was therefore requested by me to complete the procedure

adapt the telephone recordings to the legal requirements. Until

If a GDPR-compliant solution is available, the "call recording" was provisional

completely adjusted.

4.1.6

Video surveillance by employers

Employers are generally entitled to use publicly accessible sales

to monitor rooms with video cameras. To justify one

Video surveillance in the employee context must have a concrete indication

point to uncover a crime. Signed under pressure

Declarations of consent to video surveillance are invalid.

The uncertainty as to how video surveillance will be implemented after the change in the Federal

of the Data Protection Act and the introduction of the General Data Protection

ordinance in May 2018 can be used in a legally compliant manner is both

large for private individuals as well as for tradespeople. So reached

me, on the one hand, a number of telephone inquiries and letters about

Reassurance that the previous video installation is compliant with the law

may be. On the other hand, future camera operators wanted to know what they were in front of

New installation would have to consider.

Numerous requests for advice and complaints were processed this year

Employees addressed to me, their subject

the video surveillance was by your own employer. So busy

I deal with cases from the areas of gastronomy, hotel industry, but also

with traders to senior care services.

In one case, two employees of an on-

line wholesale (with a total of 25 employees) independent of

each other with me that video surveillance both in the office (major

raumbüro) as well as in the warehouse and in the outdoor area of the company premises

would take place. Photographic material that was made available to me showed that

that with dome cameras, multiple work areas and desks in the

open-plan office could be viewed.

The company premises were fenced in, access to the opening times

but unrestricted and possible for everyone. Although it is one

Traded online, it was stated that on-site sales were common

took place and customers viewed and bought goods. To this end

a goods table was positioned in a corner of the open-plan office to

to present products. The individual prices of the products were on the table

between a small single-digit euro amount up to approx. 500 EUR. Around

to deter the presented goods from being stolen or

If necessary, to punish a theft were a dome camera and a

Stick camera installed in the open-plan office. As another purpose of surveillance

it was stated that thefts had already taken place more frequently.

However, there were no criminal charges.

The shooting angle of the dome camera could not be covered by the black

glass dome cannot be seen. The stick camera was on desks

and a safe within the open plan office. The supervision

of the storage room and the outdoor area was carried out by stick cameras.

Video surveillance was activated at the entrance to the building and in the

Storage area indicated by pictogram.

Legal Assessment

Video surveillance in public spaces, i.e. the areas frequented by customers

areas, is publicly accessible according to § 4 BDSG (video surveillance

rooms) i. V. m. Art. 6 (1) lit. f GDPR (lawfulness of processing)

to judge.

According to data protection law, employers are generally entitled to

to monitor publicly accessible sales rooms with video cameras,

to protect against crime, e.g. B. against theft or vandalism.

The sales area and the area for the presentation of goods were

comprised of.

The purpose of such video surveillance does not have to be exclusive

may be to ward off criminal offenses committed by customers. Rather he can

Employers also pursue the purpose of protecting themselves from criminal offenses

to protect employees. Such video controls are common in the

checkout areas of retail stores. In such cases must

video surveillance disclosed or made recognizable what

usually by signs and a clear camera orientation

happens. That way customers and workers can know that

they are filmed. In addition, the employer or shopkeeper must do so

Delete footage as soon as possible.

The rest of the monitored area, in which there are only employees

were staying is in accordance with § 26 BDSG (data protection for purposes of

employment relationship).

Video surveillance to uncover criminal offenses in the employee

context was inadmissible because there was no concrete clue

or suspicion existed against one or more employees who

had to be clarified. A rationale for monitoring office workplaces

could not be accomplished.

The declaration of consent that the employer provides to its employees

had caught up with and who had been pressured to sign them

considered ineffective because it was not voluntary. a one

Approval within employment relationships is according to § 26 paragraph 2 BDSG

only possible in exceptional cases, especially if for the employees

legal or economic advantage is achieved or employer and

Employees pursue common interests. This was not the case here.

Result

Online trading was checked on site. At the appointment were next to the

management, the company data protection officer and a legal

representative present. Each camera has been checked. It could be ascertained

that changes have already been made to that situation,

presented by the complainants during the verification process.

In the meantime, consents signed by the employees

Obtained declarations of consent for video surveillance at the workplace and

submitted to me, but for lack of the voluntary nature of signing

classified as ineffective.

In addition, the following measures were subsequently implemented:

– The camera, which was aimed directly at the office workstations, was

removed.

– So-called “private zones” were used for the rest of the monitoring

directed, or existing zones were expanded so that no jobs

affected by the continuous monitoring.

– The open-plan office was structurally redesigned. So became a mirror wall

through which the workplaces could be seen far and wide.

– The signage has been expanded to include the name and contact details

of the person responsible, the contact details of the data protection officer,

the purpose of the processing, the legitimate interests and the

extended storage time.

– In addition, a large screen was installed in the open-plan office,

which depicted the surveillance monitor of each camera and with it

guaranteed full transparency.

The cameras in the storage room were exclusively on the storage aisle and

directed to the delivery gate and not objectionable.

The cameras in the outdoor area were data protection compliant only on that

own property aligned.

Even if the camera installations and surveillance system through

me were checked and the video surveillance in the company in the future

carried out with the greatest possible transparency, the relationship of trust seemed

permanently broken within the workforce. Both complainants

no longer work for the company.

4.1.7

Photographs and GDPR – by no means impossible

A perennial favorite among the complaints received by my agency

are those about the publication of images, especially on the Internet. To-

In the period under review, there were countless requests for advice on admission

and publication of photos and videos approached me. Since the

Unfortunately, the legal situation in this regard has not been very clear since the data protection reform

is, there is uncertainty among many responsible persons as to what the conditions are

now apply to the taking and publication of images of people.

Over the entire reporting period, dozens of written

physical and telephone inquiries on the question of under what conditions

the production and publication of photos and videos according to the new

data protection law is permissible. Some of the inquiries came from professional

photographers, but above all from companies, private individuals and associations,

who for various purposes photos and videos on their websites, blogs

and wanted to publish in company or association magazines. In

There was obviously a lot of uncertainty about this question, which certainly wasn't

most recently through publications with partly questionable content and lively ones

discussions on internet forums and social networks.

It was not uncommon for fear or anger to be expressed that

due to the DS-GVO no more photos were supposedly taken

or may be published if the people depicted are not

had expressly consented thereto in writing. Of course this is not

the case.

Digitally captured photos and videos depicting individuals

recognizable and identifiable contain personal data. The

Photographing or filming (data collection) and the publication of the

Images (data processing) therefore fall within the scope of the

GDPR. Just as under the old law, however, two cases are (largely)

Excluded from data protection law: For photography too purely personal

Personal and family purposes (e.g. holiday photos) are subject to data protection law

not as long as the privately recorded photos and videos are not in one

be published in a larger circle (e.g. Internet, club magazine). One

Another exception applies to the recording and publication of images

and videos for journalistic purposes (e.g. in newspapers, television,

professional blogs etc.). As before the data protection reform, in

in this area only the Art Copyright Act (KUG), whose

Application permitted by the GDPR as an exception. In all other cases

apply since May 2018 to the taking and publication of photos and

Videos exclusively the rules of the DS-GVO. All non-journalistic

responsible persons (e.g. clubs, companies, website operators

etc.) when dealing with photos and videos must therefore now comply with the

GDPR requirements.

Taking and publishing images is hassle-free afterwards

permissible if the persons depicted have given their consent (Art. 6

Paragraph 1 sentence 1 lit. a GDPR). The requirements apply to the consent

from Art. 4 No. 11 and Art. 7 GDPR. You don't necessarily have to afterwards

be given formally or in writing, but may also be oral or

even implied, for example by posing in front of the camera,

be explained. However, in case of doubt, the responsible

duty of knowledge. In addition, given consents can be revoked at any time

The person responsible must inform the data subject before obtaining consent

their scope and revocability.

However, the GDPR also provides for the possibility of using images and videos without

to record and publish the express consent of those depicted

. According to Art. 6 Para. 1 lit. b DS-GVO im

Take pictures of their contractual partners as part of their order and
process (e.g. application photos, wedding photos, etc.). In most
cases, however, based on a weighing of interests according to Art. 6 Para. 1 lit. f
DS-GVO to assess whether the taking of photos and videos or their
publication is permitted or not. After that, it has to be weighed
between on the one hand the interests of the photographer or the body that
wants to use images, and on the other hand the rights and interests of
person(s) depicted. As a rule, the person or agency that
wants to take or publish images, legitimate interests in doing so,
for example for artistic reasons or because they use them for their
business activity required or would like to use for their external presentation.
The people depicted, on the other hand, have a general interest, don't they
depicted without their knowledge or against their will or a greater one
to be presented to the audience. This interest is due solely to the recording
me from photos or videos in public regularly only slightly
affected. The publication or distribution of the captured images

adversely affects the rights and interests of those affected
much more. The stronger the rights and interests of the people depicted
affected by the images (e.g. detailed portrait photos, photos
in explosive situations/poses) and the more vulnerable they are (e.g.
children, helpless people), the sooner the publication of pictures
and possibly even their inclusion inadmissible. The balancing of interests
falls however always in favor of the person responsible, if the
Publication of the respective picture also after the already after old

Legal situation applied rules of the KUG would be permissible (in particular

§ 23 KUG). In these cases, images may continue to be used without consent

of those depicted are made and published.

All persons depicted in photos and videos must have basic

additionally according to Art. 13 or 14 DS-GVO about the background of the survey

and processing of your data. Fulfillment of the legal

In practice, however, information requirements are often difficult because the

captured situations are often fleeting and between photographer and

Affected often no verbal communication takes place and no medium

is used, through which the information can be made easily accessible

could. If several people are photographed or filmed at the same time

and some of them are not even aware that they have been recorded

(e.g. for larger events or recordings in inner cities),

it is regularly disproportionately complex or even impossible and

therefore also dispensable according to Art. 14 Para. 5 lit. b DS-GVO, information

to grant data protection. Those affected who know that they

are formed, the person responsible must, however, look up the information

Art. 13 GDPR. This can be done, for example, by passing

leaflets or by displaying the information in a visible way

Venue (possibly in cooperation with the organizer).

Ultimately apply to the recording and publication of photos and videos

of people largely the same even after the data protection reform

Requirements as under previous law. There are no changes

in the production and publication of pictures to purely private as well

for journalistic purposes. In the other cases, too, the requirements

changes of the GDPR only in a few points (e.g. consent,

Information obligations) are somewhat stricter than those of the previously applicable KUG.

93

The Hessian Commissioner for Data Protection

47th activity report on data protection

4.2

Europe, International

4.2.1

International data transfers - Privacy Shield relaunched

test bench

Also this year an employee of the HBDI was a member of the delegation

European supervisory authorities working 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 review took place in Brussels in the year under review. The approximately 40-strong

The US delegation was led by Secretary of Commerce Wilbur Ross.

The European delegation, led by Commissioner Jourová, sat down

seven representatives of the European data protection supervisory authorities and

representatives of the European Commission.

As in the review last year (46th activity report, point 4.1,

p. 55 ff.), the test initially included questions about the practical implementation

of the Privacy Shield. The focus here was mainly on the process and content

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 second annual Privacy Shield review was published by the

European Data Protection Board (EDPB) at https://edpb.europa.eu/

our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-

review-report-22012019_en published. It could be stated altogether

that the processes being carried out on the part of the US Department of Commerce and

taken by the Federal Trade Commission in the right direction

point. The conclusions drawn by the Article 29 Working Party in

their report on the first review of the EU-US Privacy Shield for this

field were all accepted and it was worked on

worked to further improve the practical implementation in this sense.

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 should be considered more closely in the coming year is the

ter transfers from Privacy Shield certified companies to third parties.

From the EDPB's point of view, it must be ensured here that the privacy

Shield also adhered to the conditions laid down for this purpose in reality

become. Finally, the area of employee data should continue

and keep an eye on the recertification process.

In addition to the practical implementation questions, the question also took up again

after government access to data under the Privacy Shield in the USA

were transferred, a large room. Here, too, can be held

are that some conclusions of the Article 29 Working Party

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

These were just prior to the second annual Privacy Shield review

enough new members for the Privacy and Civil Liberties Over-

sight board appointed to make the body quorate again.

However, it should also be noted that the position of the ombudsperson, who

was created specifically with the Privacy Shield to provide a way for

to open up to those affected to assert their rights in the event of state access to personal

enforce related data effectively, still only on an interim basis

is occupied. The European Commission has prompted this to the USA

in their conclusions on the second Privacy Shield review

set an ultimatum. If the USA does not have a candidate by February 28, 2019

have nominated for the office of ombudsperson, announces the European

Commission, "appropriate measures under the General Data Protection

regulation" to take. A possible measure would then also be the

Suspension of the Privacy Shield. The report of the European Commission

is at https://ec.europa.eu/info/sites/info/files/report_on_the_second_

annual_review_of_the_eu-us_privacy_shield_2018.pdf available.

Overall, it can again be stated that the area of international

nal data transfers continues to be burdened with serious uncertainties.

In addition to the indirect threat of the European Commission, the Privacy

Shield are still pending before the ECJ, whose

Output far-reaching importance for the admissibility of data transfers

in countries outside the EU.

4.2.2

Europe-wide cooperation with the other European ones

Supervisory authorities under the General Data Protection Regulation

The General Data Protection Regulation (GDPR) results in

Cooperation of the supervisory authorities in Germany and Europe

rich innovations. The new European staff unit set up at the HBDI

and international acts as a link for communication between

the HBDI and various offices outside of Hesse in Germany,

Europe and the world.

The DS-GVO forces the individual supervisory authorities to a much narrower

cooperation than before. She consistently pursues the idea of

One stop shop. This means that a company that is a data processor

processing procedures across branches in several Member States

uses a procedure or uses a procedure at only one branch that

but significant impact on data subjects in more than one

member state has to deal with only one supervisory authority (lead supervisory

supervisory authority) should have to deal with.

However, the one-stop shop also applies to those affected: they have

the opportunity to lodge a complaint with any supervisory authority

authority (which thereby becomes the supervisory authority concerned within the meaning of Art. 4

No. 22 DS-GVO) in Europe. The communication with the

Those affected are then assigned solely to this supervisory authority, even if

it is not responsible for the body against which the complaint is directed.

From this it follows that at least complaints against positions outside Germany
lands of the HBDI no longer for the body against which the
serious, "competent" supervisory authority may be submitted.
It is now rather the case that such cases between the HBDI and the or
communicated to the other supervisory authorities concerned and together
need to be edited.
The aim of the new procedural regulations is to create a Europe-wide
ensure uniform interpretation and application of the GDPR. About it
In addition, communication with the supervisory authorities should be
processing bodies as well as for data subjects are simplified.
The procedures used here are essentially
regulated in Chapter VII of the GDPR. For the required cooperation
enabling and facilitating also electronically, among other things, IMI
(Internal Market Information System)
tem) used. Since 05/25/2018 were from the HBDI in the reporting period
already more than 400 cases registered in IMI and counting in the

to work on a new form of European cooperation. Almost all
of these cases would either not have happened to the HBDI before the GDPR came into force
not known or directly to the "competent" supervisory authority
been referred, in whose supervisory area the body against which the
lodges a complaint, has its registered office.
An additional novelty for the work of the HBDI in cases that are
GMO now processed and coordinated with other supervisory authorities in Europe
is the fact that the work is almost exclusively in English.

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,

which has to be dealt with.

4.3

General administration, municipalities, police

4.3.1

Project "Digital Model Authority"

In 2018, the Hessian state administration launched the "Digital Model

authority" started. The aim is to provide a variety of administrative services

digitize. The HBDI accompanies the project in the steering committee and,

if necessary, also in the sub-projects.

The OZG as a legal framework

The Online Access Act (OZG) is a federal law that has been in force since

08/18/2017 is in force. It obliges the federal and state governments (according to the justification

and intention of the federal government including the municipalities), within five

years their administrative services also electronically via administrative portals

to offer tale.

Essential targets of the OZG are

– the rapid digitization of online access to administrative services

until 2022,

– the linking of individual administration portals to form a portal network and

– the provision of interoperable user accounts for a uniform,

convenient and secure access to administration services offered online

services, regardless of whether they are municipal, state or

federal level.

97

The "Digital Model Authority" project

The "Digital Model Authority" project is intended to use the example of the three government

executive committees the conversion of authorities into digital service providers

be set in motion. It's all about digitization

of online access and internal administrative processes. should

the processes must be free of media discontinuities and a faster, more efficient and economical

ensure more efficient processing. But it also applies to the municipalities

to be involved in the processes.

The project structure sees a steering committee for project management

before. I am a member of the steering committee as an advisory member. Under

the steering committee is the project management, under which in turn

sub-projects and support services.

In a first step, five technical sub-projects (TP) were started. For the

For the “recognition bonus” sub-project, see also my contribution under Section 4.3.2.

There were also sub-projects that served in particular to

To record states and to systematize overarching aspects.

The privacy aspect

From my point of view it was essential to ensure that the data protection

legal requirements are complied with. There were several talks about

check with the project management. As a result, a structure was found that

the essential data protection checks and approvals in the

sub-projects, whereby it is in the coordinating cross-sectional area (as

Share Service referred to) there is a coordinator who can answer questions about

Available.

The standard process provides for compliance at a number of points

ensure compliance with data protection regulations:

– During initiation, the record of processing activities

created by the person responsible.

– At the end of the phase, e.g. decided whether a data protection

assessment must be carried out.

– In the following implementation plan, in particular, the requirements

of Art. 25 GDPR data protection through technology design and through

data protection-friendly default settings ("Privacy by design" and "Privacy

by default") must be observed.

– At the end of the implementation plan, it is checked whether the data protection

common assumptions are still valid. If not, are appropriate

to make adjustments.

– There may be changes in the subsequent implementation.

These must be clarified with the cross-sectional area. After that the

Opinion of the responsible data protection officer requested

to start the pilot project if the opinion is positive.

– At the end of the pilot project, the experiences will be evaluated and it

there may be changes. If relevant changes are made

again a consultation with the cross-sectional area. It is going to be alright

checked whether the data protection requirements are still being met.

If this is the case, the transition to regular operation takes place.

If the sub-projects are carried out according to these specifications,

compliance with the requirements of the GDPR and the HDSIG

be taken.

4.3.2

"Digital model authority" - sub-project "recognition bonus"

"Recognition bonus" is a sub-project of the "Digital Model Authority". It

The aim is to make the granting of bonuses to members more voluntary

Digitize fire departments. Municipalities and their fire brigades are involved

and also regional councils involved.

what it's about

Since 2011, volunteer firefighters in operational departments have

gen and since 2017 voluntary helpers in the units

of the Hessian civil protection a recognition bonus for a

active service of 10, 20, 30 or 40 years.

The applications are made by the municipalities and in cases of disaster

protection by the districts or urban districts to the state of Hesse

placed. The responsible regional council processes the applications.

In the previous process, the applications in paper form reached the executive committees,

where they were transferred to Excel spreadsheets for further processing.

In the "Digital Model Authority" project, the application and disbursement

ment of these recognition bonuses as an administrative service,

in which digitization can take place quickly and become a significant one

Acceleration and also improvement (see also the article

under Section 4.3.1).

The sub-project "recognition bonus"

For the sub-project, employees of the government

together with representatives of ekom21, the specifications for a web-based

Developed database application. The eGovernment platform served as the basis

"civento". Together with representatives of the HMDIS, the appropriate

Documents created and presented to me. A threshold analysis was performed

the conclusion that no DPIA is required; the result was for me

understandable. Also the decree was revised and an agreement

according to Art. 26 DS-GVO.

It was difficult to prevent the double award of a recognition

identification bonus in the process in accordance with data protection. same

applied when someone did not want to receive a recognition bonus, although they

would have been entitled to him under the decree. Here had to § 28a HDSIG

be resorted to in order to obtain a data protection-compliant solution.

The planned solution

In principle, applications can only be submitted electronically. For the

The State of Hesse provides electronic applications to the municipalities and

Counties or urban districts have a corresponding IT system free of charge

(civento recognition bonus) available.

The IT system consists of an online part for the application. The

Municipalities and districts or urban districts can use the data

recording for the application to the units of the voluntary fire brigade

or delegate disaster control. To make sure only

the authorized organizations via the online portal to submit the application

prepare, these organizations receive appropriate access via

User ID and Password. Alternatively, the municipalities and counties

or district-free cities, the applicant data using a recording tool

record directly in the system.

After the data of those to be honored have been recorded by the authorized

Organizations check the municipalities and rural districts or independent districts

Cities this information and submit the application for recognition premium

responsible regional council. The data will be sent electronically to the

submitted to the regional councils.

The following data is collected for the purpose of submitting an application:

From the applicant:

- Surname

– authorized representative

- Address

- E-mail address

– phone number

– planned award date

The information is pre-controlled based on the stored user data.

From the honoree:

- Family name

- First name

- Birth date

- Gender

– Place of residence: street

– Place of residence: house number

– Place of residence: addendum to the house number/letter

- E-mail address

– hours of service

If the application is made, the data record is sent to the responsible government

sent to the Board of Directors.

If the application is rejected, a reason must be given.

the. In this case, the data will not be transmitted to the government

presidencies. The reason for the rejection is only for internal purposes of the

provided by the applicant.

If the certificate was handed over, the data will also be carried out

the communities or districts expanded and the regional councils

transmitted:

– Handover of the certificate at the scheduled time

– Handover of the certificate "Date" if different from the planned time

– No delivery of the certificate and impediments

When the certificate is handed over, the honorees receive their personal

cover letter from the district president

ten another letter. This letter contains the access data (PIN)

for the civento portal. The honorees can enter their bank details there:

– IBAN

- BIC

– possibly deviating account holder

Alternatively, the applicants or the regional councils can do this

capture information.

After collecting the data of those to be honored, the municipalities check
and districts this information and submit the application by means of data transfer
communication to the regional councils. The regional council checks independently
pending the information again and created - if the requirements are met
gen - a certificate, a cover letter from the district president or the
District President and a cover letter asking for the account details
recorded via the online portal. The documents will be sent to the applicants
delivered by post. If a recognition bonus is rejected,
the regional council informs the municipalities and districts at
Indication of the reasons for rejection.
After the award of the certificates and the delivery of the cover letter to the
The communes and districts transmit the information to the Re-
government presidencies. The regional councils arrange after the recording
of the account data (in the online portal either by the honorees or by
the municipalities and districts) the payment of the recognition bonus
by creating a corresponding disbursement order. Should the
Acquisition of the account data at the request of the honoree by the municipalities or
districts, this can only be done via the online portal.
To do this, the honorees must provide the access data from the cover letter
can give The regional councils can use the account details under
record the transaction processing directly in the transaction.
The data of the municipalities and counties will be transferred to the at the end of
Honor deleted the following year. The data of the regional councils are
deleted after the end of the tenth year following the award.
A transfer of data and documents into the system of permanent

Long-term storage by the state of Hesse is planned. For this purpose, in

As part of another sub-project of the digitization program

the technical and organizational requirements have been created.

4.3.3

Publications on municipal websites

Numerous inquiries from local authorities and complaints from local authorities

officials, but also of citizens concern the

publications on municipal websites. You can already find this

Statements in my 43rd activity report.

The municipalities pursue different purposes with publications.

It is about creating transparency, enabling participation and

to inform citizens. To what extent does the publication

clearing of directly personal data or data that

permit a personal reference, must be checked on a case-by-case basis. are there

Necessity and proportionality of a publication also after

the range of the medium used and thus the depth of the intervention in

assess the right to informational self-determination.

As a rule, published facts of a municipality are only

a limited group of people, for example for their citizens

Citizens of the community matter. Such an addressee limitation

publication on municipal websites is not possible.

Personal facts are presented there to a global public

made accessible and also enable appropriate and successful

Search queries without a global need to know.

The information interest of the internet public in personally identifiable information

Information about citizens has to the Inter-

essen of those affected by the publication to withdraw.

It follows from this that an ultimately worldwide publication of personal

ment-related data only in justified individual cases via municipal

websites may take place. In these cases, the provided

to limit the content in such a way that the information relates only to the desi-

intended group of recipients. For example, the publication

a personnel change in an important position within a company

Municipality on the basis of § 66 para. 2 HGO to limit that

this position is now perceived by person B and no longer by person A

is taken. More information about the respective persons or the

Reasons for changes are allowed in the absence of a requirement

not be published.

4.3.4

Information from the police information systems of the State of Hesse

Due to the new regulations of the EU data protection reform, the citizens

and citizens to make use of their right to information easier and

the new communication channels are also taken into account. Appropriate

Citizens also experience relief when claiming

exercising their right to information vis-à-vis the Hessian police.

Responsible for providing information from the police information system

POLAS-Hessen is the Hessian State Criminal Police Office (HLKA).

Before May 25, 2018, this required a cover letter with attached,

credible or confirmed copy of an identity document and the information

a postal address of the person requesting the information. The desire for

I had accepted a copy as this was considered mandatory in order to

to clearly identify the person concerned and to avoid misuse

the. This previous procedure made it the reporting entity

Make sure in the past that it's pretty easy to do that

Information was provided by an authorized person and only to

the beneficiaries arrived.

This practice could not be maintained under the new legal situation

become. The general conditions for the information from the police

Information systems now result from § 29 HSOG and § 54 HDSIG.

From § 54 para. 4 HDSIG it follows that only in the case of justified doubts

additional information on the identity of the person concerned

may be required. Accordingly, the reporting body must

Individually check whether a request for information is due to the present

information can be unequivocally assigned to a specific person and

that the final information is transmitted to the authorized person.

The reporting entity must have a level of certainty about the

Obtain the identity of the applicant who is a locating in the concerned

databases and continue to have an unequivocal adherence to the calculation

authorized information. To find people in

police databases are basically information on name(s),

First name(s) and date of birth required for the provision of information

data protection reasons in writing by post

done, a postal address. As far as a person, for example due to

of multiple stocks in one file, cannot be identified beyond a doubt,

the necessary information may be requested from the person concerned

be changed that enable identification. Justified doubts about the

The applicant's identity can also be determined in part by the police

Database deviating information arise, or even if a

specified sender address cannot be assigned to the applicant.

The HLKA has adapted its practice to these requirements. After my

So far, this was only known in an extremely small number of inquiries

It is necessary to obtain additional information from the data subject.

4.3.5

Data exchange between Chambers of Industry and Commerce and the

financial management

The Chambers of Industry and Commerce are authorized to set the

to collect the data required for chamber contributions from the financial authorities.

Data protection report from 05/25/2018

Traders have approached me several times with the question of whether the

financial administration is authorized to personalize the Chambers of Industry and Commerce

Name-related data regarding the financial (tax) situation

to be sent to traders. The trigger for the inquiries was mostly

that the tradesmen from the Chambers of Industry and Commerce

gene membership and contribution determination had been written.

§ 3 para. 2 IHKG regulates that the costs of setting up and operating the in-

Chambers of Industry and Commerce etc. through contributions from members of the Chamber

be raised according to a fee schedule. are members of the chamber

in addition to companies also natural persons, provided they are subject to trade tax

are assessed and in the district of the Chamber of Industry and Commerce a

business premises (§ 2 Para. 1 IHKG). Submit the registry courts

the chambers of industry and commerce, the entries in the commercial register.

The chambers of industry and commerce are data protection law according to § 9

Para. 2 IHKG (in conjunction with Art. 6 Para. 1 lit. e DS-GVO) authorized to determine

to the chamber affiliation with the tax authorities

raise.

§ 9 paragraph 2 IHKG

The chambers of industry and commerce ... are entitled to determine the chamber

affiliation and to determine the contributions of the chamber-related information on

Trade tax assessment ... as well as the ... required assessment bases

to raise the tax authorities.

This power of collection of the Chambers of Industry and Commerce is carried out in the tax code (§ 31).

a corresponding transmission obligation of the tax authorities, which in particular

which is aimed at the chambers of industry and commerce.

§ 31 paragraph 1 AO

The tax authorities are obliged to provide tax bases, tax base amounts and

Tax amounts to corporations under public law ... for the determination of such

Notify taxes that are attached to these tax bases, tax bases or

Link tax amounts.

I have informed the inquirers about this legal situation.

4.3.6

Production and use of 360° panorama shots for

Calculation of recurring road contributions

The creation of 360° panoramic images of buildings and streets

by a private company is permissible under data protection law. Also the

transmission of such recordings to a municipality and their use for reporting

calculation of recurring road contributions to fulfill a public

task is not objectionable.

It had to be clarified whether the creation of 360° panorama shots of buildings

and roads of a private company and the forwarding of these

Recordings to a municipality, which uses these to calculate recurring

Street contributions used, data protection law is permissible.

A municipality bought 360° panoramic photos from a private provider

ment to determine the inventory of streets and buildings in the municipality.

For this purpose, the roads were driven with special vehicles that

Video cameras and a corresponding sensor system are equipped. By

The data collected from the video vehicles provide information about the size of

Properties whose development (e.g. residential or commercial buildings,

one or more floors, etc.) and the condition of the road. These dates

can provide information about the factual circumstances of an identifiable person

give and are therefore personal data. The data thus collected

used the municipality to calculate recurring road contributions.

Preparation and transmission of panoramic images by the

Pursue

The processing of personal data is permitted, among other things, if

they are necessary to protect the legitimate interests of the person responsible

and interests or fundamental rights and freedoms worthy of protection

Those affected do not outweigh (Art. 6 Para. 1 lit. f DS-GVO). One can

legitimate interest is already a non-material or economic interest

of the person responsible or of a third party (cf. Sydow, Europäische

General Data Protection Regulation, 2nd edition 2018, Art. 6 GDPR, para. 54).

In the present case, the business concept of the commissioned company is based

We are committed to providing 360° panoramic

take measurements of buildings and streets and prepare them for

place. On the part of the company is therefore a business and therefore

economic interest in the processing of personal data

to see. Legality, however, depends on the fact that

106

Data protection report from 05/25/2018

the interests of those affected within the framework of those of the person responsible

made balancing does not outweigh his legitimate interests.

During the inspection, vehicles in the vicinity are also detected

and recorded their license plate numbers. Furthermore, persons

drawn who are on the streets. This represents a significant

encroachment on the fundamental right to informational self-determination

for this reason, the persons admitted by the company

and license plates are pixelated and thus made anonymous. The publication

of panoramic shots does not take place.

It should be noted that the right of objection according to Art. 21 DS-GVO of

data subject has the right if certain conditions are met

grants a lawful and legal basis of Art. 6

Paragraph 1 sentence 1 lit. e and f DS-GVO processing concerning you

prevent personal data. The right to object is on

the existence of reasons arising from the particular situation of the

affected person. It then causes responsibility

literal to weigh up these specifically asserted reasons with the

own legitimate interests in the processing. personal

Data of objecting persons may only be processed if

if compelling legitimate grounds for processing are proven

the specific reasons asserted by the data subjects

person outweigh.

The form of survey described above is based on these conditions

and transmission of the data by the commissioned company in frame

the balancing of interests in accordance with Article 6 (1) (f) GDPR. The

particular situation of the data subject is under consideration

of Art. 21 Para. 1 S. 2 DS-GVO to be taken into account.

Use by the municipality to calculate recurring

road posts

I also checked whether the data processing on the part of the municipality as

recipient of the panoramic images is permitted. As the legal basis for

Processing according to the General Data Protection Regulation came under Article 6 Paragraph 1 Letter e

GDPR under consideration. Thereafter, processing is permitted if it is for the

Performance of a public task that is entrusted to the person responsible

was worn is required.

According to § 93 Hessian Municipal Code (HGO) i. V. m. § 11 paragraph 1 sentence 2

The Municipal Tax Act (KAG) is intended to allow the municipality to rebuild

and expansion of public roads, paths and squares (traffic facilities),

which goes beyond the ongoing maintenance and repair, contributions

raise. Section 11a KAG grants a right to choose, this also over

to collect road fees. The entertainment of public

roads and the associated collection of contributions

a public task within the jurisdiction of the municipality.

The amount that the property owners in this connection to

have to pay consists of the size of the property, the type of use, the

Number of floors and the contribution rate according to the billing

planning area together. The 360° panorama shots of the buildings and

Roads provided this data, which was ultimately used to calculate the

sweeping road posts were required. This data will be internal

used by the community for this purpose.

Thus, the panoramic images for the contribution collection of road

construction measures are used as part of the fulfillment of the task and are therefore

permitted under data protection law.

4.4

school, colleges

4.4.1

No WhatsApp in everyday school life for teachers –

Is there an alternative?

The use of WhatsApp in schools by teachers has

increased sharply in the reporting year. The guidelines of the Kultus-

Ministry for the use of social media by teachers

enough attention.

Messenger WhatsApp

WhatsApp is a so-called instant messenger service that allows

between registered users text and voice messages as well as photos,

Exchange videos, audio files and contact data and via IP telephony

to make phone calls over the Internet. According to its own statements, WhatsApp had

one billion users in 2016. The daily volume

of communication was 42 billion messages, 1.6 billion photos

and 250 million videos. This makes WhatsApp the most-used trade fair

ger service worldwide. The number of WhatsApp users in Germany is increasing

32 million heads estimated. In October 2014 WhatsApp was taken over by the

Taken over by the social network Facebook.

Unlike Facebook, which uses advertising based on data from the

Users generated its sales, was the business model of

WhatsApp long unclear. The assurance in connection with the

acquisition of WhatsApp by Facebook to continue working independently

and not to mix the data of both services with each other was made by

WhatsApp changing its terms of service mid-year

canceled in 2016.

What data is stored by WhatsApp?

Data that WhatsApp has, among other things, are:

– phone number

– Profile name, profile picture

- News

– Group affiliation

– Favorite lists

– Usage Information

– transaction data

– Device and connection data

– location data

– cookies

– status information

From this, partly detailed relationship, communication,

supply, usage or interest profiles.

The data protection issue

Processing takes place when using a messenger such as WhatsApp

of personal data. The user must log in,

Communication content is exchanged, including so-called traffic data

develop. In addition, when you register, everyone is automatically in the mobile phone

transfer stored contacts to the provider. For this data processing

processing is either a legal basis or consent of the

affected persons required. The user of WhatsApp is for the transmission

the contact details of other people stored in his mobile phone

responsible for data protection. Therefore, before registering the

Messenger service have the appropriate permission. the official

Bad Hersfeld court has the decision of March 20th, 2017 (F 111/17 EASO).

this topic stated that whoever through the use of whatsapp the

allows his mobile phone contacts to be shared without prior notice

to have obtained permission from his contacts

committing a criminal offense and putting themselves in danger

am going to be warned by them at their expense.

Whether and to what extent a teacher uses WhatsApp in their private environment
uses is primarily their personal affair. But when it comes to the
Processing of personal, school data is located
Teacher in a different legal context. The teacher acts on behalf of
the school, this is the responsible body and must always be responsible for
the security and traceability of the data processing and the
guarantee communication. According to § 83 of the Hessian School Act (HSchG)
The processing of personal data is only permitted insofar as this is necessary for
lawful fulfillment of the educational and educational mandate of the school
and for any related purpose or performance
school organizational measures are required. Also from § 3 para. 5 of
Regulation on the processing of personal data in schools
this obligation for schools and thus also for the teachers. He-
Requirement requires that the purpose only with this data processing
can be achieved. A mere simplification of everyday school life can
not justify necessity. Thus, for the use of WhatsApp
no legal basis.
Consent cannot be assumed without further ado either.
the. On the one hand, the terms of use of WhatsApp require one
Minimum age of 16 years. On the other hand, consent is only effective
if given voluntarily. Such voluntariness can be found in schools
Connection can usually hardly be assumed.
Finally, with the use of WhatsApp, a transmission of the
Data linked outside of the European Economic Area. the
company is based in California/USA and would have to comply with the data

protection regulations of the European Union for data transfer in

subjugate the United States. Since WhatsApp Inc. does not subscribe to the Privacy Shield

subject to agreements (see https://www.privacyshield.gov/list), the

Transmission already inadmissible according to the specifications of Art. 44 DS-GVO.

Alternatives to WhatsApp

Again and again the impression is given that there is no such thing as WhatsApp

alternatives. The Stiftung Warentest z. B. already had trade fairs in 2015

ger services and products like Threema, Hoccer

or signal attested privacy-friendly functionalities. That's how they stand

Servers in Germany (Hoccer), Threema (Switzerland) or the USA (Signal).

The stash cat service, which I looked at, would also be one

acceptable alternative. Personal data is not or only in

collected to a small extent, cell phone directories not issued

read. At Hoccer, for example, each user gets a randomly generated

Numeric code provided, so to speak as a user name. Friends

can be added via the numerical code or via a QR code.

End-to-end encryption is also guaranteed.

So the question arises as to why teachers, when they are at school with their

Class want to communicate, do not use these services. the cult

minister during a conversation in June last year

also addressed this issue. It was expressed that he

the need for a data protection-compliant, national trade fair

ger service for schools. However, the ministry still stands

at the beginning of such considerations and last but not least there are also financial ones

Constraints to which the HKM sees itself exposed.

Irrespective of this, however, it is subject to the specifications of the DS-GVO for

Schools or teachers are obliged to keep data processing within the framework

to organize the use of such services in accordance with data protection.

4.4.2

Internet-based learning progress diagnostics with quop

The Hessen-wide introduction of the learning process diagnostics software quop

I accompanied data protection law. Regarding the requirements that

resulting from the General Data Protection Regulation, had to go through the

Contract processors and the Hessian Ministry of Education a number of

specifications are implemented.

What is quop?

The Internet-based learning progress diagnostics with quop is based on a series

of findings from research and practice. The procedure quop recorded

the performance development of students in short periods of time

Intervals in the central performance areas of reading (grades 1 to 6),

Mathematics (grades 1 to 6) and English (grades 5 and 6)

at the computer.

The diagnostics, which are geared to the course of learning, pursue the goal of teaching

provide a reliable basis of information for individual adaptation

and optimizing student learning throughout the school year

to provide. This gives teachers ongoing information about

the actual competences of individual students and

can do this in a goal-oriented manner with individual measures for the child, e.g. B. one

Changes in the scope and content of the teaching content, react.

Aspects of data protection law

order processing

In the process, a processor is involved who is responsible for the hes-

The Ministry of Education and Cultural Affairs (HKM) runs the process centrally. With this

was a contract for order processing in accordance with Art. 28 DS-GVO

complete as part of the application personal data

of the students and the teachers are processed.

What personal data is collected?

The teachers are systemically informed of their surname, first name, e-mail address,

Class-subject combinations and phone number saved. Of the

Pupils are assigned surname, first name, password

Test series (subject and level), gender, birthday, special funding

may (yes/no), migration background (yes/no) and year of enrollment.

As part of the automated evaluation after processing

Test tasks are data of the students regarding the

learning level in reading and/or mathematics and/or English,

available to the student and the teacher.

Technical data protection aspects

technique of the procedure

Computer-based procedures for the school must be fundamental for there

existing framework conditions are suitable. School computers have in

usually no uniform, technical standards and different

periods of use. Also, some old devices with inconsistent

maintenance and safety concepts as well as various

drive systems used.

Both teachers and students see quop as an in

A web application that can run in a browser is provided via the Internet.

This has the advantage of not having to install any additional software

the workstation computers in schools is necessary. An application

in the domestic area of the students is not planned.

On the other hand, the software can be used on the processor's platform

maintained centrally as part of the constantly necessary updates

become.

encryption

The personal data between the computers in the school and

the processor's server are using the current procedures

transmitted protected for transport encryption. When processing

The data is stored pseudonymised. The processor has

no access to the pseudonyms. Access to the pseudonym (i.e. the

Link to name and a number under which the data is stored

are) is rather bound to the authorizations of the respective teacher.

access to the application

Access to the portal is password-protected. The initial password will be the

Posted to schools via the HKM and is a school password. The

The teacher logs into the portal using the school password,

completes your own user account (registration) and can then use

work with the application with an individual user account/password.

The teacher can now set up their class within the application and

the necessary individual passwords for the students

invest.

Activation of additional teachers

The "lead" teacher can, to the extent necessary, for further

teachers have access to the assessments in the form of reading

activate authorizations and withdraw them again. This stands

in connection with an additional and extended advisory

may by e.g. B. Substitutes, on the one hand, if necessary, classic

Cover representation functions and about the learning status of the students

and students need information, as well as a specific

A need for advice among the teachers themselves who are in contact with the children

are. The lead teacher then ensures that the

Access can be withdrawn if it is no longer required.

deletion of the data

If the responsible teacher changes classes or leaves the school, so

all permissions are revoked. If a student leaves

If you enter the class or change schools, the personal

or personal data at the end of the respective school year

turned off. The same deletion period applies if quop is no longer available in class

should be used. Otherwise, the data will be stored for as long as

until the student has completed grade 6.

Client segregation

The software provider has in the previously offered form of the method

the separation of the data for the schools of different federal states only

individual characteristics of the database. That will do it

Methods meet the requirements for nationwide use

are not fair. Thus the different contractual requirements

the commissioning countries and, if necessary, individual schools also independently

can be implemented from each other is an improved client separation

tion, e.g. B. through a customer-specific virtualization. I have

the Hessian Ministry of Education pointed out that a

Implementation of this technical requirement by the processor for

data protection-compliant implementation is essential.

Admissibility under data protection law

According to the Hessian School Act, personal data from

be processed by the schools.

Section 83 (1) HSchG

Schools may collect personal information from students, their parents and

Teachers process, insofar as this is necessary for the legitimate fulfillment of the educational

and educational mandate of the school and for a purpose related thereto or

is required to carry out school organizational measures.

An implementation decree of the HKM describes and regulates how to deal with

quop in detail. In this way, the scope and use of the learning

diagnostics regulated. After information in the overall conference and

With the consent of the school management, the respective teacher can opt for the

Register the use of quop with the Hessian Ministry of Education. about a

registration process, the teacher is then given access to a

personal user account. Further information in the decree concerns access

rights and erasure periods.

Along with the enactment, the procedure is based on a legally sound one

Provided basis, which are based on uniform standards.

4.4.3

"School without racism - school with courage" - also a

welcome project has to respect data protection

The procedure for obtaining the “School without Racism –

School with Courage" is in accordance with the current data protection regulations

regulations are not compatible and must therefore be adapted in accordance with data protection regulations.

On the occasion of the request for advice from a Hessian school on the above

mentioned project I was informed of the following facts:

An association with a federal coordination office in Berlin issues a

nationwide project those schools that are after the

have qualified to receive the “School

without racism – school with courage”. According to the association,

developed the project in Belgium in 1988 and meanwhile in Belgium, the

Netherlands, Austria, Spain and Germany successfully implemented.

One of the aims of this project is to promote an open

dealing with discrimination of any kind as well as the further development

development of the students' own ideas and projects

Dealing with discrimination and racism as well as prevention

and overcoming racism.

Prerequisite for obtaining the award "School without racism -

School with Courage" is, among other things, that at least 70% of the

School members (consisting of students, teachers and others

employees at this school) with the goals of the project

and work towards it. As proof that this requirement is met

is, among other things, one of the association's schools available

“Copy template signature list” provided. Contents of this list are below

other things, the first and last names as well as the dates of birth and signature

of the school members who support the project. The completed and

signed lists are attached by the school administration to the

respective application for admission to the project “School without Racism – School

with courage” to the federal coordination office of the association. On

The Federal Coordination Office informed me of my request, these lists

served to check the information provided by the school management [achieving the

required (minimum) percentage of signatories] by the

Association.

From a data protection point of view, this procedure is to be criticized:

For this data processing within the meaning of Art. 4 No. 2 DS-GVO is neither

a legal basis in the Hessian school law still in the data

basic protection regulation. Also lay the necessary informed

The consent of those affected is not required for this.

Art. 4 No. 2 GDPR

For the purposes of this Regulation, the term means:

“Processing” any operation carried out with or without the aid of automated processes

or any such series of operations involving personal data such as that

Collection, recording, organization, ordering, storage, adaptation

or modification, retrieval, retrieval, use, disclosure by

transmission, distribution or any other form of provision, comparison or

linking, restriction, deletion or destruction; ...

For the lawfulness of this data processing, however, a consent would have

6 Paragraph 1 lit. a DS-GVO or a statutory

basis must be available (Art. 6 Para. 1 lit. e GDPR).

Article 6 paragraph 1 lit. a and e GDPR

The processing is only lawful if at least one of the following conditions

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;

...

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; ...

Furthermore, the above-described data transmission by the school is on

the federal coordination office of the association to achieve the desired

ten purpose not required and already contradicts the principle of

Data minimization according to Art. 5 No. 1 lit. c GDPR.

Article 5(1)(c) GDPR

Personal data must be adequate and relevant to the purpose and

be limited to what is necessary for the purposes of the processing ("data minimization").

After all, this data processing process of the school as well as the

coordination office of the association does not comply with the data protection

moods compatible and therefore illegal.

To check the number of signers

names and dates of birth are not required. Much more

would be an official statement from the school management regarding what has been achieved

Percentage of supporters of the project sufficient

according The required percentage can be checked with a

anonymised procedures. For example, it would be conceivable here

Conducting a written anonymous survey within the school,

in which those affected simply tick on a questionnaire

– whether they identify with the goals of the project and

want to support

– whether they don’t want to support the project or not

– whether they wish to abstain.

These anonymous questionnaires could be kept at school and the

be made available to the coordination office of the association on request.

This would fulfill the control purpose.

I shared my view with both the school concerned and that

Hessian Ministry of Culture and just put these my just

described alternative concept for data protection compliant design

of the criticized procedure.

The school then refrained from using the “copy template

signature list". Rather, the consent of the students

Students by querying and noting the number of by show of hands

granted consents carried out. However, this procedure is also not

data protection compliant: Since the query in the respective classes is not secret

has taken place, it is to be feared that the students will refuse to issue their

felt compelled to agree. After all, the outcome depended on their approval.

Receipt of the “School without Racism – School with Courage” award

for school. The students could therefore fear

from reprisals from classmates or negative ones

Consequences on the part of the school have given their approval. Questionable

is therefore whether their consent is actually voluntary in each individual case and

thus effective within the meaning of Art. 4 No. 11 DS-GVO.

Art. 4 No. 11 GDPR

For the purposes of this Regulation, the term means:

"Consent" of the data subject, any voluntary for the specific case, in informed

Wise and unequivocal expression of will in the form of a declaration

or any other clear affirmative action by which the data subject

indicates that they are no longer processing personal data relating to them

data agrees; ...

I have also pointed out this aspect to the school concerned. Also

the Hessian Ministry of Education stood up to my data protection criticism

and open to my conceptual suggestions. The

final coordination with the Hessian Ministry of Education to change

Change of the criticized procedure at Hessian schools is present

not yet finished.

In a further step, nationwide coordination with the state

data protection supervisory authorities and ministries of education with regard to a

data protection compliant design of this project.

4.5

traffic, services of general interest

4.5.1

Admissibility of accident data storage under data protection law

The delivery of a new car to the buyer with a standard

built-in accident data memory does not require any express data protection

legal consent of the buyer.

With the ongoing digitization of vehicles, they are also increasing

Complaints against its storage and assistance systems. So wore one

Appellant that equipping a vehicle with a

Accident Data Recorder (UDS) with express consent from the buyer

requirement. With a technical device that is suitable, personal

Recording the driving behavior of the driver is according to data protection law

regulations to require express consent. She appealed

to the lack of such consent and required the seller to

Taking back the purchased vehicle step by step against the repayment

the purchase price paid.

An accident recorder is an electronic device that allows the many

technical sizes while driving depending on the setting for about

30 seconds before and about 15 seconds after the triggering event (e.g.

accident) are stored permanently and can be retrieved after an accident

can. This way the happening can be done at a later date

reconstructed and the question of guilt can be clarified more easily.

The data protection regulations do not contain a general prohibition

to install accident data storage in the vehicles. With what equipment

a vehicle is delivered is a question of sales contract law

Agreement. The purchased item must have an agreed quality

be handed over. If the delivered vehicle has a different quality

than agreed, there is a defect according to the material defect rights

sales regulations triggers. These are towards the seller

of the vehicle and – if necessary – before the civil courts

to fight

The data protection regulations only apply if

a person or body who is not the data subject, the data from the

vehicle raises. In the case of the offline vehicles, whose control units are the

Do not send data out of the vehicle, the regulations of the

General Data Protection Regulation (GDPR) and the Federal Data Protection Act

zes (BDSG) if the information - for example from the workshop - from

be read from the accident data recorder. Exactly at this point in time

must also provide them with the privacy information from the collecting party

be made available (Art. 13 Para. 1 S. 1 DS-GVO).

There are occasional demands in the press that car manufacturers introduce a kind of

Issue data passport for the car, which tells about the data processing in the

vehicle cleared up. But these are demands that are made to the legislature

are directed. The applicable data protection law knows no such far-reaching

information requirements.

As part of an exchange between the independent data protection supervisory

and the German Association of the Automotive Industry (VDA) created a sample text

for data processing in the vehicle. This contains general information

and should serve as an overview of the data processed in the car. This

Sample text (https://datenschutz.hessen.de/datenschutz/verkehr-versorger/
data-processing-in-vehicle) is used by automobile manufacturers at con-
contact points to those affected (e.g. in sales prospectuses).

4.5.2

Stored data from measuring devices - right to information
the landlord/house manager

Tenants must exercise their right to information about the data stored in a measuring
data collected by a measurement service provider on behalf of the lessor
of the landlord or the property management are charged, compared to the
Landlords / the property management claim.

This was increasingly applied to processors in the reporting period
The right to information according to Art. 15 DS-GVO gave me cause to intensively
to deal with this regulation.

A metering service provider acted as a processor for landlords/house
administrations and took on tasks such as

the checking, assembly and data management of radio-based measuring devices
such as heat cost allocators and wireless smoke detectors. He also posed for his
Client also compiled the utility bill and did the math
these directly with the respective tenants. With the validity of the data protection
Regulation, the measurement service provider received several requests for information
according to Art. 15 DS-GVO of apartment tenants, where the measuring devices
of the measurement service provider were used. The tenants demanded
ment of their right to information, in particular information on the

data recorded by measuring devices.

First of all, it should be noted that the data collected by the measuring devices

data is personal data in accordance with Art. 4 No. 1 DS-GVO.

Because personal data means all information

hen relating to an identified or identifiable natural person

relate. A natural person is then already identified as identifiable

considered if they are direct or indirect, in particular by means of attribution

identified to an identifier such as a name or identification number

can be.

Own the measuring devices, such as a heat cost allocator or wireless smoke detector

a device number and are assigned to a residential unit, possibly even one

Space allocated in the housing unit. The residential unit is

hen further data a tenant and thus an identifiable natural

assignable to a person. In addition, for example, data of the home

and water consumption information about the number of people present,

the periods of their presence and absence, the use of certain rooms

as well as allowing conclusions to be drawn about the heating behavior of the occupants. The

Consumption data are therefore to be regarded as personal data.

According to Art. 15 DS-GVO, the person concerned has a right from the person responsible

to obtain information about whether personal data is being processed

be served. If this is the case, the person responsible has information about it

this personal data and the supplementary information

to be granted in accordance with paragraph 1.

Affected rights such as the right to information in accordance with Art. 15 DS-GVO are included

however, according to the wording of the law, always towards the person responsible

to assert.

The person responsible within the meaning of the General Data Protection Regulation is

who alone or jointly with others about the ends and means of

Processing of personal data decides (cf. Art. 4 No. 7

1st clause DS-GVO). In the present constellation, this represents the

The landlord or the property management. They decide

namely, among other things, which device is used, in which rhythm the results

raising the meter readings and preparing the utility bill

he follows. The measurement service provider, who only works on behalf of the lessor

the landlord or the property management collects and manages data is in

In this context only processors according to Art. 4 No. 8 DS-GVO.

This is dependent on the responsible person's instructions and acts

as a "supporting tool" for the client.

The lessor/the manager therefore remains responsible for data processing.

tenant or the property manager. The processor only has the

Obligation according to Art. 28 Para. 3 S. 2 lit. e DS-GVO, the person responsible in the

Answering requests to exercise the rights of data subjects

support. The person responsible can therefore instruct the contractor

provide the necessary data and information to him,

so that he can provide his tenants with complete information or also

instruct the contractor to provide the information. addressee

of the request for information is the person responsible, i.e. the landlord

Landlady or property management.

I have therefore pointed out to the tenants that they should

entitlement to the future against their respective landlords/property management companies

and not applicable to the measurement service provider as a processor

to have to do.

4.5.3

Results of the check for compliance with data protection regulations

Auto repair shop regulations

Modern motor vehicles generate more and more data. Many of them will

needed in the workshop for inspection, service or repair.

Purely technical data is also personal data if it is about the

Vehicle identification number with owner data or customer data

be linked. In June 2017, a nationwide examination of

Auto repair shops through six supervisors to process

To understand vehicle data and the relevance of data protection law

and compatibility study, on which this joint report is concerned

relates.

From my department were 20 workshops to answer one

extensive catalog of questions. Ten of the audited workshops

ten were those of a car manufacturer based in Hesse, others

ten authorized workshops from various automobile importers.

Among other things, the workshops were asked which personal

The data obtained is read out of the vehicle during a visit to the workshop

and stored in the workshop's data processing system.

Central topics of the survey were the legal basis for the data

processing, the transfer of data to the manufacturer or to others

Third parties such as insurance companies and customer information

about processing their motor vehicle data. The answers of the

sites of all participating federal states were evaluated anonymously.

The result showed that data processing is mandatory for repair,

Service and maintenance required data including data transmission

the manufacturer is permitted in accordance with Article 6 Paragraph 1 Clause 1 Letter b GDPR. For

in these cases there is no consent to data processing

Need. Some workshops still had approval for one

Data processing presented, but it was so broad that it was a lump sum

consent to any data processing. this consent

was also linked to order acceptance. This practice violates

however against the data protection regulations. For one thing, she has to

Consent to data processing to be earmarked. It must be from the

It should be clear which data is collected and for what purpose

and how they are processed. On the other hand, the submission of an

Consent must be voluntary, i.e. it must not be linked to any disadvantageous consequences

become. Acceptance of the motor vehicle for repair may not be excluded

be made dependent on whether the customer signs the consent.

The DS-GVO stipulates that the customer in a precise, transparent, ver-

receives information in a comprehensible and easily accessible manner

relate to processing. The workshops stated that information

Information on data processing either in the operating instructions or

are present in the declarations of consent or the customers through

service staff would be informed. I recommended the workshops to

information sheet on data processing to customers with the content according to

Art. 12, 13 DS-GVO or to be printed on the order.

More difficult to answer was the question on what legal basis

lay the linking of the technical data with the name of the customer

or may be transmitted with the vehicle identification number. Many

The transmissions take place on the basis of the fulfillment of the contract within the framework of the

Workshop contract in accordance with Article 6 Paragraph 1 Clause 1 Letter b GDPR. Below falls

For example, in the case of guarantee, warranty and goodwill cases, the

tion of the reimbursement by the manufacturers and the consultation of the

manufacturer in the event of particular difficulties in the context of specific repairs

manuals (technical hotline, vehicle diagnostics/telediagnostics).

122

Data protection report from 05/25/2018

The data protection legal basis for the data processing of the required

relevant vehicle data for product monitoring/product monitoring

and for possible product recalls is Article 6 Paragraph 1 Clause 1 Letter c GDPR. It

here lies the fulfillment of a legal obligation of the automobile manufacturer

lers from the Product Liability Act. Since constellations are conceivable here

are in which both the workshop and the manufacturer have the same data

of the customers process for their own purposes would be a common one

Processing according to Art. 26 DS-GVO conceivable, with the consequence that

the workshops and the manufacturers in a joint agreement

specify who is to comply with which information obligations.

For data processing for the purpose of product/quality improvement

6 (1) sentence 1 lit. f GDPR

be used. The same applies to data processing in the context of

Marketing campaigns and customer satisfaction surveys. These could

However, it can also be processed anonymously.

In contrast, the central management of an electronic maintenance

and repair history at the car manufacturer (digital service record)

only be carried out with the explicit consent of the owner. same

applies to participation in customer remuneration and bonus programs.

The audit showed that the workshops are hardly aware of which ones

Data they collect for what purposes and forward it to the manufacturers. The

Data processing for own purposes and for purposes assigned to the manufacturer

serve are perceived as not separate from each other. Thus missing

it is also often a matter of properly informing customers and

a proper agreement between workshops and manufacturers.

4.6

healthcare

4.6.1

Examination of the information according to Art. 13 DS-GVO im

health sector

Information according to Art. 13 DS-GVO must above all be specific and trans-

be parent. In the health sector, the information is for those affected

generally communicated in paper form, so that they have the opportunity

take them with you for further viewing. In addition, consent from the

to separate information according to Art. 13 DS-GVO.

In the context of complaints and advice questions I received numerous

Documents to fulfill the obligation according to Art. 13 DS-GVO submitted for examination

lays. These were documents from a wide variety of

health areas such as B. from (dental) medical practices, psychotherapists,

Hospitals, medical supply stores, physiotherapists, nursing services,

Naturopaths, medical clearing houses and health authorities.

During the examination, it turned out that when the information

flyers largely make the same mistakes.

So I often had to point out that the information provided to the patients

and patients or customers in paper form

are. Because health is fundamentally about personal

(treatment) contracts to be concluded, information is sufficient

the homepage of the person responsible alone. But also a notice

does not meet the requirement of “easily

accessible form" of Art. 12 Para. 1 DS-GVO. In my view, however

a media break is permitted in the form that in the flyer on more extensive

Information on the Internet is referenced.

I consider the approach of providing information according to Art. 13 to be fundamentally inadmissible

To mix DS-GVO with declarations of consent. Here is usually

informed in a document according to Art. 13 and at the end the consent in

the data processing listed throughout the document is required. From

those responsible will use the arguments of "simplicity" and

"Paper economy" in the field. In addition, it is argued that

the patients and customers not with too much

wants to "overburden" bureaucracy. However, it is overlooked that the

Data in the context of treatment in principle on the basis of Art. 9

Paragraph 2 lit. h GDPR are processed. A consent to the processing

is therefore not necessary. The information according to Art. 13 DS-GVO about the

Processing, on the other hand, must relate to all types of processing

be communicated, regardless of whether this is due to a legal

basis or consent. When mixed, the

Those affected are thus usually prompted to enter into a legally permitted procedure

to consent. Moreover, such a mixture leads to the fact that

the principles of transparent,

understandable and easily accessible form of information often not

can be complied with. In these cases, it is straight for those affected

made it difficult to differentiate which processing operations they are performing

influence his consent.

124

Data protection report from 05/25/2018

Measures taken

I took the exams as an opportunity to write these and other mistakes in

a "Checklist to prevent the most common mistakes in the application

of Art. 13 GDPR in the health sector". This

I have a list on my homepage under the link: https://datenschutz.

hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/

checklist-to-prevent-the-most-common published as a practical help.

4.6.2

Non-treatment in case of patient refusal

Patients to sign the info flyer according to Art. 13 DS-GVO

Doctors and other health professionals

must not refuse, discontinue or threaten treatment if

the patient refuses the information according to Art. 13 DS-

to sign GMO.

After the introduction of the obligation by the GDPR, the data subject

about the processing of your personal data according to Art. 13 DS-GVO

to inform, numerous cases were reported to me in which doctors

Doctors refused the patients (further) treatment,

because these require receipt or acknowledgment of the information pursuant to Art. 13

DS-GVO did not want to confirm with a signature.

In these cases, the paper was mostly returned after the signature was granted

taken to the doctor's documentation without the patient having a copy

who received the information. In many cases I have also been told that

Practice staff unnerved by questions about the paper and the purpose of the

signature respond. The paper was also given to patients on request

and patients not explained. In these cases, the patients

Patients then informed that treatment would be available without the signature of the

information not possible.

Even before the GDPR came into force, the supervisory authorities

Agree that a signature for proof of issuance of

Information according to Art. 13 DS-GVO is not required. The patient must

the information is communicated according to Art. 13 DS-GVO, an acceptance obligation

does not exist for the person concerned. I have that in mine too

Information paper on the "Implementation of the information obligations according to Art. 12

and 13 DS-GVO in the field of health professions" on my homepage

(https://datenschutz.hessen.de/datenschutz/gesundheits-und-

social affairs/healthcare/info-duties-according-to-ds-gvo). From my

It is sufficient to prove that the information has been provided that the

Issuance noted by the person responsible or a concrete procedure

regarding the implementation of the information obligation is recorded in writing.

Doctors are therefore allowed to stop treatment if the patient refuses

entin or the patient, the acknowledgment of the information according to Art. 13

Confirm DS-GVO by signature, do not reject.

However, it is not entirely unproblematic that the question of treatment

refusal is not in itself of a data protection nature, but

the design of contractual freedom between members of the

health professions and patients. According to Art. 7

Paragraph 2 sentence 2 of the professional regulations for doctors in Hesse

the doctor can stop the treatment of a patient

Patients refuse unless an emergency or special legal

there is an obligation to treat. I therefore have the problem with

discussed by the State Medical Association of Hesse, with the result that in the future

refer cases of treatment refusal to them.

In the cases of treatment refusal reported to me, I

from those responsible the information papers according to Art. 13 DS-GVO

submitted and pointed out my legal opinion. In all cases

the doctors were insightful and have their information papers

revised. The refusal to receive treatment or the threat of it

however, mostly disputed.

Due to the frequency of such cases, I have added a

conclusion of the DSK (https://www.datenschutzkonferenz-online.de/

media/dskb/20180905_dskb_aerzte.pdf).

4.7

economy, associations

4.7.1

The implementation of the GDPR in small and medium-sized companies

The reform of data protection law has particularly affected small and medium-sized companies to great uncertainty and not infrequently to being overwhelmed tion. This was reflected in the reporting period on the one hand in the strong increased number of complaints, but above all hundreds of tele- phone and written requests for advice from small companies all sectors (trade, crafts, industry, service providers, etc.). Most The questions and concerns of the small companies always revolved around the same subjects.

Over 99% of the companies in Germany belong to the so-called small and medium-sized enterprises (SMEs) that have no more than 250, often still have significantly fewer employees. Although the privacy right for decades, also for small and medium-sized companies applies, my supervisory practice unfortunately showed again and again that from often do not attach too much importance to data protection became. Only with such small companies, their business purpose precisely the processing of data is, took and takes the attention of data protection requirements regularly have a high priority a. The vast majority of small and medium-sized companies however, processes personal data only as a means to an end to be able to carry out the actual activity of the company effectively or to manage the customer, employee and other business to organize data. These companies lacked in the past

often the awareness and sometimes also the understanding that

data protection law with its diverse requirements also for theirs

activities applies.

With the reform of data protection law and the application of the GDPR since May

In 2018, however, the topic also came to the fore among small and medium-sized companies

suddenly strong in focus. This was certainly also the most extensive

owed to media reporting, which (often in overdramatic

render Form) Problems and possible consequences of the new data protection law

summoned. Although the European legislator from the entry into force of the

DS-GVO has a period of two years for preparation before it comes into force

to the new rules, many small companies

only take effect a few weeks before they come into effect, or in some cases even only

then the urgency of implementation. So are many companies that do it

The topic of data protection has so far been completely ignored or largely neglected

woke up during 2018 and met for the first time, or

at least for the first time to the required extent, with their data protection

legal obligations. This can certainly be considered one of the achievements of

data protection reform.

In countless written and several hundred telephone inquiries

small and medium-sized companies have asked questions about data protection

and my authority for advice on the implementation of the new data protection

right in their establishments. In addition, my employees

various lectures and workshops, which are primarily aimed at small and medium-sized

Companies addressed, extensive tips and hints for implementation

given of the new rules. The questions raised by the companies

were asked were mostly of a very basic nature and repeated

again and again in terms of content:

– Does the company need a company data protection officer?

– What are the information obligations and how do they have to be fulfilled?

– For which processes is an express consent of the persons concerned

required and what should it look like?

– What are the technical requirements for certain types of processing?

– What is order processing and in which cases does it exist?

– What is the record of processing activities?

– What are the consequences and sanctions for a company in the event of violations?

In the consulting practice it became apparent that many small and medium-sized

have little or no experience with the topic of data protection

had done. Although many requirements have changed compared to the old legal

situation have hardly changed, was very often after data protection law

principles that have been in force almost unchanged for years and

which accordingly has actually been around for a long time by the companies

should have been taken into account. Many questions also became formalities

that were newly introduced or changed with the GDPR. Last-

res suggested in part that some companies

certain formal requirements that are relatively easy to implement

wanted to fulfil, but unfortunately little about the basics of data protection law

noticed or understood.

Concerns were also often raised by small and medium-sized enterprises

and fears of additional bureaucracy on the one hand and

on the other hand, from alleged fines in the millions and expensive warnings

voiced. Especially the fear of the latter, fueled by lurid

reporting and dubious advisors, often resulted in

activity, sometimes also in exaggerated activism or resignation. In

In some cases, my employees were also clearly displeased with the

new rules and the associated effort involved in implementation

contrary, occasionally in a very coarse and impolite form.

The great legal uncertainty that prevailed in many smaller companies

and in some cases still prevails, was often accompanied by the expectation that

to be comprehensively advised and supported by the supervisory authority.

In view of the flood of inquiries, it was and is me and my employees

however, it is not possible to send all requesting companies in the

to the desired extent to advise you individually on your data protection issues. On the

I offer my authority's website on various data protection regulations

Topics and in particular on the data protection reform a variety of general

Notes, basic papers, helpful tips, and answers to common

asked questions, which e.g. also to small and medium-sized companies

judge. In addition, the companies find

operational data protection officers and external data protection consultants

Support and individual advice. Also many associations and chambers

support their member companies with industry-specific information

in the implementation of data protection requirements.

Towards the end of 2018, the number of requests for advice from small

and medium-sized companies, but they are at the level of the advantages

years still clearly exceeded. Whether the decline is due to this

is that companies are now better positioned when it comes to data protection

are, or that the interim panic on this subject again

flattened cannot be detected. In most small and medium-sized

In any case, data protection is likely to change over the course of the reporting period

increased awareness and many companies already have

good job in implementing the new data protection law.

4.7.2

Rights of data subjects according to the GDPR

lawyers

Affected persons can assert their rights towards lawyers

assert the DS-GVO. However, with information or

future claims not the opposite party and the opposing lawyers

to be explored.

I received several complaints in which those affected

and information according to the GDPR about your personal data

coveted by lawyers.

Among other things, a petitioner wrote to me that the lawyer did not give him any

Privacy Policy sent and therefore not about his rights and

obligations from the DS-GVO. Another petitioner complained that

that his inquiries to the law firm despite an appeal

to the new data protection law were unsuccessful. Often absent

in the complaints, however, explanations as to the relationship between the

Petitioners stand by the lawyers - whether it is about their own

lawyers or lawyers of the opposite party.

If there is an attorney-client relationship with the lawyers,

data subject to assert their rights under the GDPR against them.

It should be noted, however, that lawyers generally have the personal

process personal data within the framework of a client relationship

allowed, since the processing is to safeguard the legitimate interests of

client is required (cf. Art. 6 Para. 1 lit. f GDPR).

If there is no mandate relationship with the data subject,

the lawyers due to the lawyer's duty of confidentiality

according to § 43a paragraph 2 Federal Lawyers Act (BRAO) the information

in accordance with Art. 14 (5) lit. d GDPR and the information in accordance with

§ 29 paragraph 1 sentence 2 BDSG refuse. Art. 14 (5) lit. d GDPR provides,

that the obligation to provide information according to Art. 14 Para. 1 to 4 DS-GVO does not apply

exists if and to the extent that the personal data is in accordance with the law

of the Member States to professional secrecy, including a statutory

legal duty of confidentiality, and are therefore treated confidentially

Need to become.

Article 14(5)(d) GDPR

Paragraphs 1 to 4 do not apply if and to the extent

...

d) the personal data in accordance with Union law or the law of the member

States to professional secrecy, including a statutory non-disclosure

obligation, and must therefore be treated confidentially.

Furthermore, § 29 paragraph 1 sentence 2 BDSG provides that the right to

future according to Art. 15 DS-GVO then does not exist, insofar as the information

Information would be disclosed that is required by law or its

must be kept secret by nature. Such a right or a

such a legal provision is provided by the BRAO and the confidentiality regulated in it

The lawyer's duty of confidentiality according to § 43a BRAO.

Section 29 (2) BDSG also regulates the restriction of information

obligation according to Art. 13 Para. 3 DS-GVO and concerns the legal relationship

between the clients of the lawyers and affected third parties

clients, their personal data within the scope of the client relationship

be passed on to the lawyers. The limitation of the information

Clients' obligation to inform the affected third parties

serves to protect unhindered communication between clients

and lawyers.

§ 29 BDSG

(1) The obligation to inform the data subject pursuant to Article 14, paragraphs 1 to 4 of

Regulation (EU) 2016/679 exists in addition to those in Article 14 paragraph 5 of the regulation

(EU) 2016/679 mentioned exceptions, insofar as their fulfillment discloses information

would, by their very nature, especially because of the overriding legitimate

interests of a third party must be kept secret. The right to information

data subject pursuant to Article 15 of Regulation (EU) 2016/679 does not exist to the extent

the information would reveal information that is required by law or

by their nature, in particular because of the overriding legitimate interests of a

Third, must be kept secret. The obligation to notify pursuant to Arti-

kel 34 of Regulation (EU) 2016/679 exists in addition to that in Article 34 paragraph 3 of

Regulation (EU) 2016/679 mentioned exemption not to the extent provided by the notification

information would be disclosed which, by law or by its very nature,

in particular because of the overriding legitimate interests of a third party

have to be kept. Deviating from the exception according to sentence 3, the affected

Notify the person in accordance with Article 34 of Regulation (EU) 2016/679 if the inter-

food of the person concerned, in particular taking into account impending damage,

outweigh the interest in secrecy.

(2) If third-party data is used in the course of recording or as part of a client relationship

If this is transmitted to a person who is subject to professional secrecy, the transmitting party is obliged to do so

Body for the information of the data subject in accordance with Article 13(3) of the Regulation

(EU) 2016/679, unless the interest of the data subject in the information

granting predominates.

Therefore, in many cases I could only tell the petitioners that no

data protection violations are present and the lawyers

omit information and were allowed to refuse information.

4.7.3

Direct mail according to the General Data Protection Regulation

The data protection authorities have the "Application instructions of the data

protection supervisory authorities for the collection, processing and use of

personal data for advertising purposes". Result

is the guidance of the supervisory authorities on the processing of personal

Son-related data for direct marketing purposes under the validity of the

General Data Protection Regulation (GDPR).

The conference of independent data protection authorities of the federal and

of the federal states (DSK) decided on the orientation guide on November 7th, 2018.

It is aimed equally at those affected as well as at advertisers and

the address trade and is the "successor" of the "application notes of the

Data protection supervisory authorities for collection, processing and use

of personal data for advertising purposes", which is to be understood in

September 2014 under the validity of the Federal Data Protection Act a. F. (BDSG

a. F.) had been published.

In a comparison of the new and the old legal situation

It is noticeable that the GDPR has a priority special regulation, as set out in § 28

131

Para. 3 BDSG a. F. was provided, does not know. basis for the assessment

determination of the admissibility of processing personal data is now

a balancing of interests in accordance with Article 6 (1) (f) GDPR, in which the

reasonable expectations of a data subject.

If the general principles according to Art. 5 DS-GVO "fair procedural

wise", "reasonable for the processing purpose" and "in a comprehensible manner

way" and the information requirements according to Art. 13 and 14 DS-GVO

fulfilled, the reasonable expectations are usually adequately

be considerate.

Art. 6 (1) lit. f GDPR represents the central legal basis for the

Data processing in the advertising sector. The regulation is

relevant for any processing within the meaning of Art. 4 No. 2. She captures the

Data processing for own advertising purposes as well as for advertising purposes of third parties and

equally also the commercial data processing for the purpose

of transmission and address trading.

With recital (ErwG) 47, sentence 7, the European legislator

already made a weighing of interests in favor of the advertising industry,

based on the fact that the need for protection tends to be low

publicly accessible address data exists, at least these are not the basic

legally secured positions of the advertiser from Art. 12 and 14 GG

and Art. 15, 16 and 17 GRCh (professional freedom, entrepreneurial freedom,

freedom of ownership) prevails. The legislature has a corrective to this

Art. 21 Para. 2 DS-GVO created, where the persons concerned have a right at any time

Right of objection is granted.

According to the supervisory authorities, a weighing of interests will then be carried out

not in favor of the advertiser if data from a

online imprint for the purpose of advertising.

Although this data is generally accessible, it is not collected voluntarily,

but published due to legal obligation.

In the future, a compatibility check will be carried out in the event of a change of purpose in accordance with Art. 6

Para. 4 GDPR required.

Added to this is the duty of the person responsible, the data subject

to facilitate the exercise of their rights (Article 12 (2) sentence 1 GDPR).

From this it is derived that for the filing of an advertising objection

(also) an electronic communication channel is to be offered. Further that

Data owners and advertisers work together. The information about the

Objection to advertising is therefore from the data owner to the advertiser(s), if necessary

to pass on.

Also negative information, i. H. the information that no data was stored

are to be granted in future in accordance with Art. 15 GDPR.

The full text of the “Advertising” guide is available at

ter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/OH_

Advertisement_Stand_07.11.2018_1.pdf

4.7.4

Development of observance of data protection in associations

The European General Data Protection Regulation has for club representatives,

association officials and also association members to excitement and

security led. Contrary to general opinion, the GDPR has

sung, at the clubs only in a few areas to really substantial

Changes in data protection requirements.

The electronic data processing offers within the framework of the association and association

Bandsarbeit unimagined opportunities for optimal member support

in the context of club management and the organization of club life,

such as B. events and a league operation. Because of the required

In many respects, the amount of time involved in personal commitment

and associations strives to spread the tasks to as many participants as possible

to distribute. This results in a variety of contacts in the work of the association

points with the provisions of data protection law.

The GDPR has been in force throughout the European Union since May 25th, 2018

applicable. It applies to any type of processing of personal data

through organizations. Only in the private and family area is the

DS-GVO not applicable. The GDPR also applies to clubs.

Data is personal if it relates to an identifiable

refer person. In clubs, this is usually the data of their own

nal members or members of other associations, e.g. B. at competitions,

be. A processing of the data is present in every form of their use, be

this through the collection and storage, through the display or the

Disclosure to other members or coaches or through confiscation

of posts. Deletion also constitutes processing. Every association

processes personal data.

The processing of personal data is only permitted if it is for this

there is an explicit legal basis. The possible legal bases

are included in Art. 6 GDPR. Usually the processing of the data

permitted to the extent necessary for the purpose of the association. This

includes accounting, membership administration and implementation

of club activities.

In addition, the data can be processed if this is the inter-

required by the articles of association and the rights of the affected

do not oppose open persons. There is a balancing of interests for this

necessary.

For the processing of personal data that is not strictly necessary

is possible, the data subject can give consent. A consent

can only voluntarily, i. H. without compulsion to be granted. consents must

are expressly granted. Pre-filled crosses are not permitted.

The consent is also freely revocable. Therefore it is not possible

Consents in membership or participation applications or in the articles of association

without including the possibility of not giving consent. The

Consent is therefore required for all processing that is absolutely necessary,

no suitable legal basis.

It is also important that the persons concerned are aware of the scope

be informed in detail of the processing. This can be in an information sheet

and the membership applications. The exact scope of the necessary

Information results from Art. 12, 13 and 14 DS-GVO.

In order to be able to meet the requirements of the GDPR, you must first

be determined which personal data is currently in which way

workflow can be processed and saved. For every processing step

can then be clearly checked whether this is for the purposes of the association

is necessary and who may process the data. The result can do this

be used, the obligation to create a directory of

To fulfill processing activities according to Art. 30 DS-GVO and also the

corresponding data protection notice according to Art. 13 and 14 DS-GVO correct

to create.

The appointment of a data protection officer is necessary for ten or more persons

manoeuvrable, who are constantly involved with automated data processing.

These are primarily the association bodies and people in accounting,

but also trainers and supervisors who receive electronic lists of members or players

be made available. Even if a data protection officer

is not absolutely necessary, this can be very important for compliance with the GDPR

to be useful.

It is also necessary to check whether data security is guaranteed in club life

is. To do this, it is advisable to take stock of the devices on which

Data are stored and checking access rights. mobile devices

such as laptops should be equipped with encryption software

the. Are the club's data processed on devices that are also used by

Non-association or board members (e.g. family PC of the first

seated) are used, the club data may be shared with other users

not be accessible. This can be done by encrypting the data or

stored in a protected area.

Despite the essentially unchanged legal situation, the entry into force

the DS-GVO are extensively reported. This has increased the

perception of data protection among club representatives. Unfortunately has

this also to some actions in the permission and use of

photographs that are not justified by the GDPR.

Clubs and their members would like their results in writing and

post image. The interests of the persons concerned are also important

take into account. Have the persons concerned in the publication

of text and images, this is permissible. Consent can

be included in participation applications or player passes. The Consents

must, however, be granted voluntarily and must therefore not be compulsory

may still be hidden.

About public events may also without express consent

be reported in text and images if the focus is on the event

grund stands and individuals are not shown. Without consent

results may also be published. But reporting is allowed

only as long as there is an interest in the public, that is

for a very limited period of time. A permanent release without

Consent is therefore ruled out.

Clubs still have to make considerable adjustments. This

results, however, above all from the fact that many clubs before the entry into force of the

DS-GVO were far removed from the requirements of the previously applicable

Regulations from the BDSG a. F. to meet. From this resulted and results
a greater need for adjustment. However, this is not based on the
regulations of the DS-GVO, but in omissions of the past.
Clubs are still struggling to meet the requirements of data
to fulfill protection. An important reason for this is the partially missing
acceptance of these requirements. My callers often walk away
from that the requirements of the volunteers in the
associations are not fully achievable. However, these requirements are
like other laws - for example the road traffic regulations,
environmental protection and association law – by all members
to fulfill a community. As European law, they are also subject
not the dispositional authority of the nation states. Nevertheless, I'm going here

Present with a sense of proportion and do not make excessive demands, above all
not in terms of time. In addition, I am also available in an advisory capacity.
Because ultimately the requirements of the GDPR must be met by all clubs
and the Board of Management is initially responsible for this, I advise everyone
Associations to appoint a data protection officer. This
also applies if there is no legal obligation to place an order. min
least, each association should designate a person who is aware of the topic
Privacy accepts.
The clubs have given me a lot of inquiries in the last reporting period
burdened. Many of these requests are still pending.
However, more and more brochures for clubs are being published

which provide answers to most and most typical questions.

4.8 Debt collection, credit bureaus

4.8.1 Permissibility of the transfer of personal data by the Credit industry to credit bureaus

For the transmission of personal data to credit agencies by Kreditinstitute usually does not require the consent of those affected.

During the reporting period, many of those affected put the question to me asked whether their credit institutions are allowed to transmit data to credit bureaus, even if they have the "consent" submitted by the banks and savings banks Declarations of Indemnity" would not sign.

As it turned out when the facts were examined, it was so-called "declarations of consent" in all cases for information write informing those affected that the Banks personal data such as the conclusion of current accounts, credit or credit card agreements to credit bureaus. In In no case were they actually declarations of consent.

Unfortunately, I had to realize that in some cases on the part of individual consultants ter the impression was given to their customers that the signature of this information letter on the continuation of business relationship is required.

In a form described here as an example with the designation "Transfer of data to SCHUFA and exemption from banking secrecy" it is merely an information letter that the bank sends to you

Data protection report from 05/25/2018

Customers to fulfill the obligations according to Art. 13 DS-GVO

must ask.

The bank states the legal basis for the transmission of the

Data to the credit agency is based.

The customers are asked in the letter to hand over the

Confirm information to the customer. This is only done for

Proof of compliance with the requirements of Art. 13 GDPR. Therewith

was, contrary to statements by bank employees,

no consent to the data transfer given. Also, the signature

not required by data protection law in the case of a copy of the letter.

In terms of content, however, the document is not objectionable. The bank calls

the correct legal bases on which a transfer of your data to the

Credit reporting can be supported. In this respect, the bank comes through the

delivery of this information sheet to the aforementioned information obligations

and can also prove this after the customer has signed it.

However, the signature is not required for data processing.

The legal bases on which the bank transfers personal

general data to credit agencies, the regulations of Art. 6

Paragraph 1 lit. f GDPR.

Art. 6 Para. 1 GDPR

The processing is only lawful if at least one of the following conditions

conditions are met:

a. The data subject has their consent to the processing of data concerning 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 which the

Controller is subject to;

i.e. 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.

Point (f) of the first subparagraph shall not apply to public authorities in the performance of their duties

processing carried out.

For example, before concluding a credit card contract, there is

an active business relationship on the part of the bank is a legitimate interest

to find out whether the borrower already has other liabilities

and/or whether and how these may have been returned. Therefore the

Collect bank data from the credit agency and conclude accordingly

of such a contract then also to them.

This procedure is therefore not approved by my authority under data protection law

objected to.

4.8.2

The implementation of the "Code of Conduct" in the area of credit bureaus

After the GDPR came into force, the “Rules of Conduct for the

Review and deletion periods of personal data by the German

Credit agencies” (Code of Conduct) as part of a voluntary

Commitment according to Art. 40 DS-GVO the legal regulations

on the checking and deletion periods in the area of credit bureaus.

The subject of a large number of incoming complaints is the deletion

of entries on claims in the database of credit bureaus. Through

the entry into force of the DS-GVO is, however, the formerly in § 35 para. 2 sentence 2

No. 4 BDSG a. F. contained verification and deletion period for claims no longer apply.

Up to and including May 24th, 2018, credit agencies had to

Sentence 2 No. 4 BDSG a. F. the data they store when they are done

Matters at the end of the third calendar year or in the case of unresolved issues

facts at the end of the fourth calendar year beginning with the

calendar year, which followed the initial storage, to ensure that

whether longer storage was required. The result

this test could depend on various factors and

did not always have to immediately, even with settled claims

result in cancellation of the claim. For example, one was longer

continuous storage permitted if information about payment disruptions

in the past, even after they have been dealt with, there is still a considerable

could have informative value about the creditworthiness of the person concerned.

With the date of May 25, 2018, the "Code of Conduct" of the association "Die

credit bureaus e. V.”, which represents the interests of the major German business

representing credit bureaus, by the state commissioner for data protection

and Freedom of Information North Rhine-Westphalia (LDI NRW).

The "Code of Conduct" is a code of conduct that is

As part of a voluntary commitment in accordance with Art. 40 DS-GVO

not replace legal regulations, but rather for the area of economic

substantiate credit bureaus. Approval by the LDI NRW

was preceded by a decision of the data protection conference, so that ensured

is that the approval of all German data protection supervisory

authorities.

Due to many complaints regarding the storage of receivables

In practice, the insurance data are those under Section II No. 1a) and b) of the “Code of

Conduct” provisions are of importance. The Code of Conduct

regulates under number II no. 1a) that personal data about overdue and

undisputed claims remain stored as long as they are not settled

was announced. The need for ongoing storage

is transmitted three years to the day after the occurrence of the respective event

checks. Pursuant to Section II No. 1b) of the "Code of Conduct", deletion will take place

of the personal data then exactly three years after settlement

a claim.

As a result, it can be stated that the "Code of Conduct" in particular

through its reference to a day-specific deletion, the application of the law

simplified, the storage period shortened and for transparency regarding

which contributes to checking and deletion periods. So, under the voluntary

Commitment clearly defined standards created in the field

of the credit bureaus guarantee a uniform application of the GDPR.

4.9

Internet

4.9.1

Publication of employee photos

If employee photos are published, a written declaration

consent of the affected employees within the meaning of Section 26 (2) BDSG

to be required. The possibility of withdrawing consent pursuant to Art. 7

Para. 3 GDPR must be observed.

In the reporting year, I received numerous inquiries about how to do it in the future

data protection compliant with the publication of photos of employees

to deal with. So far, the Art Copyright Act (KUG) was applicable here,

according to the subsidiarity clause of § 1 Para. 3 BDSG a. F. as area

specific regulation took precedence.

The General Data Protection Regulation (GDPR) has been in effect since May 25th, 2018

as a regulation under European law, application priority over national law

enjoy. This means that the question of the applicability of the KUG is being discussed again.

Art. 88 GDPR contains an opening clause for data processing in

Employee context, due to which national legislators are more specific

regulations can be issued. The German legislator has of this

Right exercised and in § 26 BDSG the data processing for

Purposes of employment regulated, but without being specific

to address the issue of the publication of employee photos.

Legal bases for the processing of employee photos

§ 26 paragraph 1 BDSG

Personal data of employees may be used for the purposes of the employment relationship
be processed if this is necessary for the decision on the justification of a
employment relationship or after establishing the employment relationship for his
implementation or termination or to exercise or comply with any law
or a collective agreement, a company or service agreement (collective agreement)
resulting rights and obligations of employee representation are required
is. Employees' personal data may be used to uncover criminal offences
only be processed if there are actual indications to be documented
justify suspicion that the person concerned committed a criminal offense in the employment relationship
has committed, the processing is necessary for detection and the protection-worthy
the employee's interest in the exclusion of processing does not prevail,
in particular the type and extent are not disproportionate to the occasion.

Section 26 (1) BDSG – Necessity

Section 26 (1) BDSG requires data processing to be carried out
of the employment relationship is "required". necessity means
that the legitimate interests of the employer worthy of protection
of data processing and the personal rights of the employee
are to be brought to a gentle balance that is as beneficial to both interests as possible
largely taken into account. A balancing of interests is therefore necessary
between the interests of the employee and those responsible
position in terms of a proportionality test.

Section 26 (1) sentence 1 BDSG then serves as the legal basis only for the
Considering that the visual presentation of the employee(s)

status of the employment contract, such as for a photo model.

Should, however, "normal" employees in the public presentation

of the company in the form of images or film sequences

this is not usually done to carry out the employment relationship

necessary, as it mainly serves advertising purposes.

140

Data protection report from 05/25/2018

§ 26 paragraph 2 BDSG - Consent

§ 26 paragraph 2 BDSG

Is the processing of personal data of employees based on

of consent, for the assessment of the voluntary nature of the consent, in particular

or the dependency of the employed person in the employment relationship

as well as the circumstances under which the consent was given.

In particular, voluntariness can exist if the employed person has a legal

cher or economic advantage is achieved or employer and employed person

pursue similar interests. The consent must be in writing, unless otherwise

another form is appropriate due to special circumstances. The employer has

employed person about the purpose of the data processing and about their right of withdrawal

according to Article 7 paragraph 3 of Regulation (EU) 2016/679 in text form.

According to Section 26 (2) BDSG, the lawfulness of the processing can be based on a

transparent and comprehensive consent of the employee

become. The provision regulates the conditions for consent in employment

specific area based on Art. 88 DS-GVO. to note

are as process standards Art. 6 Para. 1 lit. a DS-GVO and Art. 7 DS-GVO.

Art. 6 Para. 1 GDPR

The processing is only lawful if at least one of the following conditions

conditions are met:

The data subject has given their consent to the processing of their personal

personal data given for one or more specific purposes

Art. 7 GDPR

(1) If the processing is based on consent, the person responsible must prove it

can that the data subject in the processing of their personal

data has consented.

(2) If the consent of the data subject is given in the form of a written declaration that

other facts are concerned, the request for consent must be intelligible

and easily accessible form, using clear and plain language, in such a way that

it is clearly distinguishable from the other facts. are parts of the statement

not binding if they constitute a violation of this regulation.

(3) The data subject has the right to revoke their consent at any time. Through

the withdrawal of consent will invalidate the legality of the consent

processing that took place up until the revocation is not affected. The person concerned will

informed of the submission of consent. The withdrawal of consent

must be as simple as giving consent.

(4) When assessing whether consent was given voluntarily, the circumstance in

to the greatest extent possible, whether, among other things, the fulfillment

of a contract, including the provision of a service, from consent

to a processing of personal data which is necessary for the fulfilment

of the contract are not required.

According to this, the consent must be given before publication and informed,

This means that the individual uses must be specified precisely,

the manner in which the image is presented must also be regulated.

This is of great importance for the effectiveness of a given consent

criterion of voluntariness. This can then be accepted in particular

become, “if for the employed person a legal or economic

Advantage is achieved or employer and employee alike

pursue interests". About these situations explicitly mentioned by law

In addition, a voluntary decision by the members

workers to go out when they have a real choice. This would be

e.g. B. to accept when employees publish their

You can also reject photos without having to fear any disadvantages.

According to § 26 paragraph 2 sentence 3 BDSG, the consent basically requires the

Written form. Section 26 (2) sentence 4 BDSG requires that those affected understand the scope

to assess their decision.

Art. 7 Para. 3 DS-GVO should be emphasized, according to which those affected have an explicit

and a right of revocation at any time is granted, to which prior to delivery of the

consent must be indicated. As this may cause problems

it is recommended that the question of the obligation to delete be addressed at the time of issuance

to regulate the consent.

Submissions that are available to my authority have so far regularly concerned the

Facts that an employee from the company

has been eliminated, but her/his picture is still on the company's website

is published. If the publication is based on § 26 paragraph 1 sentence 1

BDSG, the purpose falls when the employee leaves

for publication, with the result that Art. 17 Para. 1 lit. a DS-GVO

applies: "The personal data are necessary for the purposes for which they are

collected or processed in any other way is no longer necessary."

More problematic is the case when an employed person already has their

lawfully granted consent to the publication of their image

and the employer a possibly costly advertising campaign

must stop/delete.

According to the case law of the Federal

labor court (BAG judgment of 11.12.2014 - 8 AZR 1010/13) the KUG

application reached. After this was in the case of revocation of consent

to make an overall assessment in the publication of image material

and to require the employee to state a reason

why he/she now has his/her right to informational self-determination

want to exercise in the opposite direction.

In the case of the BAG it was about a company video that was purely for illustration

purposes served. In the opinion of the BAG, the

Intensity of intervention in the personal rights of the (former) employee

tigten: The picture only had an illustrative character and hardly had anyone

relation to the personality of the person concerned, the employee could

not request the deletion. The connection also had to be taken into account

of the picture with further information about the employee. Will about

the identity of the employee is emphasized by a text

raised, called her/his name or just with her/his affiliation

recruited to the company, although she/he has already left,

there is in any case a legal right to erasure.

I am of the opinion that these ratings of the BAG also under the

Application of the DS-GVO and the new BDSG continue to apply, so that the

employed person must continue to justify the revocation of consent

and then the weighing of interests mentioned above would have to be carried out.

This legal opinion can be supported e.g. on the principles of

Good faith and duty of care under labor law.

Since the existing right of revocation only takes effect from the time of revocation and

therefore, once a photo has been published, it cannot be undone

can be made and, moreover, does not always lead to the

Publication for the future should be about the exact

Conditions already informed in the context of granting consent

become.

4.9.2

Data economy through the GDPR: Radical changes to the

DENIC e. G. when registering German domains and at

Whois information

DENIC e. G. has the

Registration process for DE domains completely redesigned. radical

Changes were also made to the so-called “Whois service”, the

previously an almost unlimited query of the data of domain owners

and the persons responsible for the domain. This query

opportunities were provided by DENIC e. G. in terms of sustainable

Data minimization and avoidance significantly restricted. in the environment

My authority was involved in the design process in an advisory capacity.

DENIC e. G. in Frankfurt am Main is the central German procurement

and registry for Internet domains below the "country code

Top Level Domain" (ccTLD - country-specific Top Level Domain) ".DE",
such as B. "hessen.de" or "datenschutz.de". DENIC e. G. operates in
Within the Domain Name System (DNS) the primary name server for
all currently more than 16 million Internet domains with the domain ending "DE".
The hierarchically structured DNS system ensures that every
Internet address unique and uniquely addressable is what is the basis of each
internet offer and every internet use. Members of DENIC e. G.
are Internet Service Providers (registrars) who serve their customers among other things
the registration of one's own DE domain at DENIC e. G. and
often also the storage space for a corresponding homepage in the world
Wide Web (WWW/Internet) on the provider computers and others with it
offer related services. Registration of the desired
Domain of the often private end customers at DENIC e. G. takes place via
these internet service providers (registrars).
For the registration of a domain, DENIC e. G. so far next to
the required technical data always include the specification of the name
and address of the applicant/organization (domain owner)
as well as the corresponding information on the administrative contact person (as
person legally responsible for the domain residing in Germany
and addressee for queries) and to the technical contacts.
The data on the domain owner and on the person of the administrative
spokespersons were listed in the Whois database of DENIC e. G. saved
and were via the Whois service until before the GDPR came into effect
on the DENIC e. G. Accessible worldwide without restrictions. The

DENIC was responsible for the daily number of whois data accessed by third parties

at about 12,000. So every month the data from

DE domain owners and the personal data of administrative

ven contact persons of DE domains via DENIC's Whois service

e. G. queried on the WWW and sent to the users of DENIC's Whois service

e. G. transmitted. For what purposes these queries are made in each case

remained unknown because - as was previously the case with all Whois services worldwide

of the domain registration offices – neither an identification nor

thetification nor the indication of a legitimate interest of the query

was made.

This has repeatedly led to problems in my office in recent years

Entries of affected domain owners and administrative contacts,

in which those affected criticized the publication of their data because they

feared their misuse or for other reasons a secrecy

asserted a need for service (cf. also the submission of the state government

regarding the thirteenth report of the state government on the activities

the one responsible for data protection in the non-public area in Hesse

regulators; LTDprints. 15/1539 of 08/30/2000, no. 9.2 and 9.3). There

for the domain owner or the administrative contact person as direct

Contract partner of DENIC e. G. however as part of the contract (cf. § 28

Paragraph 1 BDSG old) also the local domain guidelines and the domain

Conditions applied in which the internationally customary publication of the

Data provided via the Whois service failed the complaints

cannot be remedied by my authority. A right to an anonymous

In any case, domain registration is not permitted under data protection law

derive The persons concerned were therefore regularly recommended by my authority

foal, an authorized representative such as B. a lawyer at the

DENIC e. G. to register, so instead of their own data

Data could be retrieved via the Whois service.

At DENIC e. However, G. was always very closely observed as to how

the critical discussion about the Whois service in recent years

developed at European level and what efforts in particular

the European data protection authorities about the so-called Article 29 data

protection group to ICANN (“Internet Corporation for Assigned

Names and Numbers”, which coordinates the assignment of unique names

and addresses on the Internet, organizes the "Domain Name System" and the

corresponding assignment of IP addresses, also regulates the Whois service)

undertook to ensure the hitherto almost unlimited publication in the future

personal data of domain owners and administrative

interlocutors of domains to prevent or at least to effectively

restrict. For DENIC e. G. it was foreseeable that the European

European Data Protection Board (EDPB) as

successor body to the Article 29 Working Party

to curtail the Whois service under the data protection

improved framework conditions of the GDPR would continue. Under the

Impression of this discussion on an international level and against the background

the forthcoming revision of European data protection law

due to the DS-GVO on May 25, 2018, DENIC e. G., her

Data collection and processing in connection with registration

from DE domains to be significantly more data-efficient from this date.

The Whois service of DENIC e. G. was at the effective date

the DS-GVO will be amended in such a way that significantly less data is now available

Domain queries to significantly fewer queryers in a new, tiered

procedures are transmitted to authorized bodies. these changes

were presented to me for data protection assessment; the DENIC

e. G. received intensive advice on this.

145

Since the GDPR came into effect on May 25th, 2018,

Providers (registrars) in addition to the necessary technical data to the

DENIC e. G. only the data of the domain owner passed on. This

Domain owner can be a natural or legal person and his

also have offices abroad. Data on the administrative contact person

(always a natural person) and the technical manager

and zone managers are appointed by DENIC e. G. not now

are no longer available there and can no longer be included

DENIC e. G. be queried.

The provider (registrar) through which a domain is requested provides additional information

Two non-personalized e-mail addresses are available for each domain

then be published in a Whois query for the respective domain.

One of the email addresses should be used for complaints against the domain or the

Owner are used (Abuse-Request), the other email address for everyone

other contact purposes (general request). The release of data from

domain owners and administrative contact persons of domains

in these cases, completely without the involvement of DENIC e. G. exclusively

via the provider (registrar) via the e-mail

addresses. DENIC e. G. published in a Whois query next to

only the domain status (registered or

not registered) and some purely technical data on the requested domain.

For the legally unproblematic Whois queries by the domain

Owner himself (to check his data) and by other DENIC members

(in the event of an intended provider change) were my authority

suitable methods are presented:

In the case of queries by the domain owner himself, the domain

E-mail address and zip code provided during registration

become. The query result is given to the query via a time limit

valid link presented, sent by e-mail to the deposited or indicated

email address of the domain owner is sent. For the purpose of

Provider change, an additional password is introduced, which is specified

must be if a provider (registrar, DENIC member) from this

Reason wants to know the owner data.

For other reasoned Whois queries, different PDF

Applications for owner information are offered so that DENIC e. G. before the

Data transmission can check in each case whether there is a legitimate interest on the part

of the requester is available, on which a data transmission to this is based

can be. The completed applications will be sent to DENIC e. G. after

Receipt (letter post, fax) checked and assessed manually. After that granted

DENIC e. G. Domain owner information if appropriate

legitimate interests or reliable legal bases on justified

Application only to the following places:

1. Authorities in the context of their sovereign activity (e.g. in the area of

criminal prosecution, averting danger or garnishment order),

Owner of a name or trademark right through the domain

may be injured

2.

3. Claimants who are in possession of an enforceable title and who

civil seizure of domain contractual claims of the

main holders intend and

Insolvency administrator over the assets of a (also presumed)

domain owner.

4.

In all other cases, DENIC e.G generally does not provide any information

more. Nevertheless, in my opinion, it is still fundamentally

provides that if there is a suitable legal basis from DENIC

e. G. and other violations of rights by a website from the

Provider via the provided abuse address the data of the domain

be issued to those responsible for legal claims to be correct

can be addressed and enforced.

I was given the relevant application forms for advice and

submitted a data protection statement. The new procedure

of domain registration and in particular the limitations of the

Whois service regarding the queryable data and the queryable

right places were expressly welcomed by me. The elevation and

Processing of personal data by DENIC e. G. orients himself

today on the principles of data avoidance and data economy.

DENIC e. G. practices data protection through technology in an exemplary

design i. S.v. Art. 25 GDPR and recital 78 (privacy by design).

The first few months with the new Whois system have also shown

that the number of Whois queries made per application has definitely increased

within limits and that manual processing means DENIC e. G. not

overburdened. Whereas in the past around 12,000 Whois queries were carried out daily by third parties

have been made over the internet, the number of queries has gone through

authorized third parties (authorities, owners of name or trademark rights,

holders of enforceable titles and insolvency practitioners) to around 40 per day

reduced. The new Whois method compared with the

previous procedure, i.e. more than 11,000 transmissions per day

transferred data to third parties avoided. In my opinion, this can be justified

and law as a great success and an exemplary implementation of the GDPR

by the German domain registry DENIC e. G. be rated.

147

The Hessian Commissioner for Data Protection

47th activity report on data protection

4.10

technology, organization

4.10.1

Standard data protection model becomes concrete:

Apply GDPR compliant measures

From the point of view of information technology, there is a series of articles in

of the General Data Protection Regulation (GDPR), the taking and the

Provision of appropriate measures make it necessary so that permanently

personal data is processed in accordance with data protection regulations.

It is inherent in at least the following articles that controllers and
Processors have to decide what is in the information technology
needs to be done and how IT systems are integrated into a company or organization
should be embedded in the organizational structure: Art. 13 to Art. 22, Art. 25,
Art. 30, Art. 32, Art. 35 i. In conjunction with Art. 36 GDPR. In any case, technical
and to take organizational measures (TOMs). With the standard
data protection model (SDM) and its building blocks in an updated
the catalog of measures has been started, various such instructions
to publish.

Standard data protection models and building blocks in the catalog of measures

The Standard Data Protection Model (SDM) provides a method
provides, with the responsible and supervisory authorities in the development,
in data protection advice and in the examination of data processing
be able to assess whether personal data complies with data protection regulations
GDPR are processed. The conference of independent data protection
Federal and state supervisory authorities (DSK) recommended this
model to be used for testing. The manual for the standard data
protection model in the test version (version 1.1) is available for download
at https://www.datenschutz-mv.de/static/DS/Files/Data Protection Model/
SDM-Method_V_1_1.pdf ready (last accessed: 19.11.2018). Through the AK
technology, these and other sources mentioned in this article are
provided and cared for. The corresponding entry can be found at https://
www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

Guide to the Standard Privacy Model is a framework created by
specific actions to be taken to supplement the requirements
to support the GDPR even better from the point of view of information technology.

There will be a so-called module for each such measure.

The first building blocks are available and will be published in the press release

from September 10th, 2019 at https://datenschutz.hessen.de/pressemitteilungen/

press release-on-the-standard-data-protection-model (last accessed: 19.11.2018)

explained. These seven building blocks relate - listed in alphabetical order

Order – on retention, privacy management, documentation,

Deletion and Destruction, Scheduling, Logging and Segregation.

Technical data protection: protection goals

Both the SDM manual and the respective modules for designing

technical and organizational measures are evaluated

goals of technical data protection - the guarantee goals.

The guarantee goals are integrity, confidentiality, availability,

Unlinkability, transparency and intervenability. In every building block

of the catalog of measures it is explained which guarantee objective is to be

Application of the correspondingly described technical and organizational

technical measures can be implemented.

building blocks

The building blocks described below have been approved by regulatory authorities

from Hesse, Mecklenburg-Western Pomerania, Saxony and Schleswig-Holstein

and developed and published by the Evangelical Church of Germany.

They are not a publication of the Conference of Independent Data Protection Supervisors

supervisory authorities of the federal and state governments.

With the ever-shortening innovation cycles in IT development

it is required, the controllers and processors, specifically

make recommendations to the respective IT departments. The test

Exercise of the following building blocks is welcome, with those processings

can be made more GDPR compliant. The naming of the published

th blocks are in alphabetical order – except for the block

Data protection management, in which basic aspects of management and

the permanent, constantly to be evaluated implementation of data protection law

requirements are considered.

Building block: storage

Personal data must be kept. You are from the time

the survey over the entire duration of the legally required storage period

ten until the time of separation (delivery to archives, deletion and

destruction) ready for processing. Therefore, storage includes

the collection, storage and storage of personal data.

The module describes technical and organizational measures for

Storage of personal data in electronic form in operational

ative operation or in the productive system or in paper form. Downtown

The focus is on the guarantee goals of availability, integrity,

intervenability and transparency.

A tiered concept is proposed for data to be retained that

a balance between paper form, storage in operational IT systems

men with any necessary emulation and virtualization techniques as well as

the transfer of data objects into newer digital representations

allows.

In this block the retention of data in the form of a data

backup (back-ups) not considered. To clarify data protection law

Requirements regarding data backup will have their own in the future

Provide a building block in the catalog of measures.

Building block: documentation

From the point of view of technical data protection are with a documentation

to fulfill several tasks, which are essentially the guarantee goal

serve transparency. Depending on the

direction of the documentation is also used or must be taken into account.

These tasks are listed below and briefly explained:

1.

With regard to the use of IT systems for processing personal

There is an obligation to account for the data obtained in accordance with Art. 5 Para. 2

GDPR. The person responsible is obliged to prove that the

data protection requirements according to paragraph 1 there

are complied with, each with at least one data protection law

finalize the term: “lawfulness, processing in good faith

and belief, transparency, purpose limitation, data minimization, correctness

security, storage limitation, integrity and confidentiality”. Apparently

is that a documentation of the processing represents what is processed

and how it is carried out in order to

to meet the requirements of Art. 30 GDPR.

2. The documentation serves specifically - also with regard to Art. 25 and

Art. 32 GDPR –

a. ensuring the transparency of databases,

b. the representation of the transformation of data into an adequate model

dell for the actual organizational and technical implementation

a processing

c. the description of the components used and their functionality

nationalities and interfaces,

150

Data protection report from 05/25/2018

i.e. defining the processes within IT systems, organizational

tion and beyond IT system and organizational boundaries as well

e. the traceability of decisions and in the administrative

act.

Points a and e focus on the previously mentioned “what”. point c. delivers

Information about the "how". The points b and d have connecting

Character. Here the perspective is crucial, whether more the "what" or

more the “how” is considered. So e.g. B. from an organizational perspective

Defining the processes a "how" to make an organization capable of acting

to do and to keep. On the other hand, the same determination from the

perspective of IT, which has to implement IT-supported processes,

an answer to the question "what" to do. Finally, in the

Summary of points a to e make it clear that data protection law

Requirements always only in a cross-organizational and cross-disciplinary way

team can be permanently implemented by the person responsible.

3. For reasons of general traceability, it is advisable to

for the documentation of data protection requirements structural

to make determinations. Such determinations may relate to

a. the structuring of the overall documentation,

b. the processing in paper form or electronically,

c. the adequacy and scope,

i.e. the completeness,

e. the revision strength,

f. the necessary timeliness and also

G. the updating of the documentation.

4. In addition, the documentation for compliance with rights should be

data subjects (Articles 12 to 22 GDPR) can be used, e.g. B.

Processing operations depending on the area of application and application

to specify the case.

In addition to these essential tasks, there is a differentiation in the module

takes place when the processing involves a high risk for rights and freedoms

affected persons exists.

Building block: planning and specification

The aim of this module is to show which activities from operational

rative design of a processing activity in self-evident

way with the implementation of data protection requirements

permit. In this way, reference to a procedure becomes more responsible than the client

taken, in which he plans and explains what and how through an order

taker, e.g. B. also contract processors, is to be provided or in what way

data protection requirements for IT-supported processing

are to be implemented.

In addition to planning, the focus is on the specification of a processing

task. The reason for this is that a specification can be used in many ways in

of IT must be reused in order to have a functional IT and

to maintain high-quality processes in the long run, in the same way

meet data protection requirements. Like from IT development

known, regular comparisons at different levels are one

Processing activity between the target from the specification and the actual

required during operation.

In order to be able to carry out such target and actual comparisons, at least

necessary:

– a description of the processing activity, as also specified in Art. 30

DS-GVO is required,

– a documentation of the legal bases on which the execution

the processing activity takes place,

– a documentation of the person responsible and the participants in one

organization or a company,

– a specification of technical processes,

– a specification of the specialist application with a description of typical applications

events in the area of application of the IT systems and/or their components,

so that involved or potentially unauthorized third parties are identified

can,

– a description of functional and, given in an appropriate form

non-functional requirements and their interfaces, which are required in

way in connection with a risk assessment for rights

and freedoms of data subjects,

– a provision and documentation to be taken or taken

technical and organizational measures and

- A specification for the administration of technical systems and pro-

programs naming the administrators themselves, so that availability

security, confidentiality and integrity even under stress for the whole

operating life of the systems and programs are guaranteed.

Therefore, this building block is used for your own control in the organization or

in the company as well as the verifiability by the responsible data

protection supervisory authority. From an organizational control perspective, it stands

Guarantee goal of transparency in focus. Add to this from view

of information technology

– the guarantee and verifiability of availability, confidentiality

and integrity as well

– the requirement to implement that processing on the basis

of IT-supported processes must also be guaranteed under load.

Building block: logging

With logging, processing that has already been carried out, processing

processing activity or specifically a processing operation. She

serves to test one or more events that have already taken place

have. A comparability between intended and

to establish activities that are also carried out in compliance with data protection

must. From an organizational point of view, it is about the traceability of

technical and/or administrative decisions and their implementation.

From a technical point of view, organizational and technical measures are allowed

consider with which technical and/or administrative decisions in

of IT can be realized. This also applies to the permanent operation of IT. Here

it must be proven that the respective logging is valid, comprehensible,

is up-to-date and complete, with any logging only earmarked

may take place. At the same time, with regard to log data, it must be ensured

make it possible to determine at which level the logging took place

and how, if applicable, the log data belong together. Accordingly is closed

take into account that the implementation of logging in their character

is cross-processing and cross-system.

Depending on whether a processing and / or system-wide

logging is available, a distinction must be made between:

– user activities in a specialist application,

– system activities,

– Administrative activities or also

– Activities via interfaces.

Typical log data is determined by:

- A time component or a time of a to be logged

event or the logged event during operation,

- an indication of an entity - i. i.e. R. with reference to the IT used

System – to record who logged,

– an indication of a reason or a specific event in order to

to record why a log was made and

- An indication of the storage location, so that it can be determined by whom and

at which point was logged.

Thus, the use of logging serves to implement the guarantee

goals of transparency and integrity.

In addition, the earmarking must be guaranteed. With log data is particularly

ders to be handled with care, since in them using IT-supported

Evaluation mechanisms during operation potentially monitoring

not affected persons is created. Therefore, the processing of

Log data only take place in well-defined periods. are accordingly

technical and organizational measures in accordance with Art. 32 DS-GVO

seize. Finally, a corresponding documented

consideration when using logging, e.g. of processing operations

for which log data is stored.

Furthermore, mechanisms for processing log data are also required

consider, to which a filtering, a normalization, an aggregation,

a categorization or a prioritization. Various possible

Various mechanisms for logging are implemented in the block.

Module: delete and destroy

In general usage, deletion describes the inaccessibility

data and includes both reversible and irreversible pro-

cess. In the legal sense, deletion is the permanent rendering unrecognizable

stored personal data using appropriate processes. Here

These processes range from making individuals irreversibly inaccessible

personal data up to the physical destruction of an entire

data medium (destruction). The module describes the data protection

legal requirements.

The module is used to support the guarantee goals of confidentiality

capability, intervenability and non-chaining.

The obligation to delete, taking into account available technology

nologies and the implementation of appropriate measures

active personal data depending on processing-specific

Deletion periods as well as backup copies, log data in IT systems

and temporary data for processing reasons, especially in

IT-supported processes.

Different approaches, taking into account the area of application and

Information technology uses are for deleting and destroying

explained in operational operation in the module.

154

Data protection report from 05/25/2018

Building block: Separation

From a data protection and information technology perspective,

different purposes different powers regarding the processing

processing of personal data. Accordingly, to enforce the

Guarantee goals non-chaining, integrity and confidentiality as well

enforce different separation measures. The deployed

Technology based on data, IT systems and processes must be

based on the stated purpose and the state of the art

set up and operated permanently. Are a completed

Data management or processes to be implemented independently of one another

implement, then the IT system must be multi-client capable.

In this module, seven test steps for client separation are specified,

which can be carried out within the company or organization. On

In this way, it can be independently and automatically assessed whether a

Processing is data protection compliant. These seven steps consist of:

1. a preliminary legal consideration, in particular under

Addition of special legal provisions,

2. an examination of an existing foreclosure requirement,

3. an examination regarding an organization-related separation requirement,

4. an audit-proof design of the transmission of personal

gener data between two clients,

5. an implementation of completed transactions within a man-

dance,

6. an examination of independent configurations of different

dance and

7. a restriction of the cross-client administration of the

worked personal data.

These seven steps are detailed in the building block.

Building block: data protection management

The building block for data protection management has a different character than that

components shown so far. Data protection management aims at one

controlled, managed process throughout the life cycle of a

or several processing activities, as per Art. 30 DS-GVO

manage. The following SDM-based lifecycle is intended to be Responsible

and processors support that data protection requirements

ments, in particular through suitable technical and organizational measures

Measures, specified, documented, implemented, permanently according to the status

of the technology are held, evaluated and verified. The

The associated continuous improvement process can be summarized as follows

Figure "Privacy Management Cycle" showing a permanent

detailed observation of ongoing operations.

Figure: Data protection management cycle

(Source: Building block – data protection management, published on September 10th, 2018)

The individual phases and the necessary activities associated with them

are explained accordingly in the block.

Conclusion and Outlook

This breakdown of the building blocks published to date provides a glimpse into

how the implementation of data protection requirements

with a focus on taking appropriate technical and organizational

rical measures should be taken. Controllers, processors

and IT managers are recommended to share their experience in testing the construction

stones to the data protection supervisory authorities involved in the development

to share; e.g. B. by email to: sdm@datenschutz-mv.de.

Further building blocks are to be added in quick, albeit loose succession in 2019

to be published.

4.10.2

MUST lists in Europe to carry out a

Data Protection Impact Assessment

With the entry into force of the General Data Protection Regulation, the

data protection supervisory authorities are obliged to compile a list in accordance with Art. 35 Para. 4

to publish. In this so-called MUST list are processing

to name processes for which the responsible data protection supervisory authority

considers a data protection impact assessment to be mandatory.

A data protection impact assessment (DPIA) must be carried out if

the execution of a processing of personal data potentially

there is a high risk for the rights and freedoms of data subjects.

Already in the previous 46th activity report for the year 2017

in "2.6 Data Protection Impact Assessment (DSFA) according to DS-GVO: What can

are provided by them?" the relevant framework conditions

explained (source: https://datenschutz.hessen.de/sites/datenschutz.hessen.

de/files/2017_46_TB_0.pdf; last access: 26.11.2018).

German MUST list

The Conference of Independent Data Protection Authorities

The federal and state governments (DSK) established a nationwide coordinated list

according to Art. 35 Para. 4 DS-GVO in the sub-working group DSFA (UAG DSFA)

developed by the Technology Working Group (AK Technik). My co-worker has

regularly attended the meetings of the UAG DPIA. In doing so

causes the original list to be shortened by five entries. One

A clearly arranged MUST list is to be preferred, since it is for Hessian companies,

Firms and businesses must remain manageable.

The structure of this German MUST list is already based on the

Requirements of a guideline of the Art. 29 Group (today: European Data

data protection committee; EDSA) entitled "Guidelines on Data Protection

Impact Assessment" (WP248 rev.01; 13.10.2017; source: https://ec.europa.

eu/newsroom/article29/item-detail.cfm?item_id=611236). Herein are nine

Processing operations that may require a DPIA:

– Evaluate or classify (scoring)

– automated decision-making with legal effect or similar

significant effect

– systematic monitoring

– confidential or highly personal data

157

The Hessian Commissioner for Data Protection

47th activity report on data protection

– Large-scale data processing

– Match or merge records

– data on vulnerable data subjects

– innovative use or application of new technological or organizational

organizational solutions

– preventing a data subject from exercising a right or

the use of a service or the execution of a contract

These processing operations in connection with the

area of the respective IT and with regard to the (application) context in mind

a processing activity according to Art. 30 DS-GVO. Such

possible processing activities have been further specified and

Examples added. This MUST list is found with an explanatory

accompanying text at https://datenschutz.hessen.de/sites/datenschutz.

hessen.de/files/HBDI_Verfertigungsstufen-Muss-Liste.pdf (Status: August

2018 in version 1.1, last accessed on November 26, 2018). Apart from the

text I have decided not to make any changes compared to the

original, DSK-aligned version of the list, though

this would have been possible for me. In my view, this should be a MUST list

especially companies, firms and companies in the IT sector provide clarity

ten. This is particularly important if you are in Germany

work. Other data protection supervisory authorities of the countries have individual

duel adjustments made. The MUST list is not final.

If the controller or processor has a high risk of

Rights and freedoms of data subjects in risk assessment for

determines a processing activity (Art. 30 DS-GVO), then he has in each

case to carry out a DPIA. In addition, the responsible data protection

regulatory authority request a DPIA.

Submission of the MUST list to the European

Privacy Committee

This DSK-coordinated MUST list was created as part of an Art. 63

procedure, the consistency procedure, in accordance with Art. 35 Para. 6 for the submission of a

Statement according to Art. 64 GDPR sent to the EDSA. The until August

2018 MUST lists submitted for comment by 22 Member States

were by the expert group "Technical Subgroup" for the EDPB in

evaluated in a synopsis. The expert group found that

that only three entries of the submitted lists are the same across Europe

Assessment documents:

– Generic data are to be evaluated like biometric data; cf

Art. 9 GDPR.

– Health data must be subject to differentiated consideration

and are therefore in the application context and the technology used

consider.

– The highlighting of geolocation data must not result in

every small or medium-sized business is required to have an operational

having to appoint a data protection officer.

Each Member State was assigned a specific opinion by the EDPB.

Posted. This statement by the EDPB regarding the German MUST list

was published on September 25th, 2018 at https://edpb.europa.eu/sites/edpb/files/files/

file1/2018-09-25-opinion_2018_art._64_de_sas_dpia_list_en.pdf published

light. An adjustment in relation to the listed recommendations was made in

made by the UAG DPFA. Here is another vote in

the DSK off. I will continuously inform on my web presence,

if there are any changes here. controllers and processors

to be recommended, for processing operations carried out by consulting the competent

Gen data protection supervisory authority according to Art. 36 DS-GVO are approved

or should be approved, the current at the relevant time

MUST keep list.

application and outlook

With regard to the EU-wide coordination, it should be noted that a union

harmonization of national MUST lists for carrying out a DPIA

will take a while. In the meantime, five more submissions have been submitted

EU member states and signatories to the GDPR such as Norway

opinion by the EDPB. These submissions were still

not by the expert group "Technical Subgroup" according to one

procedure, comparable to that of September 2018. Because even

here the focus has shifted to the fact that IT developments are a Europe-wide application

is to be allowed.

It seems to me that I am particularly interested in how the requirements are changing

in the MUST list for carrying out a DPIA in practice.

Further influences from legal practice will have to be taken into account,

especially against the background of inherent demands on the

technical implementation

- in lists of processing activities in accordance with Art. 30 GDPR,

– for the security of the processing according to Art. 32 DS-GVO or

- when introducing certifications in accordance with Art. 42 and Art. 43 GDPR.

The acceptance and the effect of the MUST list will depend heavily on

genes, whether a Europe-wide harmonization of the development and use of

advances IT systems in complex and complicated IT landscapes,

so that GDPR-compliant processing is guaranteed.

4.10.3

Data protection impact assessment based on the methodology model

French supervisory authority

From May 25th, 2018, the person responsible according to Art. 35 Para. 1 DS-GVO

to carry out a data protection impact assessment in advance if the intended

Processing likely to pose a high risk to rights and freedoms

of natural persons. The data protection impact assessment

contains a systematic description of the planned processing

aisles and purposes, assessment of necessity and proportionality

of processing, risk assessment and measures to deal with the

risks. This requires structured documentation that is

should be available. As an example, the software platform of the

serve French supervisory authority.

The French data protection supervisory authority Commission Nationale

de l'Informatique et des Libertés (CNIL) is responsible for carrying out the data

Privacy Impact Assessment (DPIA)

short: PIA) according to Art. 35 DS-GVO a software platform developed and

made available for use (source: https://www.cnil.fr/en/open-source-pia-

software-helps-carry-out-data-protection-impact-assessment, last call:

10.12.2018). I have the software platform in the German language

Version and with a view to possible applicability in small and

medium-sized enterprises (SMEs) tested.

course of the procedure

The implementation of the DPIA with the CNIL software platform starts at

assuming that a completely new processing of personal data

is developed. It is based on a questionnaire based on the

text of the GDPR and is divided into four parts: (1) context,

(2) fundamental principles, (3) risks and (4) affirmation.

In the beginning, the context of the processing activity is to be described. In addition

does it belong

– the responsible

– additional legal norms, such as special legislation, and

– Any technical norms or standards used

to name.

Furthermore, the data to be processed and their associated data are required

Processes in use, specifying one or more specific IT applications

to identify connections. It is therefore advisable to use appropriate directories

of the processing activities in accordance with Art. 30 GDPR.

This must already contain the legal basis for processing personal

5 to Art. 7, if applicable Art. 8 or Art. 9

DS-GVO be recorded.

Furthermore, the list of processing activities contains the basics in

Procedure according to Art. 24 DS-GVO or Art. 28 DS-GVO as well as the

Implementation with technical and organizational measures for one

planned according to Art. 25 DS-GVO and permanent operation according to

Art. 32 DS-GVO to be documented.

Finally, the risk assessment for which a DPIA is to be carried out should

have already happened. If a high risk cannot be contained,

then the person responsible is obliged to notify the responsible data protection

supervisory authority before the start of the processing of personal data

to consult Art. 36 GDPR; s.a. Short Paper No. 5: Consequences of Data Protection

assessment according to Art. 35 GDPR, e.g. B. at https://datenschutz.hessen.

de/infothek/kurzpapiere-der-dsk, last accessed: 12.12.2018).

The second step is under the heading of basic principles

to examine for future processing activities whether the legal

lawfulness and the proportionality of the processing of personal data

data is preserved. The processing purpose is to be determined and

to check whether this purpose is in line with the GDPR. For this are

Requirements from Art. 5 DS-GVO to be considered. There are questions about this

answer, which z. B. on the consideration of data minimization,

the storage period or the correctness of the processing. The

Answers must be given in the context of any special legislation to be considered

genes and technical standards are given.

As a third step, the risks of the processing activity are considered,

which are directly related to the technical and organizational

rical measures. The relation to accompanying organizational

However, measures are only produced indirectly. stand in the center

this part of the DPIA IT security measures such as encryption,

Anonymization, data separation, entry, entry and access control,

Logging in terms of traceability and others more. Also the

Evaluation of the technical measures to be taken follows from the per-

perspective of IT security.

The fourth step in conducting a DPIA is a so-called

confirmation off. This includes a risk matrix that is stored in the software platform

form is referred to as risk mapping. This risk mapping resembles one

Risk matrix as derived from the technical standards of the ISO/IEC 31000 series

known for risk management. The creation of such a risk matrix

is i i.e. R. dependent on the company's internal risk model.

The risk model of the CNIL methodology of a DPIA

The CNIL software platform applies an IT security-driven risk

model with which the possible areas of application and the associated

Use cases are evaluated from an organizational or company perspective

the. Risks are the focus of consideration, one of which is a danger in

Depending on a possible probability of occurrence.

The probability of occurrence of these risks results from a

own organizational or company-specific risk model, the

i. i.e. R. a component of quality assurance processes for the production of a

product is. So here is the severity of a potential risk to the

Case rated that a faulty, consequently functionally restricted bis

non-functional product is used. In such a risk

model is used to calculate the possible severity of damage

possible consequential damage in the area of application with regard to the application of a

faulty, functionally restricted or even non-functional product

referenced. The difficulties resulting from this approach

result from different interpretations of what counts as a risk and what

could represent such a thing.

From a data protection point of view, the consideration of the risks is based on questions

of IT security narrowed. In fact, no risk assessment under

taking further data protection requirements into account.

Reference is made to individual known risks, the majority of which

are derived from the field of IT security. According to Art. 32 GDPR

should a more comprehensive consideration of possible risks depending on their

Severity and its probability of occurrence. The DS-GVO-

upcoming innovations for the field of information technology

not yet fully implemented in the CNIL software platform

integrated. From the point of view of IT, e.g. B. Confidentiality, internal

integrity, availability and resilience of the systems and services

(Article 32 (1) (a) GDPR). The consideration to preserve the

The rights of those affected only happen indirectly and can be found in parts in

the principles or in the assessment of the risks, although the use of these

software platform is advertised with it.

Used by small and medium-sized enterprises (SMEs)

The software platform of the CNIL can be used in different ways

or also in the own network of an organization or a company

to get integrated. For the application in practice it will be decisive

how an organization or a company with regard to the IT equipment

are asked.

For the installation of the software platform of the CNIL in small and medium

ler companies a separation of the tool - at least through

Virtualization – recommended. The storage of the performed DPIAs

requires a special configuration, e.g. B. runs over a port 8080.

Company or organizational security measures for

stored documentation of the respective DFSA must be carried out so

that they remain available in their own interest and treated confidentially

become. Furthermore, working with concurrent access is possible

People with different responsibilities are not recommended,

because no authorization concept is stored and therefore no role and

Rights concept is implemented.

Overall, this CNIL software platform is a first approach to

familiarize themselves with questions about the DPIA. Whether she is for permanent

Operation is suitable, practice will have to show. Here z. B. in

internal project has not yet been investigated which influences changes

changes over a longer period of time if a DPIA

has to be adjusted or how stable the provision of the DFSAs will prove to be.

Such an assessment of a permanent use of the software platform

the CNIL is not possible. Decisive for acceptance in SMEs

be how further development and maintenance of the software platform of the

CNIL, e.g. e.g. through security updates. Here will

also play into the extent to which compatibility is maintained, so that

already created DPIAs re-opened in the software platform and again

can be stored and thus the provision of adapted DPIAs

is made possible.

163

4.10.4

Basics and framework conditions for accreditations and

Certifications according to GDPR

With the entry into force of the General Data Protection Regulation, the data

protection supervisory authorities asked to promote certifications. As part of

data protection certifications are through accredited certification

deliver data protection criteria according to Art. 42 Para. 5 DS-GVO

test. In Germany only by the German accreditation body

(DAkkS) accredited certification bodies Certification according to Art. 42 and

Art. 43 GDPR i. V. m. § 39 BDSG. About data protection criteria

by an accredited certification body using specific

To have certification programs checked are interlocking test

implement procedures. This is a nationally coordinated

th accreditation and certification procedure, the DS-GVO-compliant

Processing of personal data guaranteed.

accreditations

With the application of Art. 43 DS-GVO is an accreditation procedure

in agreement between the competent independent data protection

Federal and state supervisory authorities and the DAkkS, which according to

§ 39 BDSG the entrusted body of the federal government for the implementation of accreditation

editing is to implement. In accordance with Art. 43 (1) (b) GDPR
the application of the technical standard EN ISO/IEC 17065, where in
this also already provides that further requirements of the independent
pending data protection supervisory authorities must be taken into account.
Such additional data protection requirements that apply to accreditation
of certification bodies by the DAkkS and the respective responsible
data protection supervisory authority can be found in “Requirements
for accreditation according to Art. 43 Para. 3 DS-GVO i. in conjunction with DIN EN ISO/
IEC 17065" published by the Conference of Independent Data Protection Supervisors
supervisory authorities of the federal and state governments on August 28, 2018
became. These extensions to DIN EN ISO/IEC 17065 are available at https://
www.datenschutzkonferenz-online.de/media/ah/20180828_ah_DIN17065-
Supplements-full-V10-final_V3_DSK.pdf available (last accessed December 20, 2018).
With regard to the actual application of these extensions, it should be noted
know that a binding opinion of the European Data Protection
Committee (EDSA) pending, even if the extensions are already in
a required procedure according to Art. 64 DS-GVO in German
were transmitted. According to this, there is the disputed requirement that documents
ments subject to an Art. 64 procedure in English only

can be submitted (on European cooperation see also 46th Ta-
activity report, Section 4.2).
Even if the previous version of the publication of the EDPB
for accreditation “Guidelines 4/2018 on the accreditation of certification
bodies under Article of the General Data Protection Regulation (2016/679)"

when preparing the "requirements for accreditation according to Art. 43
Para. 3 DS-GVO i. V. m.: DIN EN ISO/IEC 17065” was taken into account
more likely to assume that over the comparison of the configurations
of these data protection requirements from other EU member states
ten adjustments will also be made in the German version. The
publication of this guideline, which has already been revised
at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/
guidelines-42018-accreditation-certification-bodies-under_en (last call:
12/20/2018). An appendix specifies the EU-wide coordinated in the EDPB
requirements for certification bodies to be accredited; he was on
December 14, 2018 at https://edpb.europa.eu/our-work-tools/our-documents/
guidelines/edpb-guidelines-42018-accreditation-certification-bodies_en dated
EDSA published (last accessed: 20.12.2018).
According to the hierarchy of technical standards, the standard is EN ISO/IEC 17065
a follow-up standard to the EN ISO/IEC 17065 standard
Application of the technical standard EN ISO/IEC 17067 to design content,
which the accredited certification bodies as part of a certification
process have to check. If it is essential here that the data protection
supervisory authorities present their data protection content.
certifications
In the accreditation procedure of certification bodies according to Art. 43 DS-
A test procedure is stored in the GVO, which is an organizational test of the
accrediting certification procedure. In addition to the exam in
As part of the accreditation, test procedures for certification are to be
design and implement, based on defined data protection regulations
Criteria a test system and methodology for a specific certification

enable the object of the insurance.

The first EU-wide specifications for the objects of certification can be found in a guideline from the EDPB entitled “Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679”, which was already published on May 30, 2018 and at https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_de can be found (last call:

12/20/2018). A revised version of this document is for starters announced in 2019. This guideline on certification criteria will appendix, the certification criteria according to Art. 42 Para. 5 again concretized.

Participation of the HBDI

Since 2016 an employee in the field of information technology constantly in the nationwide working group "Certificate tion" under the leadership of the Independent State Data Protection Center active in Schleswig-Holstein. This demanding and complex job requires additional human resources. So are now also legal reports included.

Three of my employees from the areas of information mation technology and the law are based on appropriate Training courses and training for the implementation of accreditations qualified in agreement with the DAkkS.

In Hesse, at least three accreditations will be granted in 2019

Certification authorities expected to which I am in agreement with the

DAkkS will participate. Further, I will have an increased focus on the

lay down the necessary test criteria as well as the test system and methodology,

so that in a certification period, continued compliance with the

DS-GVO in respective certification programs according to Art. 42 Para. 1

GDPR can be guaranteed. Such certification programs are

by future accredited certification bodies because they

Basis for data protection checks within the framework of to be issued

certifications are.

Conclusion

From an information technology point of view, the involvement of the HBDI is crucial,

because certifications as proof of GDPR-compliant processing

in Art. 30, 32, 35 i. In conjunction with Art. 36, reference should be made to recital 90. One

Certification always means anticipating a data protection law

Examination that may take place when a certification is granted. At the entrance

e.g. B. a complaint that has a data protection or information

technical examination of the security of the processing in accordance with Art. 32 DS-GVO

certifications can be issued by those responsible as proof

processing in accordance with data protection regulations. Data protection-

legal requirements and test criteria with test system and methodology

accredited certification bodies must in future be compared with those

desires, which have already been implemented by me today. This is an essential

A prerequisite for certifications that are finally granted, if necessary within the framework of

To be able to recognize sanctions according to Art. 83 DS-GVO.

4.11

fine proceedings, reports of data breaches

4.11.1

Europeanization of the fine procedure and collision points with

the national law

The legislator has given it to the Member States in accordance with Art. 83 (8).

DS-GVO is responsible for the procedure for punishing violations

against the GDPR with appropriate procedural guarantees.

Due to this obligatory opening clause, § 41 BDSG

a bridge to the existing national procedural law in the OWiG, Ge-

law on criminal proceedings (StGB) of the Code of Criminal Procedure (StPO) and

the Courts Constitution Act (GVG) was built. Practice shows that this

subject to the pending case law of the highest court, the

Federal legislature has not succeeded without collision under European law and it

may require improvement after a practical phase.

Since May 25th, 2018, Art. 83 Para. 4, 5, 6 DS-GVO has been in force

Catalog of fines applicable throughout Europe. The material eu

European data protection law should be effective with national procedural guarantees,

be enforced in a proportionate and dissuasive manner. When implementing

§ 41 BDSG takes over the switching point in national law, because there the

Applicability of national procedural law and the extent of

applicability in the sanctioning of violations of the GDPR is regulated.

The first practical experiences have shown that three points always

raise questions again:

– the so-called “functional company concept” and the applicability of the

§§ 9, 30 and 130 OWiG

– the question of a framework for fines or a cap

- the punishability of Art. 33 DS-GVO reports in fine proceedings

§§ 9, 30 and 130 OWiG

In the first draft of the Federal Data Protection Act, Sections 9, 30 and

130 OWiG in the application still excluded. The one that came into force

Version of § 41 Para. 2 S. 1 BDSG leaves it with the applicability of this

norms. This raises questions in the practice of fines.

§ 41 paragraph 2 sentence 1 and 2 BDSG

For proceedings due to a violation under Article 83 paragraphs 4 to 6 of the Regulation (EU)

2016/679 apply, unless this law provides otherwise, the provisions of the

law on administrative offenses and general laws on criminal procedure,

namely the Code of Criminal Procedure and the Law on the Constitution of Courts, accordingly.

Sections 56 to 58, 87, 88, 99 and 100 of the Administrative Offenses Act do not apply

Application.

In the GDPR, the EU level starts from the functional company concept

(see ErwG 150 sentence 3), refers to the term "economic entity"

and deems it a fine of a company or a

Group to be sufficient if it is certain that an employee or a

Employee of the company against a hitting the company

breached duty.

Recital 150 sentence 3

Where fines are imposed on companies, the term "company" should be used for this purpose.

men” within the meaning of Articles 101 and 102 TFEU.

By assuming that an entity is any entity that is independent

on the legal form and the way it is financed economic activity

exercises (so-called functional company concept), it is fundamentally possible

lich, an entire group for the data protection violation of a subsidiary

responsible. It comes to the legislators of the

DS-GVO does not refer to the property as a legal entity, but only to the

exercise of factual economic functions. The reference point "funk-

national company concept" serves as a simplification mechanism on the

legal consequences page. The data protection fine under European law is primarily due to

the company/association fine. the natural person

who worked for the company recedes into the background.

In the German procedural law of administrative offenses is the proven

§ 30 OWiG a participation and sanctions standard, the imposition of

fines against associations. She is a pure legal

follow-up regulation. Section 30 OWiG is based on the legal entity principle. The

legal entity principle focuses on specific legal entities and not

like the European data protection law, on the economic entity.

Legal persons are therefore all social organizations to which the

legal system recognizes its own legal personality (Göhler/Gürtler

OWiG § 30 RdNr. 2), such as B. AG, GmbH, the cooperative or the

registered association. As an association of persons is the legal person

the legal partnership (e.g. OHG, GmbH & Co. KG, KG,

GbR) equal.

In essence, companies cannot act themselves. Therefore will

the behavior of natural persons is legally attributed to them. Over

the attribution norms close this gap. § 30 OWiG

to the act of a manager representing the entity. Who

In § 30 paragraph 1 no. 1 to 5 OWiG

Are defined.

The list in Section 30 (1) OWiG was last expanded in 2002 to include number 5,

because the national legislation has been adapted to European requirements

should be (Bundestag publication 14/8998, p. 6, 7, 10).

Section 30 (1) No. 5 OWiG

does anyone

1. …

...

5. as another person who is responsible for the management of the operation or company of a

ristic person or an association of persons named in numbers 2 and 3

acts responsibly, including monitoring the management or the

other exercise of control powers in a managerial position,

committed a criminal offense or misdemeanor by the duties imposed by the legal

meet the person or association of persons, have been injured or the legal

person or the group of persons has been enriched or should become so

be fined against them.

A kind of general clause was introduced by Section 30 (1) No. 5 OWiG

and the group of leaders expanded considerably. is decisive

after that less the formal legal position, e.g. B. Managing Director, than that

material criterion of the person responsible for the management of the company

Acting, i.e. persons who belong to the group responsible for the management of the company

or persons responsible for the company (BT-

Drucks. 14/8998, p. 7). Although this broad approach of national law will
still not in line with EU data protection law. It turns in this
context, the question of how to handle those cases in which a
management function is not detectable. Because of the possible
Difficulties with instructions can result in effective sanctions for violations

be hindered against the GDPR. It does exist according to Section 30 (4).
S. 1 OWiG the possibility of an "isolated" association fine. But also
for the imposition of an "anonymous" fine, it should be noted that
if any leader committed the act. It takes one
Acting as a manager i. s.d. § 30 para. 1 no. 1 to 5 OWiG. Dem can
under certain circumstances by means of an interpretation of
oppose § 30 para. 1 No. 5 OWiG on a transitional basis. It would be anyway
desirable that the federal legislature examines whether and how
BDSG, comparable to the regulations in § 81 GWB, special procedural
regulations on administrative offenses law. Unless this
is not an option, the question arises as to whether Section 30 (1) No. 5 should not
OWiG in the light of the European requirements and in the course of a
dernization taking into account the national constitutional
requirements must be adapted to current requirements.
Section 9 OWiG is closely linked to Section 30 OWiG. The different understanding
between European and national level also applies to § 9 OWiG.
As far as one takes the European understanding as a basis, the question arises
whether § 130 OWiG, which is a fact that uniformly and conclusively

Violation of the duty of supervision regulates, at least for the area of application

of the facts of the DS-GVO is obsolete. In my opinion, he can

connection with violations of the GDPR do not apply.

It is likely that these open questions will be clarified in court

be supplied.

Fine framework or cap limit

The federal legislator has the applicability with § 41 Abs. 1 S. 1 BDSG

of § 17 OWiG excluded.

§ 41 paragraph 1 sentence 1 BDSG

For violations according to Article 83 paragraphs 4 to 6 of Regulation (EU) 2016/679 apply, insofar as

this law does not provide otherwise, the provisions of the law on regulatory

adversities accordingly. Sections 17, 35 and 36 of the Administrative Offenses Act

do not apply.

This allows the regulator to impose fines from EUR 0 upwards

and instead of the framework of fines on which the OWiG was based

based on the capping limit discussed in the EU. To date there was one

Fine framework provided with a minimum fine of 5 EUR. Current

is in the committees of the EDPB, the task force calculate administrative fines,

discussed in connection with the interpretation of the basic regulation whether

the DS-GVO is based on the capping limit or a framework for fines.

As a rule, Europe knows the capping limit, the national regulatory

Adversity proceedings know the fine framework. During the sizing

of a fine moves within a framework nationally

capping limit, a fine is initially detached from the capping limit

calculated and then capped. This type of fine

However, in the case of companies with very high sales, this has the consequence that

two companies for one and the same act as a result of capping an and

would have to pay the same fine for offenses of different severity.

As a result, if the case should occur at all, it seems strange

sam, since there is then the same fine for offenses of different severity

would exist. However, the application of the capping limit requires that the

fines are based on guidelines.

Art. 33 GDPR and the fine procedure

The feedback from companies shows that the federal legislature

with the regulation in § 43 Abs. 4 BDSG succeeded an unfortunate one

to create an appearance that leads to a false assumption among those affected.

The companies and individuals walk away as a result of the regulation

out that a violation or a data breach (data breach) that they have about the

"Art. 33er portal" to the supervisor, cannot be punished.

§ 43 paragraph 4 BDSG

A notification under Article 33 of Regulation (EU) 2016/679 or a notification

according to Article 34 paragraph 1 of Regulation (EU) 2016/679 may in a procedure according to

Law on administrative offenses against the reporter or notifier

or his relatives specified in Section 52 (1) of the Code of Criminal Procedure

consent of the reporter or notifier.

The companies must report a data breach in good time according to Art. 33 DS-GVO

report, otherwise there is a risk of a fine according to Art. 83 Para. 4 DS-GVO. In the

In the event of a data breach being reported, the reporting party will

Regulation in § 43 paragraph 4 BDSG assumes that the facts

is blocked for punishment in fine proceedings, unless that approves

the usage. The first practice in the year under review has shown that above all

the economy assumes that reporting data breaches is a

administrative fine proceedings - in two respects.

It is correct that a failure to report a data breach in a timely manner

to a fine ^Sm. i.e. Art. 83 Para. 4 DS-GVO leads.

171

The Hessian Commissioner for Data Protection

47th activity report on data protection

However, it is also correct that a notification according to Art. 33 GDPR or a

Notification according to Art. 34 DS-GVO against the reporting person or

Notifying or his in § 52 paragraph 1 of the Code of Criminal Procedure

only with the consent of the reporting or notifying party

can be used.

In addition, I assume that if a company has a data

panne reports, this does not mean that the data protection policy contained therein

shock per se cannot be punished. The contents of the Art. 33 notification,

I do as part of the supervisory procedure or a fine procedure

could have determined myself, I can punish in the fine proceedings, provided that

they could have been recognized by my own examination. The one in the

The principles developed in case law on Section 97 of the Insolvency Code

to use here.

4.11.2

The first fine proceedings under the GDPR regime

Irrespective of the collisions resulting from the structure of the German regulatory

adversarial law and the sanction system of the reformed European

Data protection law arise, prepares the application of the new facts

From the point of view of fines, only a few problems so far.

As in the previous

ing reporting periods by the data subjects directly as well as

brought to the attention of the police or the public prosecutor's office. Included

the number of fine cases to be processed increased significantly in 2018

taken. As early as August 2018, the average was the same as in previous years

administrative offense proceedings initiated.

For actions that have been completed before May 25th, 2018,

reason for the in § 4 paragraph 3 of the law on administrative offenses (OWiG)

established principle of most-favoured-nation generally continues to

money regulations of § 43 Federal Data Protection Act (BDSG old version) in the

Version of the notice of March 14, 2003 (BGBl. I. S. 60) and the

in § 43 Para. 3 BDSG a. F. Standardized fines of up to EUR 50,000 or

300,000 euros. At times, fines are therefore still issued according to age

legal position to be enacted.

With regard to the cases to be prosecuted, after the change in the legal

location so far only minor differences, because the majority

of the violations of data protection law that became known here

already threatened with a fine under the old law. The majority of speech

The facts mentioned above occurred during the processing of personal

gener data in the context of direct advertising. This means that most of the

Violations of the fine provision of Art. 83 (5) that are currently being pursued

of the General Data Protection Regulation (GDPR), compared to the regulation

of Art. 83 Para. 4 DS-GVO the imposition of significantly higher fines

provides. In this context, it should also be noted that Art. 83

Para. 2 DS-GVO regarding the fine stipulates that these are for violations

effective against Art. 83 Para. 4 to Art. 83 Para. 6 DS-GVO in each individual case,

should be proportionate and, in addition, dissuasive. Before this

Background are sensitive fines for effective enforcement

Regulation depending on the circumstances of the case also already at supposed

"lighter" violations possible.

Unsolicited promotional emails

In one procedure, the person concerned informed me that they were participating in a

I took part in a competition organized by a company based in Hesse.

Although the data subject thereby ordered the e-mail newsletter

ruled out, she subsequently had one from the company

Received an email with promotional content.

In principle, the sending of an advertising e-mail constitutes an unlawful

processing of personal data if, after the exercise of the

Right of objection according to Art. 21 DS-GVO takes place or not through a

permit is covered. Violations committed in this context

can be fined up to

EUR 20,000,000 or in the case of a company up to 4% of the worldwide

annual turnover.

In this specific case, it is the company that arranges for the e-mail to be sent

had, part of a corporation. The worldwide annual turnover of the parent company

company is in the higher three-digit million range, so this is the case

the scope of the percentage upper limit opened up for the first time

could be. The procedure is not yet complete.

Publication of the contact details of the

Data Protection Officer

So far, only a few administrative offense proceedings have been initiated due to violations

against the new rules of conduct and bans of the GDPR.

One of the first offenses to be punished against a by the

DS-GVO newly created obligation concerned a violation of Art. 83 Para. 4

lit. a GDPR i. In conjunction with Art. 37 (7) GDPR.

173

The Hessian Commissioner for Data Protection

47th activity report on data protection

In the summer of 2018, it was brought to my attention that a company

on its website instead of the contact details of the data protection officer

only a general contact address of the company is listed

had. A publication of the contact details of the data protection officer

was not done in any other way.

According to Art. 37 Para. 7 DS-GVO, the person responsible or processor

workers are now obliged to provide the contact details of the data protection

commissioned to publish. However, the GDPR does not define what

is to be understood specifically by the term "publication". through the

newly introduced obligation to publish the contact details of the

Data protection officers should protect the rights of the data subjects

be secured. In particular, the persons concerned should

Be able to publish at any time, from their right

to make use of Art. 38 GDPR. To do this, they should focus on simple

and directly in a confidential manner to the data protection officer

can turn. Logically, the purpose of the regulation is not given by a

one-time or short-term publication of the contact details is sufficient,

so that this can only be done by permanently finding the contact data
can be achieved. A measure of publication that meets the requirements
37 Para. 7 DS-GVO corresponds to, for example, the
Specification of the contact details of the data protection officer at a
easy to find place on the website (data protection declaration, cf. Art. 13
Paragraph 1 lit. b DS-GVO). The permanent visibility of the contact data
enables the data subjects to contact the or the at any time
record data protection officer.
Violations of Article 83(4)(a) GDPR i. In conjunction with Art. 37 (7) GDPR
may be fined up to EUR 10,000,000 or in the case of a
up to 2% of annual worldwide sales, depending on the amount
is higher, be punished. Especially against the background of significant
Those responsible or processors should always avoid the threat of fines
ensure that data subjects have the opportunity available
stands, directly to the data protection officer
to approach. A personal e-mail address or radio
tion e-mail address (e.g. "datenschutz@..."), a telephone number for
direct contact and/or a specific postal address
provided by the data protection officer in a suitable manner
become. The indication of the name of the data protection officer is
However, it is not required, although it is recommended to mention it (cf.
Article 29 WP, WP 243 rev.01, 2.6).

4.11.3
Notification of Personal Data Breach

according to Art. 33 GDPR

Violations of the protection of personal data are according to Art. 33

GDPR to report to the supervisory authority, unless there is a risk for

the rights and freedoms of those affected can be excluded.

Personal data breach (data breach) solves

if the requirements defined by the legislator in Art. 33 DS-GVO are met

Prerequisites an obligation to report the incident to the supervisory

stop listening However, this is not a new rule.

Also in the BDSG a. F. was there with the

§ 42a BDSG a. F. such a norm, the content of which is clearly different

from the regulations of Art. 33 DS-GVO.

§ 42a BDSG a. f

Information obligation in the event of unlawful knowledge of data

Represents a non-public body within the meaning of Section 2 (4) or a public body

according to § 27 paragraph 1 sentence 1 number 2 states that stored with her

1. special types of personal data (§ 3 Paragraph 9),

2. personal data subject to professional secrecy,

3. personal data relating to criminal acts or misdemeanors

or the suspicion of criminal acts or administrative offences, or

4. Personal data relating to bank or credit card accounts

unlawfully transmitted or otherwise unlawfully made known to third parties

and there is a threat of serious damage to the rights or those worthy of protection

interests of those affected, it has to inform the competent

notified supervisory authority and the data subject. The notification of

Affected must be done immediately, as soon as appropriate security measures

of the data has been seized or not taken immediately and criminal prosecution

is no longer endangered. The notification of those affected must include a statement
the nature of the unlawful acquisition of knowledge and recommendations for measures to
mitigation of possible adverse consequences. The notification of the responsible
The supervisory authority must also present possible adverse consequences of the un-
lawful knowledge and the measures taken by the body thereupon
contain. Insofar as the notification of those affected involves a disproportionate effort
would require, particularly given the large number of cases involved, occurs at their
Advertise public information through advertisements that are at least half a page
include, in at least two nationwide daily newspapers or through one
others that are equally suitable in terms of their effectiveness in terms of informing those affected
Measure. A notification issued by the person subject to the notification obligation may
criminal proceedings or proceedings under the Administrative Offenses Act
against him or a relative referred to in Section 52 (1) of the Code of Criminal Procedure

of the notifier only with the consent of the notifier
be used.

Art. 33 GDPR

(1) In the event of a breach of the protection of personal data, the responsible
verbatim immediately and if possible within 72 hours after the breach
became known to the competent supervisory authority pursuant to Article 55, unless
that the personal data breach is not likely to result in a
risk to the rights and freedoms of individuals. If the notification is sent to the
If the supervisory authority does not respond within 72 hours, it shall be given a reason for the delay
to add.

(2) If the processor has a personal data breach

becomes known, he reports this to the person responsible immediately.

(3) The notification pursuant to paragraph 1 shall contain at least the following information:

a) a description of the nature of the personal data breach,

as far as possible, specifying the categories and the approximate number of those affected

persons, the affected categories and the approximate number of affected personal

son-related datasets;

b) the name and contact details of the data protection officer or another

point of contact for further information;

c) a description of the likely consequences of the violation of the protection of personal

personal data;

d) a description of those taken or proposed by the controller

Measures taken to address the personal data breach

and, where appropriate, measures to mitigate their possible adverse effects

effects.

(4) If and to the extent that the information cannot be provided at the same time,

the Controller may receive this information without further undue delay

make available gradually.

(5) The person responsible documents violations of the protection of personal data

including all related to personal data breaches

Data standing facts, their effects and the remedial measures taken.

This documentation enables the supervisory authority to verify compliance with the

provisions of this article.

Determination of the obligation to report

When comparing both standards, some key differences become apparent

recognizable.

While according to § 42a BDSG a. F. an obligation to report only after a data breach was triggered with certain types of data, the legislator waives to such a restriction. These data also had to be sent to the "old" Standard unlawfully transmitted or unlawfully made known to a third party not have reached. This restriction is not found in Art. 33 GDPR.

176

Data protection report from 05/25/2018

This means that since May 25, 2018, any violation of protection of personal data lead to a reporting obligation under Art. 33 GDPR can. This could, for example, include the unintentional destruction of important and difficult-to-recover personal data be what according to the regulations of § 42a BDSG a. F., however, no message would have triggered.

However, not every data breach automatically triggers the obligation to message off. Both the legislator and the legislator have included in the respective standards with regard to a risk assessment. While according to § 42a BDSG a. F. the threat of serious impairment impairment of the rights or legitimate interests of those affected triggered the obligation to report, the legislator has significantly lowered the hurdle puts. Now only then is there a report to the supervisory authority refrain if the injury is unlikely to pose a risk to the Rights and freedoms of the natural person. In each individual case, therefore to make a forecast decision, which is also documented accordingly should be, so that if there is no notification and at the same time Complaint by the person concerned can be checked by me.

In addition, the scope of the GDPR includes in contrast

on the previous legal situation according to § 42a BDSG a. F. both non-public and

also public authorities.

The requirements of Art. 33 DS-GVO are therefore clear from a

higher number of cases met, leading to a sharp increase in reporting

ments in my authority. That was the case throughout 2017

a total of 85 reports according to § 42a BDSG a. F., while for 2018

a total of 681 reports were recorded. These numbers settle

from 51 reports according to § 42a BDSG a. F. and 630 reports under Article 33

GDPR together. Considering only the period from 05/25/2018,

an annual number of cases of about 1,000 can be assumed, what

represents an increase of 1,176% compared to the previous year.

Legal consequences if there is a reporting obligation

If it has been determined that the requirements for reporting are met

are, the person responsible now has this to the supervisory authority

report. While the period according to § 42a BDSG a. F. still relatively undetermined

("immediately"), the legislator has a 72-hour period

introduced (Article 33 (1) sentence 2 GDPR).

It has not been regulated how the message is to be transmitted

average is. Various options are conceivable, such as by post, by

fax, by e-mail (ideally encrypted) or by notification via the

Registration portal of my homepage, on which I have a form with all for the

Provide the data fields required for reporting.

While a reportable incident according to § 42a BDSG a. F. in any case

in addition to reporting to the supervisory authority, an obligation to notify

correction of the data subject triggered, the legislature has now

differentiated. There is only a notification obligation if the

Data breach likely to pose a high risk to the rights and

freedoms of the natural person (Art. 34 DS-GVO). Here too

each individual case must be examined.

Art. 34 GDPR

(1) If the breach of the protection of personal data is likely to have a high

risk to the personal rights and freedoms of natural persons, so be-

the person responsible shall inform the data subject of the violation without undue delay.

(2) The notification to the data subject referred to in paragraph 1 describes in clearer

and plain language the nature of the personal data breach and

contains at least the information referred to in Article 33(3)(b), (c) and (d).

and recommendations.

(3) Notification of the data subject pursuant to paragraph 1 is not required,

if one of the following conditions is met:

a) the person responsible has taken appropriate technical and organizational security measures

ments and these precautions on those affected by the violation

personal data have been used, in particular those through which the

personal data for all persons who do not have access to the personal

related data are authorized to be made inaccessible, for example through encryption

selung,

b) the person responsible has ensured through the following measures that the high

Risk to the rights and freedoms of data subjects under paragraph 1 of all

probability no longer exists

c) this would involve a disproportionate effort. In this case,

to make a public announcement or similar action,

through which the data subjects are informed in a comparably effective manner.

(4) If the person responsible has not already informed the data subject of the violation of the

protection of personal data, the supervisory authority can be found at

taking into account the probability with which the breach of protection

related data leads to a high risk, require the controller to do so

make up for it, or it can determine with a resolution that certain of the

the above conditions are met.

§ 43 Para.4 BDSG limits the consequences of a report according to Art. 33

DS-GVO for a fine procedure.

178

Data protection report from 05/25/2018

§ 43 paragraph 4 BDSG

A notification under Article 33 of Regulation (EU) 2016/679 or a notification

according to Article 34 paragraph 1 of Regulation (EU) 2016/679 may in a procedure according to

Law on administrative offenses against the reporter or notifier

or his relatives specified in Section 52 (1) of the Code of Criminal Procedure

consent of the reporter or notifier.

Failure to report may result in a fine. Also

violations of any orders by the supervisory authorities

de, which have been issued as a result of Art. 33 DS-GVO, or at the

Review of incident identified (new, additional or ongoing)

Data protection violations are punished accordingly (see

also Section 4.11.1).

In conclusion, it can be stated that the regulations of the GDPR

to an intensive discussion of the responsible body with the

breach of data protection and significantly more often to a report of the data protection

infringement leads to the supervisory authority.

Submission of a notification according to Art. 33 DS-GVO

In the case of a report pursuant to Art. 33 Para. 1 DS-GVO, the minimum requirements are

ments from Art. 33 Para. 3 on the content and scope of the to be provided

to fulfill information. To support those responsible in this, stand up

my website at https://datenschutz.hessen.de/service/messen-von-

personal-data-breach digital form

available for download. The structure and content of this form are

coordinated across Europe. I recommend those responsible to use the

form and filling it out carefully to ensure that

they fulfill their obligations according to Art. 33 Para. 3 DS-GVO.

To send a completed form to me, and thus to

submitting a report according to Art. 33 Para. 1 DS-GVO, are responsible

different modes of transmission. In addition to the postal

Sending the printed form I have two digital transmissions

averaging alternatives opened up. Responsible persons should be able to

are transferred, comply with their obligation to comply with the 72-hour period

to comply with Art. 33 Para. 1 DS-GVO without restriction. A message is

therefore possible at any time, regardless of the opening hours of my authority.

As a first, digital alternative, there is the possibility of transmitting a

Message as an e-mail attachment. It should be noted that reports after

Art. 33 Para. 1 DS-GVO often contain sensitive information. To their

To meet protection requirements, corresponding e-mails should only be sent

be sent end-to-end encrypted. More information about

encrypted e-mails can be sent on my website at https://

datenschutz.hessen.de/service/verschl%C3%BCsselte- kommunikation-mit-

dem-HBDI can be looked up.

As part of the preparation for the entry into force of the GDPR on

05/25/2018 I have another digital possibility to submit a message

33 Para. 1 DS-GVO. This is above my website

at https://datenschutz.hessen.de/service/melden-von- leeches-

of the protection of personal data and is characterized by

easy usability. In particular, except for one are available for use

e-mail account does not have to meet any further requirements. As a reason-

location of submitting the completed form can be found on the above

page, a so-called upload link can be requested. Here acts

it is a hyperlink specific to the notification, pointing to a dated

The email address given to the person responsible will be sent. When opening

of the upload link in a browser opens a page in HessenDrive, a

secure exchange platform for digital documents. Here will

the possibility to upload the completed form and any

additional documents are required. As part of the upload,

the use of appropriate encryption ensures that only the

employees responsible in my authority the transmitted documents

can retrieve. By using HessenDrive, the protection requirement

sensitive information into account.

In summary, those responsible are responsible for submitting reports

according to Art. 33 Para. 1 DS-GVO several transmission alternatives for

decree. By providing these alternatives, those responsible

when submitting reports, and in particular when complying with the

72-hour period, to be given the best possible support.

4.11.4

Field report and statistics on the reports pursuant to Art. 33

GDPR in the health sector

Before the GDPR came into effect, Hesse only had to report

intended for the private sector. With the Art. 33 DS-GVO is after the

25.05.2018 now also an obligation to report data protection incidents for

intended for the public area. The first effects of this new

Regulations on the health sector are presented below

become.

Data protection report from 05/25/2018

Status in the first three months after the entry into force

GDPR

In the first three months after May 25, 2018, a total of 42 reports

33 DS-GVO regarding the health sector

HBDI received. In the future, this will be extrapolated to the year from to

160 reports per year. For comparison, here it is pointed out-

pointed out that for the entire year 2017 only 85 reports according to

§ 42a BDSG for all areas in the house.

The 42 reports from the health sector focus on

moderately as follows:

– 14 cases of incorrect mailing

– 9 cases of burglary and theft

– 5 cases of hacking attacks

– 4 cases due to loss of USB sticks and data carriers

– 3 cases of unauthorized access to databases

– 1 cases of improper setup of access rights

– 6 cases due to other events

Evaluation of the statistics

The incorrect postal dispatch is currently the most common reporting case

Art. 33 DS-GVO. This is particularly low in the area of health

surprising given the exchange of information between the many involved

Bodies and persons responsible on the basis of a legal basis or

the consent of those affected is practiced in large numbers on a daily basis.

I am assuming that there will be fewer reports in the future

NEN is because experience will form when the wrong shipment

character of a reportable event. Also, I think that

there will be a “best practice

Paper” will be given.

When it comes to reports of burglaries and thefts, I see it more

a growing number of cases. The same applies to the area of hacker

attacks for which companies and public bodies in the health

area should be strengthened (see also the small question from

the Hessian state parliament of April 12, 2018 regarding IT security in

kenhäuser and the feedback received, LTDrucks. 19/6275).

The loss of USB sticks and data carriers can be counteracted in the future

that the data stored on it corresponds to the current standard

be encrypted in a spoken way. Because of their size tend in particular

USB sticks tend to get lost quickly.

An important topic for me is unauthorized access to data

banks. In one case, the clinic concerned did not notice that

Multiple former employee access accounts improperly

have been blocked. This is reminiscent of a well-known case

Portugal, consequently in a hospital 985 active users in the hospital

kenhaus information system were registered with the profile "Doctor", although

only 296 doctors worked in the hospital (see https://www.publico.

pt/2018/10/22sociedade/noticia/hospital-barreiro-contesta-judicialmente-

coima-400-mil-euros-comissao-dados-1848479).

Outlook and hints for the future

For the future it seems important to me to remember that

also the loss and destruction of patient files in accordance with Art. 5 Para. 1

lit. f GDPR is notifiable. There have been more than that in the past

two medical practices in Hesse, where water damage to the destruction and

illegibility of part of the patient files (see also

the contribution under item 4.6.3 in this activity report).

For the further processing of the processes, it is also helpful if the

Free text fields in the reporting form for detailed descriptions of the processes

be used. Here, vague terms such as "unprotected PC"

to avoid. In addition, the incorrect shipment should be described as precisely as possible

and be described.

A general outline for reporting data breaches,

which also affects the non-public area, I have under Section 4.11.3

shown.

4.12

Labor statistics from 05/25/2018

With the validity of the GDPR, the requirements for presentation have also changed

the work statistics changed.

Art. 59 GDPR now stipulates that the annual report of a

supervisory authority a list of the types of violations reported and the types

of the measures taken according to Art. 58 Para. 2 DS-GVO.

The report is not only the Hessian state parliament, the government and the

to the public, but also to the EU Commission and the Euro

European Data Protection Committee accessible. The Independent

Federal and state data protection supervisory authorities (DSK).

182

Data protection report from 05/25/2018

decided to report with a separate and for all

"Facts and Figures" chapters in the supervisory authorities' uniform format

comply with activity reports. This is intended to provide transparency and

accessibility within the DSK and for the public. There

with these values not all activities of the individual supervisory authorities

are covered, additional explanations can be found in a further chapter

ments and representations are made.

4.12.1

facts and figures

facts and figures

a) Complaints

Number of complaints received under GDPR in the reporting period

are. Upon receipt, such processes are counted as complaints

received in writing and where a natural person has a personal

affected, to which Art. 78 DS-GVO is applicable. This closes

duties a. Telephone complaints are only counted if they

be put into writing (e.g. by a note).

b) consultations

Number of written consultations. This includes summary advice from

Controllers, data subjects and their own government.

Not: (telephone) oral consultations, training courses, lectures, etc.

c) Data Breach Notifications

Number of written reports

d) Remedial Actions

Number of actions taken

according to Art. 58 Para. 2a (warnings)

(1)

(2)

according to Art. 58 Para. 2b (warnings)

according to Art. 58 Para. 2c to g and j (instructions and orders)

(3)

according to Art. 58 Para. 2i (fines)

(4)

(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.)

f) Formal support for legislative projects

Here, as a lump sum, the total number indicated by parliament/government

called for and carried out consultations. This also includes the partial

Participation in public committees and submissions to courts.

case numbers

05/25/2018

until 31.12.2018

2,278

2.185

630

(1) 0

(2) 2

(3) 2

(4) 0

(5) 0

(1) 120*

(2) 3*

(3) 83*

*Minor

deviations

possible

14

183

The Hessian Commissioner for Data Protection

In addition, two administrative offenses were committed in the second half of 2018
Proceedings for violations of the GDPR have been completed. After
the first investigative actions it became clear that the factual
scope of application of the regulation was not open. The procedures had to
therefore be discontinued.

4.12.2

Supplementary explanations of facts and figures

The values in the table give an overview of my activities
Employees in the area of complaints and advice
genes, but there are specifics, the daily demands and challenges
and a topic-specific evaluation is not expressed therein.

With the validity of the GDPR and the following diverse - not in the matter
always accurate – reporting in the media changed the way
working situation of my authority from 25.05.2018 suddenly. From a day
the next was a rush of inquiries by telephone, e-mail and post
one that could be managed with the same human resources as before.
In particular, the telephone inquiries about the GDPR brought the
capacities of my employees and even those of the
phone system to the limits of resilience. The telephone consultations
found no record in files, but took considerable time and
resources required.

A sample count for the month of June 2018 revealed 1,703 telephone calls
Consultations that lasted longer than 10 minutes (for comparison: back in April
In 2018 there were 484 telephone consultations). Hundreds of untold
The colleagues in my office also received calls to

to either ask for brief information there or to complain about it,

that the person responsible cannot be reached by telephone

or the telephone connection is constantly busy.

The written processing of the entries and inquiries was therefore only very

sluggish, which in turn leads to complaints about long waiting times

led. With an internal reorganization, more student assistants

and the reorganization of the telephone times, the functionality of my

authority to be adequately organized again.

The months of May to August were the busiest months of the year

2018. From September 2018 the situation calmed down a bit. Until the end of the year

verbal information and advice has increased to approx. 506 telephone calls

leveled off in the month. To the same extent that the telephone advice

the number of written inquiries submitted increased

Complaints and submissions by those affected as well as reports from

breaches of data protection by those responsible (for the latter see also Section 4.11.3).

It has become clear that citizens have their rights

Demand or request information, correction and deletion more intensively,

that certain facts are subject to review by the supervisory authority

be subjected to. So have particularly the complaints in the area

credit bureaus and in the health sector compared to the previous year

folds. On the other hand, the feared wave of warnings has not materialized so far.

In over 100 lectures, training courses and workshops at associations, economic

associations, other associations, public bodies, the Hessian

Administrative School Association (HVSV) and the Central Advanced Training Hesse

(ZF) my employees have the most urgent questions

answered. In the newly founded working group of data protection officers

I am also represented by the highest state authorities.

Many data protection audits I initiated were canceled due to lack of time

deferred. Nevertheless, 15 tests still took place (on-site tests

not included in the video sector), which could not be postponed.

Six legal trainees and two interns were also employed

trained at their respective stations.

185

186

balance sheet

5. Balance sheet

balance sheet

5.1

Digitization project school diary for children professional

Traveler advances

In the 46th activity report I wrote about the digitization project DigLu (Digi-

tal learning on the go) reported (Section 9.2). It's about creation

a learning and communication platform to help children of professional travelers

to facilitate learning. The facility is an important part of this

an electronic school diary. The project has some in the reporting year

significant data protection hurdles cleared.

5.1.1

The basic legal structure of the project has been created

The supervisory authorities of the countries involved in the planned pilot

North Rhine-Westphalia, Baden-Württemberg, Lower Saxony, Saxony,

Thuringia and Hesse, together with the DigLu working group of the

Conference of Ministers of Education (KMK) adopted a concept that after

Test run the other countries should also join.

In particular, it was clarified in the concept how the project with regard to

Competence and responsibility for data processing is designed.

The six pilot countries are to sign a contract for order processing in accordance with

Art. 28 DS-GVO with the service provider Jordy Media. In addition, should

by way of an administrative agreement, the state of North Rhine-Westphalia

Take over system management for the countries. Upstream of this is an

working group that addresses the needs for possible system extensions and

of the support determines and formulates. North Rhine-Westphalia will then take over

contact with the processor, issues orders and provides the opposite

two-way communication secure. The processor (Jordy Media with the

Software DigLu) uses the technical service as

Sub-processors of the network of the entity “Baden-Württembergs

extended LAN” (BelWü). This operates the network of scientific

Facilities in Baden-Württemberg along with data center services

and is also available to other interested parties for services.

5.1.2

For software and individual questions about the processing of personal data

data still needs clarification

With regard to the software, the functionalities and data security

Health concept not yet finalized. Also with regard to

Declarations of consent and the information i. S.v. Art. 14 GDPR exists

there is a need for further clarification and coordination. That's why both mine

employees and representatives

other supervisory authorities regularly attend the working meetings of the working

group DigLu involved in the data protection framework

of the application and its specific design (e.g. logging,

role and authorization concept, organizational structure).

It turned out that the classic function of the class register

addition, there is a need to use the platform for learning and communication

to use communication. An extension of the functionalities is fundamental

possible and logical within the framework of the digitization strategy of the KMK.

However, this requires clear guidelines and regulations in order to

nationwide unprecedented project of transnational cooperation

to lead to success in the interests of the children concerned.

5.1.3

outlook

The pilot project is scheduled to start in the 2019/2020 school year. The number of children should

within a manageable framework to initially a maximum of 300 students

and students are limited. After the pilot phase, a substantive and

technical evaluation of the project to identify the need for correction

gene and, if necessary, an optimization of the software or the organizational structure

take place. In the final stage, main and base schools of all 16

federal states are working with the platform and giving the children a contemporary one

Enabling participation in school activities.

5.2

Data protection-compliant use of Microsoft Office 365 in schools

(46th activity report, Section 9.3)

With the announcement by Microsoft for the Microsoft Cloud Germany

to no longer conclude new customer contracts with the trustee model,

Schools in Hesse are again faced with the question of the extent to which the use of

Products Microsoft Office 365 or Azure in the context of the European

balance sheet

Cloud offers of the group in terms of data protection law and with regard to

technical design can be implemented in compliance with data protection.

Microsoft's change in business model

On August 31, 2018 Microsoft published the announcement, no new contracts

more to close on the basis of the Microsoft Cloud Germany. new customers

From 2019/2020 you can also access a cloud offer in data centers in

Access Germany, but in the global standard of the group

will be involved. This means that the trustee model with its

special design features to existing customers up to a maximum of

are available at the end of the contract if customers do not

go into a migration offer from Microsoft beforehand. A row

of schools and school authorities had in the past year before the

Background of significantly higher costs can not make up one

Realization with the Microsoft Cloud Germany.

The administrative modernization working group of the conference of data protection

of the federal and state governments, after the trustee

model is no longer available, decided to do the remaining

Offer now subject to the legal requirements and considerations of the GDPR

to check again. In order to do justice to the complexity of the questions

den, a separate sub-working group was appointed, which under extensive

Postponing the technical questions will first examine the extent to which

Standard contracts are suited to the requirements of the Basic Regulation

to fulfill an order processing.

Latest releases for Office 365 and Windows 10

At the end of the year, publications by government agencies

Netherlands and Germany public that particular the transmissions

of telemetry data to Microsoft itself for Enterprise license customers

zen a barely manageable problem when using Office 365 and

Display Windows 10 in the cloud environment. I have this problem

already pointed out in my 44th activity report (item 5.1).

This raises additional questions for the schools and school authorities

what measures the impermissible transfers of personal

Data to Microsoft can be excluded. Various solution

approaches are currently being investigated. My office is dealing with it

is currently dealing with the subject again at school level and is looking for

for sensible and feasible alternatives.

5.3

Handling patient records after a hospital closes –

The new regulation of § 12 Para. 5 HKHG

In the past activity reports it was repeatedly reported that

that there are currently no regulations in Hesse regarding the handling of patient

medical files after the planned or unplanned closure of a hospital

house exists. In the meantime, the Hessian Ministry for Social Affairs has told me

and integration (HSM) a draft of a corresponding regulation for

the Hessian Hospital Act (HKHG) to be amended.

background

In the past, both planned and unplanned closures

hospitals disclosed that dealing with the associated

gene patient files was not adequately regulated. In particular, it was over

In my view, it is important that both the secure storage of the files

is guaranteed in these cases, as well as that the former patients

still be able to view their patient file without any major loss of time

and a specific contact person has been named for this purpose.

With the new § 12 para. 5 HKHG, this should now be taken into account.

Section 12 (5) HKHG

The hospital operator is obliged when closing a hospital or

a hospital establishment to ensure that the medical records

the regulations on confidentiality and data protection are kept and only

are accessible to authorized persons.

The version reproduced here dates from April 2018.

it says:

“The proper backup and storage of patient records

after the closure of hospitals or after the closure of

production facilities of a hospital has been increasing in recent years

been discussed again. The Conference of Health Ministers (GMK)

this topic is also discussed and there is a need for action when dealing with

Patient files from closed facilities, such as e.g. B. hospitals and

rehabilitation facilities identified. Also the Hessian data protection officer

recently confirmed this need for action in its 45th activity report.

The new regulation of § 12 Para. 5 HKHG takes up the need for action and

obliges the hospitals or their legal successors when they close

of a hospital or a branch of a hospital therefor

190

balance sheet

to ensure that patients' right to inspect files

acceptance according to § 630g BGB is secured".

Legal Assessment

I have the following comments to the HSM on the draft

made:

In the 2017 discussions with the HSM it was discussed that the

affected hospitals as part of the closure

to create and submit a concept that shows that and

in particular how the storage and inspection of files is ensured

becomes. The concept could both the HSM and the Hessian

Mandatory submission for data protection and freedom of information

be. Ultimately, the description is "at the closure of a hospital"

relatively vague, so a more precise definition should be given. From my

ner point of view, it is therefore necessary in advance, regardless of a

impending closure, a procedure on how to proceed in the event of a

closure (in the sense of technical and organizational measures).

Section 18 of the Berlin Hospital Act also stipulates timely information

obligation to inform the technical supervisor if the closure of a

hospital becomes foreseeable (especially in the case of an application for

opening of insolvency proceedings). In my opinion, this should also be included in the regulation

be taken over.

It would also be worth considering whether in the event of the insolvency of the hospital operator

even a catch-all solution cannot be created. Independent

an addition to this seems appropriate, as is provided for in Section 39 (6) of the State

kenhausgesetzes Mecklenburg-Vorpommern (LKHG M-V), since the

Hospital carrier itself may not be able to take custody of the files:

"If a contractor takes over after a cessation of operations of a crane

kenhauses the entire stock of patient data, are considered to be

responsible body with regard to the processing of this data the regulations

this section. Upon acceptance, it must be contractually ensured that the

patients for a period of ten years after completion

treatment or examination upon request in the same way as

previously received information and insight from the hospital."

To what extent the information I provided was included in the draft

were made is not known to me.

191

The Hessian Commissioner for Freedom of Information

1. Freedom of Information Report

192

Second part

First Freedom of Information Report

1. Freedom of Information Report

193

194

Introduction

1 Introduction

Introduction

1.1

Express constitutional requirements

Originally, freedom of information was only understood in Art. 5 Para. 1

Sentence 1GG standardized basic right, from generally accessible sources

freely to inform. The provision ties in with older state constitutions

13 HV after the Second World War

Regulations in response to information suppression in the national

contained socialism. The fundamental right in Art. 5 Para. 1 Sentence 1 GG is pure

Defense law does not design and convey any information claims. About the

Accessibility and the type of access opening decides who after the

legal system has a corresponding right of access (BVerfGE 103,

44, 60). If this provision is missing, the procurement of information

not protected by the fundamental right to freedom of information (BVerfGE 66, 116,

137; BGH, NJW 2019, 757, 762). This restriction exists according to the law

decision of the Federal Constitutional Court, although the court

legal meaning of an informed public in various

connections. As it stated, only “comprehensive

Information taken care of by sufficient information sources

will enable free opinion formation and expression for the

individually as for the community” (BVerfGE 27, 71). However, that includes

Fundamental right of freedom of information a right directed against the state

on access in cases where a state responsibility

source of information based on legal requirements for public

chen accessibility is determined, but the state refuses access

(BVerfGE 103, 41, 60). This creates the fundamental right from Art. 5 Para. 1

Clause 1 GG, however, no performance dimension to which claims are based

information or inspection of files could be supported. Such claims

can, however, arise from other constitutional or ordinary legal

chen legal bases result. Such claims for information are excluded

Art. 5 para. 1 sentence 1 GG does not apply.

1.2

Freedom of Information Laws

Further information claims result from the public

principles of freedom of information laws, which are often (cf. Kloepfer,

Information Law, 2002, p. 403) on the Swedish Freedom of Print Ordinance

(Tryckfrihetsförordningen - TF) dated December 2nd, 1766

1949 under the same designation by the constitutional

195

The Hessian Commissioner for Freedom of Information

1. Freedom of Information Report

been replaced by the Swedish Press Freedom Act (SFS 1949, 105).

is. Initially, these regulations only concerned special media law

Right to information. In addition, exceptions were made to protect personal

personal and financial circumstances of the individual (Chap. 2 § 2

#7 TF). Unconditional general information rights granted

only in the USA at national level the Freedom of Information Act (FOIA),

which came into effect on July 5th, 1967 and since then has changed several times

trend has been changed. The law contains nine exceptions,

including an exception in favor of data protection (privacy); added

the so-called Glomar Response (Ellington,

in Marlin/Scott Brady/Kumar, Secrecy, Law and Society, 2015, p. 160). On the

FOIA website (National.FOIAPortal@usdoj.gov.9) will follow

to the jurisdiction of the Supreme Court the task of the law as

characterizes the basic democratic function: “The basic function

of the Freedom of Information Act is for informed citizens

that are essential for the functioning of a democratic society

are necessary" ("the basic function of the Freedom of Information Act is to

ensure informed citizens, vital to the functioning of a democratic society”).

The Supreme Court went further: “The fundamental function of FOIA

be it to ensure an informed citizenship, its functioning

needed to counterbalance corruption

and the accountability of government to the governed

guarantee" (NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 [1978]).

In Germany saw for the first time the Brandenburg files inspection and

Information Access Act (AIG) of March 10, 1998 (GVBl. I p. 46)

tongueless claims for information. The law was not considered true

referred to as the Freedom of Information Act. The purpose of the law was not primary

the right to information, but the control of the administration,

which should be made possible through transparent administrative action.

The need debate in the late 1990s

of freedom of information laws was less concerned with the question of whether

a general access to public documents as a subjective right

be granted than the impact of public and trans-

parenzprinciple on the quality of administrative action. The ambivalent

Objectives can be found in all of them with a different focus

Freedom of Information and Transparency Laws enacted after 1998

namely: Confederation: Law regulating access to information of the

Federal (Federal Freedom of Information Act - IFG) from 05.09.2005 (Federal Law Gazette I p. 2722); Baden-Württemberg: Law regulating access to domestic formations in Baden-Württemberg from December 17, 2015 (GBl. p. 1201); Berlin: Berlin Freedom of Information Act – IFG of October 15, 1999 (GVBl. p. 561);

Bremen: Law on Freedom of Access to Information for the State Bremen (Bremer Freedom of Information Act - BremIFG) from 05/16/2006 (GBl. p. 263); Hamburg: Hamburg Transparency Act (HmbTG) from June 19, 2012 (GVBl. p. 271); Mecklenburg-Western Pomerania: Regulation Act access to information for the state of Mecklenburg-West Pomerania (Freedom of Information Act – IFG M-V) of July 10, 2006 (GVOBl. p. 566); North Rhine-Westphalia: Law on Freedom of Access to Information for the state of North Rhine-Westphalia (Freedom of Information Act North Rhine-Westphalia – IFG NRW) of November 27, 2001 (GV p. 806); Rhineland-Palatinate: State Transparency Act (TranspG) of November 17, 2015 (GVBl. p. 383); Saar-Country: Saarland Freedom of Information Act (SIFG) of July 12, 2006 (OJ p. 1624);Saxony-Anhalt: Saxony-Anhalt Information Access Act - IZG LSA from 29.06.2008 (GVBl. P. 242); Schleswig-Holstein: information transitional law for the state of Schleswig-Holstein from January 19, 2012 (GVOBl. p. 89).

Data protection and with it informational self-determination understood as barriers to information claims that oppose each other were to be weighed. In the individual freedom of information laws given different weights to transparency. From this believed Transparency protagonists to set up a ranking of the laws. The means in a nutshell that a good rating of transparency by a

bad privacy rating is bought by relying on that

process. However, against this misunderstanding, front-line

genes, because the antinomy of freedom of information and data protection

development does not do justice to informational self-determination.

1.3

Informational self-determination

1.3.1

dogmatic foundations

Informational self-determination has been

several times in quality reports. After that lies the informational

Self-determination is a fundamental right that has not been named (by the legislator).

based on what was originally used for the still largely unknown

to label data protection fundamental rights. The specifications described

of this fundamental right were only snapshots. today's understanding

of informational self-determination goes beyond this approach. The

informational self-determination is based on as an institute of constitutional law

development planned. The further development should not be aimless, but

which run in an orderly manner. In order to develop in this sense

In order to be able to exert influence, it is helpful to know the previous lines of development

to sketch again roughly.

1.3.2

forerunners in writing

Informational self-determination is a construct of the Federal Constitution

sung judiciary The Federal Constitutional Court in turn seized suggestions

of the literature and dealt with the criticism from the literature

other The development of informational self-determination through the

Federal Constitutional Court is therefore only understandable if the references

to statements from the literature are also taken into account. So became

Expression and – to some extent – also the concept of informational self-

mood developed by authors who also served as trial representatives in the People's

census disputes occurred. As far as can be seen, the expression is first

used in a report that Steinmüller gave to the Federal Minister of

Internally reimbursed (published as an appendix to BT Drucks. VI/3826). There

on p. 139 there is the statement: "... must be further determined

that the general freedom of action is the right of disposal and thus the

Right of retention with regard to all individual information includes, i.e

is to be understood as a 'right to informational self-determination'." They don't

more precisely defined informational self-determination was classified as a sub-category of

general freedom of action. A fuller rationale

for this Podlech delivered in the alternative commentary on the Basic Law (1st ed.

1984, Art. 2 para. 1, para. 45). Only those who have a sufficiently secure pro-

gnose can see which information pertaining to him in particular

certain sectors of his social environment are known, specifically only who

can roughly estimate the knowledge of possible communication partners,

be able to take actions in the future of your own self-determination

to plan and decide. With Art. 2 para. 1 GG is a legal system

incompatible, in which the citizen could not know who, what, when and by

what occasion knew about him. Both authors expressed themselves in the Volks-

census dispute of the Federal Constitutional Court. Your argument to the

actual prerequisites for informational self-determination

adopted by the Federal Constitutional Court. Expressis verbis tied that

Federal Constitutional Court, however, to its own case law.

198

Introduction

1.3.3

census verdict

In the census judgment (BVerfGE 65, 1) created the Federal Constitutional Court

the fundamental right to informational self-determination in order to

future conditions of automated data processing”.

become. In doing so, it used formulations from the literature to link

analysis of several strands of argument in his previous case law.

The test standard was that in Art. 2 Para. 1 GG in connection with Art. 1

Para. 1 GG guaranteed general right of personality, which already in the

Microcensus decision gives the individual citizen an untouchable right

assigned to a rich private life (BVerfGE 27, 344 [(350)];

see also BVerfGE 120, 274 (321 f.). From the thought of self-determination

With this in mind, the Federal Constitutional Court derived the power of the individual

to decide when and within what limits

personal circumstances would be revealed (freedom of conduct).

Individual self-determination presupposes that the individual

possible to find out about actions to be taken or not to be taken

to decide freely (freedom of decision). I don't have this freedom

who does not know which information of the social environment affects him

are known. “With the right to informational self-determination would be

a social order and a legal order that enables it

incompatible, in which citizens can no longer know who, what, when and what

on which occasion knows about them" (BVerfGE 65, 1, 43). who unsure

be whether deviating behavior is noted at any time and as information

stored, used or passed on permanently, will be in the

Try not to attract attention with such behavior. who with

Calculates that about participating in a meeting or citizens' initiative

is registered with the authorities and that risks may arise as a result,

may affect an exercise of its relevant fundamental rights

waive. This would not only increase the individual development opportunities of the

Affect individuals, but also the common good, because informed

Citizens functional condition of a free democratic basic order

be. While the Federal Constitutional Court extended the scope of protection of the

circumscribed the newly created basic right in a rather vague way, it tried

for precise specifications for the barriers. After that, the fundamental right is true

not without limitations, however, there would be

tionary self-determination higher requirements than the general one

freedom of action. Interventions in informational self-determination are required

a legal basis that corresponds to the requirement of norm clarity

that the principle of proportionality is data protection specific

to interpret. Finally, it is necessary to preserve the earmarking

principle.

1.3.4

Further development

thrust of the case law of the Federal Constitutional Court

First of all, the defense against state intervention in informational self-

protection areas covered by the provision. Unlike the literature that

based primarily on Article 2(1) of the Basic Law, the Federal

constitutional court on Art. 2 Para. 1 and Art. 1 Para. 1 GG. This combination

originally served the Federal Court of Justice to strengthen the

Freedom of action in the event of serious violations of personal rights. In the-

In this context, protective spheres developed, which culminated in

"Core area of private life", which in turn immediately

was protected by Art. 1 Para. 1 GG. But was human dignity the

a fixed point for the assessment, then Art. 2 para. 1 GG had to be the second

be a fixed point. In this way, a weighting scale for interventions was created

into the newly named basic right of informational self-determination.

At the 17th Wiesbaden Data Protection Forum 2009, the then

President of the Federal Constitutional Court: "It is indeed the case

that in all of these freedom rights - the protection of personality -, but

also the special freedom rights such as the protection of inviolability

of the apartment or the protection of telecommunications secrecy

Art. 10 GG contains a core of human dignity. You are absolutely right. Basically

it is still necessary to differentiate between spheres of fundamental rights protection,

Professor Dr. Ronellenfitsch. You put it beautifully. The more

the state intervention approaches this area of the core of human dignity,

the higher the requirements for the weight of the object to be protected

Legal interest" (in: The Hessian Data Protection Officer/ The President of the

Hessian State Parliament [Hrsg.], Specifications of the Federal Constitutional Court for

the contemporary data protection culture in Germany, 2010, p. 45). The information

tional self-determination is therefore dynamic in the also dynamic

to understand the system of values laid down in the Basic Law.

1.4

Hessian solution

Under Section 2.4.1, the development of the Hessian data protection law was

part of the right to informational self-determination

that. The same development merely presents from a different angle

the development of the Hessian Freedom of Information Act. This

An intensive legal and legal-political discussion followed

ahead, which will culminate at the 15th Wiesbaden Data Protection Forum

2006 (cf. The Hessian Data Protection Officer/The President of the

Hessian State Parliament [ed.], Freedom of Information and Data Protection, 2007).

In the closing remarks at this event, the Hessian Data Protection

commissioned: “The legislators play tricks on themselves when they

the opportunities for an informed population in the interests of democracy

not use” (ibid. p. 86). He spoke on other occasions as well

Hessian data protection officers frequently for a Hessian information

Freedom Act (cf. 34th activity report, Section 2.1.2.2; 35th activity

1.3.1). In the opinion on the draft law of the parliamentary group of

SPD for a Hessian Transparency Act (Hess. TG – LTDrucks. 18/7200)

it says: "The basic law and the Hessian constitution protect the

Human beings as communicative beings through a bundle of written

and unwritten fundamental rights, including freedom of information

counts. Informational self-determination also implies the right to opt out

publicly accessible sources. task of the legislature

is to open such sources, or at least the free and safe ones

to ensure the flow of information. The production of such information

Freedom of operation has always depended on the task of data protection

recorded." The extension of informational self-determination in the

Greater access to information strengthens the legal status of citizens

and citizens and does not make them a means to an end of state control.

The Hessian legislator has therefore refrained from using the transparency

principle as a civil control instrument over the administration.

201

202

Main features of the Hessian Freedom of Information Act

2. Main features of the Hessian Freedom of Information Act

Main features of the Hessian Freedom of Information Act

The Hessian Ministry of the Interior met with me on two dates for a

Educational event for the department heads of the

carried out in the Hessian ministries, in which, in addition to the new data

protection law (esp. DS-GVO) the right to information according to the Hessian

Freedom of Information Act was explained in its main features.

2.1

scope of application

The fundamental right to access from public authorities

with regard to official information (§ 80 Para. 1 HDSIG) is

law made legal. As far as the law access to information

opened, the official information is then general

accessible sources within the meaning of Art. 5 Para. 1 S. 1 GG. fully

taken is the right to access information with regard to the police

authorities, the state office for the protection of the constitution, the state antitrust authorities,

the Regulatory Chamber of Hesse, the Chambers of Industry and Commerce, the

Chambers of crafts and notaries, Section 81 (2) HDSIG.

In addition, according to Section 81 (1) HDSIG, there is a right to information

access to certain positions only if not - pointedly formulated -

lated – the main function of the body is affected. So the claim is there

only with regard to the general administrative area at the following positions:

– Hessian state parliament

– Hessian Court of Auditors

– Hessian data protection officer

- Dishes

– Law enforcement and law enforcement agencies

– Financial authorities

– university hospitals

– research institutions

– Universities

- Schools

– Hessian Radio

– Hessian state institute for private broadcasting and new media

The legislature has provided for a special regulation for the municipalities

(§ 81 No. 7). He leaves the validity there to the Hessian information

Freedom Act to the "local parliaments" as free self-government

Task: It is up to them to decide whether §§ 80 ff. HDSIG

to be expressly determined by the articles of incorporation.

However, the law does not only open up the right to access information

with regard to certain public authorities, but granted

the claim related to all public bodies in accordance with

substantive criteria, namely special public and private concerns.

2.2

Protection of special public and private interests

In favor of these concerns, the claim according to § 82 HDSIG exists entirely

not for classified information within the meaning of the Hessian security check

1) and in the case of professional or special official secrecy

underlying file or file content (No. 4).

The claim according to § 82 No. 2 HDSIG is not generally excluded,

according to which it must be checked in each case whether the disclosure of

information may have an adverse effect on:

a)

international and supranational relations, the relationship with the federal government or

to another country

b) matters of external or public security,

c) Control, enforcement or supervisory tasks of the financial, regulatory,

Savings banks, insurance and competition supervisory authorities,

d) the success of a criminal investigation or enforcement

proceedings or the course of proceedings of a court, administrative offense

court or disciplinary proceedings.

Especially the protection of the basic rights of citizens, but also that

Protection of fundamental rights of legal persons (Art. 19 Para. 3 GG) serves the

success of § 82 No. 4 HDSIG, according to which a right to information access

does not exist in the case of secrets belonging to the personal sphere of life

or trade and business secrets, provided the data subject

has not consented.

2.3

Data protection as a prerequisite for access to information

Data protection and access to information are not independent of each other

areas of law, but the access to information presupposes the observance of the

data protection ahead. As far as personal life is concerned,

the person concerned determines whether and to what extent a right to information

Main features of the Hessian Freedom of Information Act

Access exists: Without the consent of the person whose rights are affected

there is no access to information (§ 82 Para. 4 No. 2 HDSIG).

If the consent is not given within one month after the request

the public body from which the information is requested is available, the

Consent of the person concerned to access the information of the applicant

the person as denied (§ 86 S. 2 HDSIG).

As far as the personal area of life is not affected, it is

When it comes to personal data, access to information is not subject

subject to the reservation of consent of the person concerned, but subject to consideration

retained by the competent public authority. The decision-making authority

shifts in this case from the person concerned to the public

Body responsible for deciding on access to information.

How to "Protection of personal data", according to the official headline

Section 83 HDSIG, which is to be followed by the public body, gives this

Regulation briefly and concisely:

“Information access to personal data is only if and to the extent

permitted, as their transmission to a non-public body is permitted."

Here, too, the HDSIG clearly shows that the decision of the

to regulate data protection and freedom of information in a law,

is concise in terms of the legal system, because data protection and access to information

are interlinked in the HDSIG on legal dogma:

The content of Section 83 HDSIG refers to Section 22 (2) No. 2 HDSIG and

forms together with this standard a joint provision. This requires

an assessment of the legitimate interests of the person requesting information and

the legitimate interests of the data subject. So for this review

the necessary information is available as far as possible, the application

justify his request for information (§ 85 Para. 3 HDSIG) and the in

those affected by his data must be given the opportunity to comment,

if there are indications that he has an interest worthy of protection

on the exclusion of access to information (§ 86 Sentence 1 HDSIG).

2.4

The decision on a request for information

Deadlines for the decision

The law determines the decision on an information request

deadlines. A decision must be made immediately, i.e. without culpable hesitation,

but at the latest within one month, at the latest in the case of third-party participation

within three months of receipt of a sufficiently specific

application, Section 87 (1) HDSIG. The public body can change these deadlines

extend one month if the provision of information is due in particular to

the complexity of the information request cannot be met,

Section 87 (4) HDSIG; so can with information requests without third party involvement

the deadline can be extended to two months in the case of third-party participation

four months.

The applicant must inform about such an extension of the deadline under

You will then be informed in writing, stating the relevant reasons

(§ 87 para. 4 sentence 2 HDSIG).

Notification and execution of the decision

If the request for information is granted, the information must

made accessible within the deadlines applicable to the decision

be, § 87 para. 2 HDSIG. If a decision granting the application

divorce of the public body affects the rights of other persons,

they must have the opportunity to appeal against the decision of the public

take legal action to ensure the legality of the measures taken

to have the decision reviewed. Therefore, in such a

If third parties are affected, access to information is only granted

if the decision of the public body, i.e. this administrative act,

has become incontestable/final, i.e. if no legal

helf is filed, one month after notification of the decision

Instructions on legal remedies and one year after notification of the decision

without instruction on legal remedies (§§ 58, 74 VwGO).

It is evident that in the case of a granting the request for information

decision, instruction on legal remedies is required in order to

not to unnecessarily delay the granting of payment.

Because in the case of information, the time of disclosure is sometimes a

§ 87 para. 2 sentence 2 in the case of the arrangement of the

Immediate "enforcement" (correct: "enforcement": § 80 para. 1 No. 4 VwGO) of

administrative decision granting access to information

after two weeks from the date of notification of the order

immediate execution to the third party whose data is involved. The

Third party has turn in this period of time the opportunity to provisional

To request legal protection from the administrative court (§ 80 Para. 5 VwGO).

On the other hand, the requested access to information will be granted by the public body

rejected in whole or in part, this decision must be made in writing

be justified. And it has to state whether and when an information

claim in whole or in part is expected to take place at a later date

206

Main features of the Hessian Freedom of Information Act

could be possible (§ 87 Para. 3 HDSIG). against the decision of

public body about the provision of information is a preliminary procedure

not take place, but there must be direct administrative court legal

protection can be claimed, Section 87 (5) HDSIG. Come in addition

the opportunity to contact the Hessian Freedom of Information Officer

to contact, § 89 HDSIG. In short, according to this regulation, it is

assignment and authority of the Hessian Freedom of Information Officer,

to support and support the implementation of the Freedom of Information Act

check. In addition, the Commissioner for Freedom of Information himself

a public body that is (partially) subject to access to information.

207

208

previous implementation

3. Implementation so far

previous implementation

3.1

Requests for information to the Hessian representative for

Freedom of Information

Several submissions concerned documents from Schufa Holding AG (Schufa). There

my authority the data protection supervisory authority responsible for this company

authority is (company headquarters is Wiesbaden) and there this company

with a view to its data processing, in particular the evaluation of

Creditworthiness of citizens (score value), data protection

is of great relevance from the point of view of the authorities are important in my house

Documents relating to the credit agency are available.

Among other things, the contributors wanted Report commissioned by Schufa Holding AG

had given and who deal with their scoring procedures, available

received. I have rejected the request for information,

because the documents do not concern my general administrative

rich, but are the subject of my data protection supervisory authorities

Test. In this respect, there is no access to information, Section 81 (1) No. 3

HDSIG (more detailed explanation of the reasoning of the government draft on § 81,

LTDprints. 19/5728, p. 149).

If this special regulation did not exist in § 81 Para. 1 No. 3 HDSIG,

with a view to Section 82 No. 4 HDSIG, the difficult question would have arisen as to how

far when assessing creditworthiness the trade secret of

Schufa is enough.

Assessing the reach of trade and business secrets

one of the most sensitive issues in the context of freedom of information

attack. This is shown most vividly by the

ne decision of the European Court of Justice (concerning the Federal Institute for

Financial Services Authority/Builder) completing an over

ten-year judicial dispute regarding the information

obligation of BaFin towards a person requesting information.

The plaintiff was through a financial company (Phoenix Kapitaldienst GmbH),

which was subject to the supervision of BaFin, by means of a fraudulent so-called

so-called "pyramid scheme" (ECJ, judgment of 06/19/2018

– C-15/16; NVwZ 2018/1368 ff. with note B. Huber).

Such a lawsuit would be against the Hessian Freedom of Information

commission therefore unthinkable, because with regard to his authority just only

general administrative tasks are affected by access to information.

Precisely because of this legal requirement, on the other hand, I have

se information requests answered immediately, which the file management

my authority/collaboration with the Hessian State Archive or

also the personnel expenses of my authority for the subject area "video surveillance

vigilance".

3.2

Information requests to other public bodies

Insofar as requests for information have been sent to other bodies, that is mine

only become known if in the process (often also by telephone)

Complaints or inquiries from the applicants or

have been addressed to me by the public authorities concerned.

Information requests to municipalities

There were several requests for information from local authorities. Rarely

Municipalities had not reacted at all to a request for information.

As a rule, the applicants were informed by the municipality that

the Freedom of Information Act at the municipal level only applies if

that the local council has decided by statute (§ 81 Para. 1

No. 7 HDSIG). As far as municipalities exceptionally not on an application

answered, it came to me to make submissions, which I then referred to

have answered this legal position.

In this context, by contributors, but in particular also by

harsh criticism expressed by the freedom of information officer that it was the information

detrimental to freedom of information and the associated principle of democracy

not having imposed freedom of information on municipalities by law,

does not convince me in its sharpness. On the contrary, it is just one too

expression of democracy, the introduction of freedom of information

left to the municipal level of the people's representation. that me

so far except for the big cities of Hesse (Frankfurt am Main, Wiesbaden,

Kassel, Marburg) no municipality has become known that uses the

of the Freedom of Information Act for their area

intended, also shows the distance of the local people's representatives

the freedom of information regulations in the municipal sector.

Against this background, I generally assume that the municipalities

with regard to the applicability of the Freedom of Information Act rather

will be reticent. You are also in the case of this missing application

availability does not prevent requests for information from citizens

to answer by way of free self-government.

210

previous implementation

Requests for information, in particular to ministries

The focus of my work in the field of freedom of information

concerned the coordination with the ministries when dealing with information

bear. In the area of freedom of information, this coordination between

Applicants, the freedom of information officer and

The term "mediation" has become commonplace for the public bodies concerned.

It is striking in this context that I often already have complaints

then got when the standard one month reply period

request for information was exceeded by one day (this particularly applies to

Submissions for which the “fragdenstaat” internet portal is used). This

On the one hand, the procedure appears petty; but on the other hand it is possible

through a corresponding interim message from those affected

Prevent public body, § 87 Para. 4 HDSIG. Exactly such a

However, the public authorities sometimes did not send a message

given and it is hoped that this will improve over time.

However, the applicants often overlooked the fact that in the case of third-party

instead of a 1-month period, a 3-month period applies instead, Section 87 (3) HDSIG,

and that the period only begins to run “after receipt of the sufficient

specific application”, § 87 Para. 1 HDSIG.

More important than the above, however, is the first bi-

lanz that I have not yet come across a case in which information was provided

was unlawfully not given to a correctly submitted application (in any case

not after my advice). This is reflected in Hesse so far

also no indication that in the field of freedom of information

an administrative court procedure could be pending to dispute

to clarify questions in a legally binding manner.

The costs – an extensive scientific inquiry at

Ministry of Education

In mid-2018, a professor from the University of Erfurt and the Science

Center Berlin for Social Research nationwide at the Ministries of Education

a very extensive questionnaire that covers numerous aspects of the

subject "Private substitute schools" concerned. Answering the questions was after

Statement by the Ministry of Education requires a lot of personnel and is time-consuming. To the

Questioners were therefore partly four-digit from other federal states

fees charged.

With regard to some procedural questions and in particular because of the cost

aspect, the Ministry of Education agreed with me. The applicant

were fees of EUR 600 according to the administrative cost

billed to the HDSIG. Although this is the maximum

the law for information fees in the context of freedom of information

planned, but still comparatively moderate.

§ 88 HDSIG expressly provides that the fees

taking into account the administrative costs are to be measured in such a way that the

This does not prevent applicants from asserting their

right to information be held. Definitely accordingly

the provision supporting the freedom of information as well as introducing it,

that the provision of verbal and simple written information as well as

the inspection of files and files on site are free of charge anyway.

212

materials

materials

1. Resolutions of the Conference of Independents

Federal and state data protection authorities

materials

1.1

Resolutions of the Conference of Independents

Federal and state data protection officers

from 04/26/2018

Facebook data scandal – New European data protection law

prevail on social networks!

In March 2018 it became public knowledge that one of No-

App linked to Facebook from November 2013 to May 2015, according to the

Company data from 87 million users worldwide, including 2.7 million

Europeans and about 310,000 Germans and sent to the analysis

take Cambridge Analytica. There they became evident

also used for profiling for political purposes.

For this reason, the nationally responsible Hamburg Commissioner

te for data protection and freedom of information against a fine

Facebook initiated. He is in close contact with his European

European colleagues, particularly with the Information Commissioner's

Office in Great Britain and the Article 29 Group. The data scandal

around Facebook and Cambridge Analytica highlights the

gang with millions of user data. In addition, the processes are documented

Cambridge Analytica that Facebook developers for years

of apps the mass access to data from with the users of the

Apps made possible for friends on Facebook. That happened without

consent of the persons concerned. In fact, the currently discussed case

a single app is just the tip of the iceberg. So goes the number of apps

who use the Facebook login system number in the tens of thousands. The number of

persons unlawfully affected by this, the dimension of the cam

bridge Analytica-Falls in dramatic fashion and the reason

after all Facebook users affect. The incident also shows

the risks for profiling when using social media and subsequently

ing micro-targeting, which apparently leads to the manipulation of democratic

decision-making processes was used.

The data protection conference demands from these apparently mass

violations of data protection rights of data subjects to the following consequences

pull:

– Social networks must adapt their business models to the new European

Align European data protection regulations and their social

meet responsibility. This also includes taking reasonable precautions

to take measures against data misuse.

– Facebook needs the true scope of opening up the platform to

Disclose app providers in the years up to 2015 and reliable figures

of the set apps as well as of the Facebook login system

name affected persons. Furthermore, it applies to those affected about the legal

to report injuries.

– In the future, Facebook must ensure that the specifications of the data

of the General Protection Regulation (GDPR) are implemented in a legally compliant manner:

Facebook's presentation of the introduction of automatic

Visual recognition in Europe raises considerable doubts as to whether this

Approval procedure with the legal requirements in particular for

consent is compatible. When Facebook urges users to do so and

makes it much easier for them to process biometric data

to consent than to evade it leads to an impermissible

influencing the user.

– The reactions to data protection violations are not alone

limited to the enforcement of data protection law, but also affect

competition and antitrust law. The demand for a divestiture

of the Facebook group will increase to the extent that this

by systematically circumventing data protection

to create adverse advantages in the digital services market

tried. European initiatives are needed to break down monopoly-like structures

in the field of social networks to limit and transparency of

to create algorithms.

Because data processing processes are becoming increasingly complex and for those affected

become more non-transparent, data protection supervision is faced with an elementary one

roll to. Your technical expertise is in demand, it must be organizational and

be personally able to work in an advisory and creative capacity. a strong one

Data protection law and effective supervisory authorities together reduce the

Risks for citizens in the digital society. Should

Facebook and other social networks will not be ready to European

To comply with legal regulations for the protection of users, this must be done

consistently by exhausting all existing supervisory authorities

instruments at national and European level.

214

materials

1.2

Resolutions of the Conference of Independents

Federal and state data protection officers

from 04/26/2018

Public and private background checks

Events only to the extent required and after a

due process and transparency

Increasingly in the context of public and private events

Persons who work in different functions at an event

countries want to be active or otherwise request access to security zones

(e.g. residents), by security authorities on their reliability

checked. The police also call for private events

the organizers sometimes have to make sure that everyone is in the frame

of the event are subjected to such an examination. In the

most cases, the sole basis for these measures is still the

consent of those concerned.

More than ten years ago, the data protection officers of the

Federal and the federal states in their resolution of 25./26. October 2007

pointed out that only the consent of the persons concerned in an

background check no legitimizing basis for such depths

interference with the right to informational self-determination.

The repeated demands for the creation of legal bases

since then, the legislators have taken up only a few federal states.

The conference of independent data protection authorities of the federal and

of the countries (DSK) calls on the legislators and those responsible for

half again emphatically, for a constitutional and transparent

to ensure procedures for such background checks based on

absolutely required level remains limited, both in terms of the scope of

review and the affected group of people. are there

In particular, the following general conditions must be observed:

Background checks only due to a specific

legal basis

The legislators are asked to provide sector-specific legal bases

to create that respect the principle of proportionality and from

which the conditions and the scope of the checks are clear

and recognizable for the citizens.

Background checks only to the extent necessary

Application, scope, group of data subjects and data processing

work must be limited to what is necessary. In general,

background checks are only used at such events

due to their specific characteristics as a result of a resilient

danger prognosis can be rated as particularly endangered. correspond

the personal data that is included in the comparison

referenced files and information systems are stored, not

only have a sufficient quality, only sufficiently

important offenses are included in the review. In addition, they have to

Criteria that lead to the acceptance of safety concerns, a concrete

related to the threats to be averted.

Background checks only in a transparent

Proceedings

The rights and freedoms of data subjects must be protected by a

ensure a transparent process. In particular,

re rights of the data subjects to be heard are enshrined in law.

In the practical procedure, the establishment of a

Clearing place make sense. In addition, at least the data protection

commissioned by those responsible to be involved in advance so that a

Advice on data protection law for a data-saving design and

Limitation of the specific procedure can take place.

1.3

Resolutions of the Conference of Independents

Federal and state data protection officers

from 06.06.2018

The time of irresponsibility is over: ECJ confirms

joint responsibility of Facebook and fan page operators

The independent federal and state data protection authorities

Welcome the judgment of the European Court of Justice (ECJ) of June 5, 2018,

which confirms their longstanding legal opinion.

The judgment of the ECJ on the joint responsibility of Facebook and the

operators of a fan page has direct effects on the page

driver. These can no longer rely solely on the data protection

wording of Facebook, but are jointly responsible for

compliance with data protection for the users of their fan page.

216

materials

In doing so, they must comply with the obligations arising from the currently applicable regulations

of the General Data Protection Regulation (GDPR). Admittedly, the verdict

Reference to the former Directive 95/46/EC on the protection of individuals

in the processing of personal data to the free movement of data, yes

the co-responsibility of the site operators determined by the ECJ

refers to the applicable law, in particular to that in the DS-GVO

enshrined rights of the data subjects and obligations of the processors.

In detail, the following must be observed:

– Whoever visits a fan page must be transparent and understandable

be informed about which data for which purposes by Facebook

book and the fan page operators are processed. This applies to both

People who are registered with Facebook as well as for unregistered ones

visitors to the network.

– Operators of fan pages should assure themselves that Facebook

provides them with the information necessary to fulfill the

mentioned information requirements are required.

– As far as Facebook visitors of a fan page through

collection of personal data is tracked, be it through the use of

Cookies or comparable technologies or by storing the

IP address, the consent of the user is generally required,

that meets the requirements of the GDPR.

– For the areas of joint responsibility of Facebook and

An agreement must be made between fan page operators as to which of them
which obligation the DS-GVO fulfills. This agreement must
essential points are made available to those affected,
so that they can exercise their rights.
For the enforcement of the data protection requirements for a fan page, the
Supervisory authority responsible for the respective company or the
authority that operates the fan page is responsible. Enforcement of
Data protection requirements within the area of responsibility of Facebook itself
is primarily the Irish data protection regulator within the framework of the European
Cooperation.
The German supervisory authorities point out that according to the judgment of
CJEU, there is an urgent need for action for the operators of fan pages.
There is no mistaking the fact that the fan page operators protect their data protection
can only fulfill legal responsibility if Facebook itself
contribute to the solution and offer a data protection-compliant product that
protects the rights of those affected and ensures proper operation
Europe enables.

1.4
Resolutions of the Conference of Independents
Federal and state data protection officers
from 07.11.2018
The EU Commission's proposal for an e-evidence regulation
leads to the loss of data subject rights and exacerbates them
Problem of the so-called data retention

With its proposal for an e-evidence regulation (Regulation on
European Production Orders and Preservation Orders for
electronic evidence in criminal matters (COM (2018) 225 final)).
the EU Commission an alternative to the formal legal assistance
create and give the investigating authorities faster access
enable communication data. The law enforcement agencies of
EU member states are to be given the power to
cation and internet services in other EU member states and
also in countries outside the EU (third countries) for immediate release
of inventory, access, transaction and content data.
The DSK refers to the critical opinion of the European
Data Protection Committee (https://edpb.europa.eu/our-work-tools/
our- documents/opinion-art-70/opinion-commission-proposals-european-
production-and_de). This already represents the existence of a legal basis
in question. The DSK is particularly concerned about the proposed one
Abandonment of the principle of double or double criminality.
For the first time in the field of international cooperation in criminal matters
the release of data no longer depend on whether the tracked
Act where the data is requested is punishable at all. As a result
companies based in Germany could therefore publish data
be obliged to investigating authorities in other EU member states,
although the act being prosecuted is not a criminal offense at all in Germany. The
could, for example, an abortion permitted in Germany
be or express a political opinion if im requesting this
state is punishable.
It is also to be feared that third countries will use the EU regulation as a

use the blueprint for your own regulations. Provider in EU

member states would then increasingly issue orders from

See exposed third countries with which criminal offenses may be committed

be followed by a completely different legal tradition.

The DSK also sees critically that, as a rule, any information and

Participation of the judicial authorities of the state in which the provider is located

materials

has its registered office, and thus an important procedural correction

tiv missing. Whether the legality of a request is checked depends on the

proposed procedure depends exclusively on the behavior of the provider.

Only if the company refuses to transmit data does the

ask the requesting state for enforcement assistance from the local authorities.

Only then can they intervene in the process. Will data

published, the competent judicial authorities obtain this

No Knowledge. The proposal does not provide for any information obligation towards the

authorities at the company's headquarters. Provider track but in the

Rule economic interests and are subject in their decisions

other obligations than the judicial authorities

significantly worse off.

Providers as addressees of a request no longer see themselves as

Judicial authorities of their own state, but must deal with

deal with the authorities of the issuing state. the affected

In turn, there is only one legal remedy, if at all, in the requesting

member state whose legal system is usually foreign to them.

A special procedure is provided if providers based in

Third countries rely on the fact that the ordered transmission violates the
violates local law. In this case, the proposal provides for a judicial decision
verification in the issuing state. If the court to the opinion
comes to the conclusion that there is actually a legal conflict, the competent
competent authorities in the target state of the order. The result of
Consultation is binding on the court. This rule is explicit
to greet. Because here, too, a blueprint is created for the question
what rights European companies have in the opposite situation
should if they are from third countries on the basis of their laws (such as
e.g. B. US Cloud Act) are obliged to transmit and which
Mandatory consultation of the competent authorities in Europe for
should have courts in third countries.
However, it is particularly critical that in Germany telecommunications
service providers are obliged, e.g. all traffic data for ten weeks
save. These data allow precise conclusions to be drawn about the
life of those affected, in particular their contact and interest profile
pull. The problem of this so-called data retention is exacerbated
become clear when foreign law enforcement agencies direct
gain access to such information.
The DSK therefore appeals to all those involved in the legislative process
stop the proposal for an e-evidence regulation!

materials

2.1

Decision of the Conference of Independent Data Protection Authorities

of the federal and state governments from 05.09.2018

Refusal of treatment by doctors

Refusal of the patient to take note of the

Confirm information according to Art. 13 GDPR by signature

The data protection supervisory authorities of the federal and state governments are speaking to each other

against the fact that doctors or other members of health

health professionals refuse treatment or refusal of treatment

threaten if the patient fails to provide the information in accordance with Art. 13

DSGVO does not provide her or his signature. One such practice is

not compatible with the GDPR. The information obligation according to Art. 13 GDPR

only aims to give the patient the opportunity

is given, the relevant information simply and directly

to obtain. However, she or he does not have to acknowledge this if

she or he does not want this. In order to meet his obligations to provide evidence of

to comply with the supervisory authority, the person responsible can hand over the

of the information or concerning a specific procedure

document the implementation of the information obligation, which shows that

how the patient usually receives the information.

2.2

Decision of the Conference of Independent Data Protection Authorities

of the federal and state governments from 05.09.2018

Application of the GDPR in the area of parliaments, political groups,

MPs and political parties

The conference takes the result of the deliberations of the working group

Basic questions of data protection and recommends for the

further legal practice, the positions listed below

to base the activity as a supervisory authority on:

1. Insofar as data processing by parliaments (including their organs)

finally the MPs) the core parliamentary activities

are assigned, the GDPR does not apply.

2. Parliaments (including their bodies, including the members of parliament)

only lie in the exercise of original parliamentary core activities

then data protection requirements and the supervision of the supervisory

authority if this results from a clear legal regulation.

3. The classification of activities of parliaments (including their organs

including MPs) as administrative and fiscal in

Delimitation to the core parliamentary activity requires one in each case

Evaluation in individual cases.

4. If there are no legal bases for the core parliamentary

activity exist, a data protection regulation of the parliament would be allowed

recommend, which should be based on the GDPR. A consultation

by the supervisory authority should remain at liberty in any case.

5. Parties as non-public bodies are fundamentally addressees of norms

of the GDPR and are therefore subject to the supervision of the supervisory authorities.

A possible consideration of their special status in the frame

the application of the law remains unaffected.

2.3

Decision of the Conference of Independent Data Protection Authorities

of the federal and state governments from 05.09.2018

To Facebook fan pages

With a judgment of June 5, 2018, the Court of Justice of the European Union

(ECJ), file number C-201/16, ruled that a common

responsibility of Facebook fan page operators and

Facebook exists. The conference of independent data protection supervisory

Federal and state authorities (DSK) has in its resolution of

June 6, 2018 made clear the consequences of the verdict

for those jointly responsible - in particular for the operators

and operator of a fan page. With a joint responsibility

The General Data Protection Regulation (GDPR) requires, among other things,

an agreement between the parties that clarifies how the obligations

from the GDPR are met. It's been three months since the judgment of the ECJ

past. Although Facebook has some changes in its offer - for

Example regarding cookies - made, but still will be

for people who are not Facebook users, cookies

Identifiers set, anyway, if they're about the bare home page

Fan page also call up content there. Also, as before, the

Fan page visits by those affected according to certain, sometimes preset

th criteria as part of a so-called insights function from Facebook

evaluated and made available to the operators.

Among other things, the ECJ emphasized that “the

held fan pages can also be visited by people who do not

are Facebook users and therefore do not have a user account with them
have social network. In this case, accountability appears
the operator of the fan page with regard to the processing of personal
Genetic data of these people is even higher, since simply calling up the fan page
by visitors automatically the processing of their personal data
triggers data." Official announcements from Facebook, whether and
what steps are being taken to ensure a legally compliant operation
enabling Facebook fan pages have not yet materialised. One
agreement according to Art. 26 announced by Facebook in June 2018
GDPR (joint controllers) has not yet been implemented
made available. The German data protection supervisory authorities are working
therefore towards a coordinated approach at European level
to Facebook. Fan page operators must also
their responsibility under data protection law. Without agreement after
Art. 26 GDPR is the operation of a fan page, as currently operated by Facebook
offered is unlawful. Therefore, the DSK demands that the requirements
requirements of data protection law are met when operating fan pages.
This includes, in particular, that those jointly responsible for clarity
about the current situation and provide the necessary information
the persons concerned (= visitors to the fan page)
provide. However, shared responsibility also means
that fan page operators (regardless of whether it is
are public or non-public responsible persons) the legal
guarantee the reliability of the jointly responsible data processing
and be able to prove it. In addition, those affected can exercise their rights under the
GDPR with and against each person responsible (Art. 26

Paragraph 3 GDPR). In particular, the questions listed in the appendix must be answered

therefore both from Facebook and from fan page operators

and operators can be answered.

Appendix: Questionnaire

1.

In what way is shared between you and others

The responsible parties determine which of you is subject to which obligation

of the GDPR fulfilled? (Art. 26 Para. 1 GDPR)

2. On the basis of which agreement have you

defines who has which information obligations according to Art. 13 and 14 GDPR

follows?

3. How are the essential aspects of this agreement

made available to data subjects?

4. How do you ensure that the rights of the data subject (Art. 12 et seq. GDPR)

can be fulfilled, in particular the right to erasure according to Art. 17

DSGVO, to restriction of processing according to Art. 18 DSGVO

Objection according to Art. 21 GDPR and information according to Art. 15 GDPR?

5. For what purposes and on what legal basis do you process

the personal data of the visitors of

fan pages? What personal data is stored?

To what extent are visits to Facebook fan pages pro-

file created or enriched? Will also personal data

used by non-Facebook members to create profiles?

What are the deletion deadlines?

6. For what purposes and on what legal basis are the

First call-up of a fan page, even for non-members, entries in the so-called

called Local Storage generated?

7. For what purposes and on what legal basis are

call a subpage within the fan page offer a session cookie

and three cookies with lifetimes between four months and two

years saved?

8. What actions have you taken to meet your obligations

Art. 26 GDPR as joint controller

meet and conclude a corresponding agreement?

2.4

Decision of the Conference of Independent Data Protection Authorities

of the federal and state governments from April 26, 2018

Obligation to appoint a data protection officer in accordance with Article 37 Paragraph 1 lit. c

General Data Protection Regulation for medical practices, pharmacies and

other healthcare professionals

1. Is an individual doctor, pharmacist or other family member operating a

health profession a practice, pharmacy or a health professional

undertake and are there including his person as a rule

at least 10 people constantly involved in the processing of personal data

data employs, there is a legal obligation to designate

a data protection officer (DSB).

2. Doctors, pharmacists or other members of a healthcare

berufs, which belong to several in a professional community (practice

community) or group practice are merged

or other doctors, pharmacists or other relatives

have employed in a healthcare profession is not usually of

224

materials

extensive processing of special categories of personal

related data within the meaning of Article 37 (1) (c) GDPR

– in these cases, taking point 3 into account, there is no DPO

to be named if fewer than 10 people are involved in the processing of personal

of sun-related data are busy.

3. Doctors, pharmacists or other members of a healthcare

berufs, which belong to several in a professional community (practice

community) or group practice are merged

or other doctors, pharmacists or other relatives

health professionals who are at high risk

for the rights and freedoms in the processing of personal data

data is to be expected, a data protection impact assessment is required

written and thus mandatory to appoint a data protection officer

to. In addition to extensive processing (e.g. large

Communities of practice), which are already defined according to Art. 37 (1) (c) GDPR

leads to a naming obligation, for example when using new ones

Technologies that involve a high level of risk may be the case. The

A data protection officer must also be appointed if fewer

Less than 10 people are constantly processing personal data

data to do.

4. The term "health profession" is in the sense of the list according to § 203

Paragraph 1 of the Criminal Code and includes the provisions in Section 203 Paragraph 1 Nos. 1, 2, 4 and

5 StGB listed job descriptions.

225

226

materials

3. Guides and Samples

materials

3.1

Orientation guide “Video surveillance by non-public

Place"

Status: 02/19/2014 Version: 1.1

Table of Contents

5. Other video surveillance by non-public bodies, especially video surveillance

2.3.1 Duration of storage

2.3.2 Duty to inform

2.3.3 Audio Recordings

2.3.4 Verification of legality requirements

3.1 webcams

3.2 Video surveillance in gastronomy

by neighbors or landlords

6. Checklist for the operator of video surveillance of publicly accessible rooms

1.

Opportunities and risks of video surveillance

Video surveillance (for the term see 2.1.1) is supposedly able to

provide a simple solution to certain security problems. So can

some confusing building complexes at different times of the day

and nighttimes can be easily monitored. The supervision of the system

can be carried out centrally and with little personnel expenditure. The technique is

Affordable and regular to install without any special skills.

The relevance of video surveillance in terms of data protection law is

However, operators of a video surveillance system often misjudged.

In principle, everyone has the right to be free in public

to move without changing his behavior permanently with the help of cameras

observed or recorded. The fact of being watched

can cause a change in their appearance in many people because the

There is a risk that your own behavior will be checked and not authorized

e.g. B. is published on the Internet. With continuous monitoring

chung can be the knowledge that every movement and every gesture of one

Camera surveillance, with far-reaching psychological implications

to be connected. The individual feels constantly observed and is thereby

exposed to permanent monitoring pressure. With the use of

Video surveillance systems are associated with additional risks. There is the

Risk of records being misused or used for third-party purposes

become. Electronic images can be easily stored, copied

and unlimited to a large number of recipients in the shortest possible time and without

financial expense to be passed on. Comprehensive spatial and

time monitoring enables the creation of motion and

behavioral profiles. In addition, "intelligent" video surveillance systems

teme are no longer pure dreams of the future. For example, technically it is

possible, targeted individual people automated over a large spatial

Distance to track and unique by image matching in databases

to identify. It is also feasible, "conspicuous" or supposedly not

filter out normal movements and behavior patterns

and trigger an alarm if necessary.

This orientation guide is intended to provide information on the

regulations video surveillance is permitted and which legal ones

requirements are to be complied with. If with a camera personal

data are collected, e.g. B. people or license plates

are recognizable, the so-called ban with reservation of permission requires a

legal basis for data processing. There is a difference

between the video surveillance by non-public bodies in public

accessible rooms (§ 6b of the Federal Data Protection Act [BDSG]),

materials

the video surveillance of employees (§ 32 Abs. 1 BDSG) and one

other video surveillance in rooms that are not accessible to the public (§ 28

Federal Data Protection Act). At the end you will find a list of questions, those responsible and

can serve as a checklist for data protection officers.

2.

Admissibility of video surveillance by non-public bodies in

publicly accessible spaces

Relevant provision for the admissibility check of a video

security system is § 6b BDSG, which the video surveillance of public

accessible rooms by non-public bodies. non-public

Positions are private operators of video technology, e.g. B. company or

private individuals.

2.1

Scope and requirements of § 6b paragraph 1 BDSG

The following describes when this rule applies

and what requirements it places on a video surveillance system.

2.1.1

When is video surveillance available?

§ 6b paragraph 1 BDSG defines video surveillance as observation

“optical-electronic devices”. From this term are not only

commercially available video cameras, but any device that can be used for observing

attention suit, recorded. It is irrelevant whether they have a zoom function

or have a swivel device, whether the camera is mounted stably or

is freely movable. Also the use of webcams, game cameras, digital

Cameras or mobile phones with an integrated camera is fundamental
to be regarded as video surveillance (see also No. 3.1). Requirement is
in each case the collection of personal data, i.e. that personal
sons must be recognizable on the recordings or other conclusions
on the identity of a person are possible.
The term video surveillance includes both video surveillance,
in which the images are transmitted live to a monitor, as well as
the video recording where the recordings are saved. One
Video surveillance is already in place as soon as the possibility of observation
is given, that means that independent of a possible storage
or recording of the images even with mere live observation using

optical-electronic device to comply with the requirements of § 6b BDSG
are. The concept of observation also includes digital photography, provided that
based on a certain period of time. This falls under, for example
taking photos at short intervals is also subject to the regulation.
Targeted observation of individuals is not required. The
Even then, the monitoring measure starts with the commissioning
of the cameras if the devices only record in the event of demand or an alarm.
In the case of mere dummy cameras or inaccurate indications of a video
deomonitoring go to the data protection supervisory authorities of most
Federal states assume that the Federal Data Protection Act does not
Application comes because dummies are not optical-electronic
facilities and therefore no personal data is collected
become. However, the attachment of dummy cameras and

incorrect information from persons who take note of it,

regularly get the impression that they are actually under video surveillance. There

the lack of functionality of the camera cannot be seen from the outside,

a monitoring pressure can be generated1, which can impair

of personal rights and thus civil law defense

can trigger claims. If necessary, these must be enforced through legal action

become. Whether, in addition, a regulatory intervention against

a dummy is considered, differs depending on whether the locally responsible

supervisory authority also recognizes a material competence for this. This

Those affected may find out on request.

2.1.2

What is a public space?

The application of § 6b BDSG presupposes that a publicly accessible

space is observed. These are areas within

or outside of buildings which, according to the recognizable will of the

authorized (e.g. the property owner) used by anyone or

may be entered. A public space is also present if for

access special general requirements, such as a certain

minimum age must be met, an entrance fee must be paid or

opening only at certain times. On whether the monitored

The area is private property or not, it doesn't matter. To the public

accessible spaces include, in addition to public traffic areas,

wise exhibition rooms of a museum, sales rooms, counter halls,

Gas stations, beer gardens, public parking garages, guest rooms of restaurants

or hotel foyers.

materials

On the other hand, rooms that are only used by one person are not open to the public

certain and finally defined group of people can be entered

can or may. These include offices or production areas

without public traffic. It is crucial here that the non-public

can be recognized by prohibition signs or the context of the surroundings.

Your own private apartment counts e.g. B. to the not publicly accessible

rooms. It should be noted, however, that the classification as non-public

accessible space depends on the individual case. The stairwell of a

Residential building, for example, is basically one that is not open to the public

Space. However, if there is a doctor's office or a lawyer's office in the building

law firm open to the public, then this is already sufficient,

around the stairwell during business hours as open to the public

classify Video surveillance of non-public spaces

may have to be assessed according to § 28 BDSG (see below

No. 5.). There is also surveillance of publicly accessible spaces

if, in addition to private property, the public traffic area is also

the environment and the people located there are recorded. At

a neighboring property is not a public space;

its observation is therefore not covered by § 6b BDSG. However, it works

a monitoring of neighboring properties in the personal rights

of the neighbor. This can therefore take place under civil law by means of

Defense and injunctive relief claims against the video surveillance

Put up a fight (on video surveillance in the neighborhood, cf. below

#5).

2.1.3

Admissibility of video surveillance of publicly accessible rooms

According to § 6b paragraph 1 BDSG, observing is more publicly accessible
Rooms via video surveillance only permitted insofar as it is for perception
of domiciliary rights or to safeguard legitimate interests for specific purposes
specified purposes (2.1.3.1) is required (2.1.3.2) and no indications
for the existence of overriding legitimate interests of the data subjects
people exist (2.1.3.3).

2.1.3.1

purpose of video surveillance

Before video surveillance is installed, it must be specified which one
goal is to be achieved. A legitimate interest for the operation
of a video surveillance system can be non-material, economic or legal

be natural. If video surveillance is to be used for this purpose,
Protection against burglary, theft or vandalism is fundamental
a legitimate interest to see if there is an actual risk situation
can be proven. What is required are concrete facts from which
a hazard arises, for example damage or special
events in the past. It is therefore advisable to
to document events carefully (date, type of incident, damage
height) or to keep any criminal charges. Also the preservation of evidence
recording may represent such a legitimate interest.

In certain cases, an abstract risk situation can also be sufficient
be when there is a situation that, based on life experience, is typical
way dangerous, e.g. B. in shops that sell valuable goods (e.g.

jewellers) or who are po-

tend to be particularly at risk (e.g. petrol stations).

In addition, it must be specified in advance and documented in writing

document the purpose of the video surveillance in individual cases

should. The monitoring purpose of each individual camera is separate

and specify it specifically.

2.1.3.2

Suitability and necessity of video surveillance

Before using a video surveillance system, check whether

it is actually suitable and necessary for the specified purpose. The

The necessity of video surveillance can only be affirmed if

if the intended purpose is not equally compatible with another (economic

(scientifically and organisationally) reasonable, in the rights of the data subject

less intrusive means can be achieved. Before installation

of a video surveillance system, one must therefore make do with reasonable ones

alternative methods address the personality rights

of the individual to intervene less. A fence, regular control

guards, the deployment of a porter, the installation

security locks or burglar-proof windows and doors

can, for example, also provide effective protection against burglary

and offer theft. Application of special surface coating

can provide protection against graffiti damage.

Furthermore, before a camera system is put into operation, a check

be carried out as to where and at what times

monitoring appears absolutely necessary. Monitoring can often be

be sufficient during the night hours or outside of business hours.

materials

In the context of necessity, it must also be examined whether a pure

observation by way of live monitoring is sufficient or whether it is

Achievement of the monitoring purpose of a (regularly more intervention-intensive)

recording required. In this context it should be emphasized that a

Pure recording (black box) is not suitable for preventive purposes because

there is no direct possibility of intervention. This is only

given nitoring, since then z. B. Security personnel intervene immediately

can. This means that video recording to prevent

accidents or criminal offenses.

From the aspect of data avoidance and data economy is still

to check whether, through the use of special technology, certain areas of the

field of view is hidden or the faces of people in these areas

can be "disguised" by the people who are staying.

2.1.3.3

Consideration of the legitimate interests of the data subject

Even if video surveillance is used to protect domiciliary rights or to

It is only allowed to exercise a legitimate interest

be put into operation if the interests of those affected are worthy of protection

do not predominate. At this point there is a trade-off between the

legitimate interests of the monitor and those of the monitor

to take action. Scale of the evaluation is the informational

The right to self-determination as a special form of personal rights

on the one hand and the protection of property or physical

strength on the other side. When considering the overall circumstances

relevant in each individual case. The intensity of the intervention is often decisive
the respective measure. This is determined by the type of information collected
(information content), scope of the recorded information (information
te, temporal and spatial extent), the affected group of people, the
Interests of the affected groups of people, the presence of
Alternative options as well as the type and scope of the utilization of the collected
n data determined. In cases where the video recordings not only
transferred to a monitor, but also to be recorded,
is a relevant consideration with the interests of the protection worthy of protection
to carry out the affected person again.
In principle, observations that violate the privacy of the
injure people, such as monitoring toilets, saunas, showers
or changing rooms. The interests worthy of protection prevail
also often where the development of personality is in the foreground
stands, for example in restaurants, adventure and recreation parks, where people

communicate, eat and drink or relax. Also a permanent one
Surveillance that a data subject cannot avoid
more serious interference than an observation that is only temporary
takes place and only covers parts of the room. This is for example at
the permanent monitoring of public driveways and entrances
multi-family dwellings, since the occupants rely on the use of
guarded area. Basically, the more personal
Information collected as a result of surveillance, the more intense
is the encroachment on the fundamental rights and interests worthy of protection

concerned.

The quality of the recording does not allow personal reference

legitimate interests of those affected are not violated because it

there is no data collection within the meaning of Section 3 (3) BDSG.

2.2

Individual measures before setting up video surveillance

Before using a video surveillance system, there are a number of measures to be taken

and requirements according to the Federal Data Protection Act

and comply.

2.2.1

Directory of procedures, preliminary checks, security obligations

Before the beginning of the video surveillance is on the part of the responsible body

the specific purpose of the surveillance measure (cf. No. 2.1.3.1) in writing

to set. In addition, technical and organizational measures are to be taken

(§ 9 BDSG) to ensure the security of the data. Before the

Commissioning of video surveillance is a prior check according to § 4d

Paragraph 5 BDSG required if the use of video technology from

special risks for the rights and freedoms of those affected

is. According to the explanatory memorandum to the law, there are special risks if

Surveillance cameras "used in larger numbers and centrally controlled

be" (Bundestag printed paper 14/5793, p. 62).

The company data protection officer has according to § 4d paragraph 6 BDSG

carry out the prior check and the result as well as the justification

to be documented in writing. Regardless of the implementation of a

Prior control results in the requirement of the prior purpose

from § 6b Paragraph 1 No. 3 BDSG, if the video surveillance for perception

of legitimate interests. In addition, for procedures that

process data automatically, create a process overview (cf.

234

materials

§ 4g paragraph 2 and 2a BDSG). In any case, video surveillance is

if it is done using digital technology, as automated processing

to qualify. What information is included in this overview

§ 4e sentence 1 BDSG lists them bindingly and conclusively. That one

required general description of the technical and organizational

Measures to protect data are taken with video surveillance

special importance. The video image data are subject to due to the out

improper handling may be for the person concerned

resulting impairments according to high protection controls both

in terms of entry, entry and access, but also disclosure

to law enforcement authorities in the event of a crime. In the process overview are

in addition to naming the persons authorized to access it.

The process overview is to be drawn up by the responsible body and

to be made available to the company data protection officer. This

must contain the contents of the overview of procedures apart from the information on the

range of data security management available to anyone upon request

make. This publicly available paper is called a procedural or

also "Anyone's Directory".

If there is no obligation to appoint an operational data protection officer

the head of the non-public body has the duty to

the fulfillment of these tasks of the company data protection officer

secure in another way.

2.2.2

Obligation to notify

According to § 6b paragraph 2 BDSG the circumstance of the observation and the

to make the responsible body recognizable through appropriate measures. The

Notice can be given with the help of appropriate signs or graphic symbols

(e.g. pictogram according to DIN 33450). He's like this (about eye level)

attach that the person concerned before entering the monitored area

can recognize the circumstance of the observation. The person concerned must

be able to estimate what area is being captured by a camera so it can be in

being put in a position to evade surveillance if necessary, or

adjust his behavior. In addition, for data processing

The responsible body must be recognizable, i.e. who exactly has the video data

collects, processes or uses. It is crucial that the person concerned

NEN it is easy to determine who he is contacting regarding the protection of his

Rights may apply if necessary. Therefore, the responsible body is fundamental

with their contact details explicitly on the information sign.

2.3

Implementation of a permissible video surveillance

2.3.1

storage duration

According to § 6b paragraph 5 BDSG the data of the video surveillance are

to be deleted immediately if they are no longer required to achieve the purpose

are relevant or interests of the data subjects that are worthy of protection

prevent storage. That is the case when a danger does not continue

must be averted or the preservation of evidence is not necessary.

For example, there is no robbery or theft at a gas station

come, video recordings for evidence purposes are no longer

required and must therefore be deleted. Whether it is necessary to back up the material

manoeuvrable, should in principle be clarified within one to two days

can be.2

This means that video recordings generally end after 48 hours

are to be deleted. In justified individual cases, a longer storage

be accepted within a limited period of time, such as when it is on weekends and public holidays

no business operations take place. Since the legal storage period on

Orientated to the purpose of recording, the time of the obligation to delete may vary

vary from case to case. The deletion bid is most effective through a

automated periodic deletion, e.g. B. by self-overwriting

past recordings, corresponded.

2.3.2

obligation to inform

If the camera recordings are assigned to a specific person,

to inform this person about it (§ 6b paragraph 4 BDSG). purpose of this

Regulation is to create transparency and the identified person

Verification of the lawfulness of data processing and prosecution

enable their rights. In terms of content, the obligation to inform is transferred

the notification obligation. A notice has about the nature of the data,

the purpose of the collection, processing or use and the

identity of the processing body. The need for one

Notification only exists when an actual assignment is made; alone the

The possibility to do so does not yet require a notification. The

Notification must be given upon initial assignment.

236

materials

2.3.3

sound recordings

For such monitoring measures is in the penal code (StGB) with

§ 201 (breach of confidentiality of the word) contain a regulation,

which forbids, under threat of punishment, the word not spoken in public

record or listen. So if a video surveillance camera

has an audio function, it must be irreversibly deactivated.

2.3.4

Checking the legality requirements

The operator of a video surveillance system is obliged to comply with the legal

Conditions for operation to be checked at regular intervals.

In particular, the question of the suitability and necessity of the measures

me is to be evaluated. For example, after one year, in

which the camera was in operation, no facts (anymore) establish which ones

justify the assumption that the monitored object is endangered, or

If the purpose intended by the monitoring has not been achieved, the

Video surveillance will no longer be operated. This can also be partial

range of a surveillance concern. The result of the check should

be documented in writing.

3.

Special case constellations

3.1

webcams

Webcams make it possible to post live recordings on the Internet and

to make it accessible to an indefinite number of people worldwide

chen. The problem here is that violations of personal rights

of a live broadcast cannot be undone. For

people who happen to be captured by the camera are therefore at great risk

this through the increasing quality and the simple possibility of the technical

Duplication and processing of the recordings is increased. the one

The use of a webcam is only harmless in terms of data protection if

on the recorded images - for example due to the camera positioning,

lack of zoom options or low resolution - people or

License plates cannot be recognized.

3.2

Video surveillance in gastronomy

The video surveillance of the guest room of a restaurant3 is according to § 6b BDSG

generally 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

so that video cameras are not allowed to be used for surveillance.4

The behavior attributable to the leisure sector as a guest in a restaurant

goes with a particularly high need for protection of personal rights

of those affected. Video surveillance disturbs the unimpaired

Communication and the unobserved stay of the restaurant visitors

and thus has a particularly strong impact on the guest's personal rights

a. The legitimate interest of the visitor normally prevails

the legitimate interest of the gastronomy owner in monitoring,

which is why his interest only prevails in exceptional cases

can. The same applies to café and gastro areas in bakeries, petrol stations,

hotels etc

4.

Video surveillance of employees

Particularly high demands on the necessity of monitoring

according to § 6b BDSG apply if in publicly accessible rooms with

public traffic at the same time workplaces are monitored, for example

in retail outlets. In such cases, not only the person

affected, but there is also one

Supervision of the employees working there. For such areas where

the probability of criminal offenses to a business-typical risk

belongs and the recording of the employees is only a side effect of the

permissible surveillance of public traffic, predominates in some

In individual cases, the legitimate interest of the employer in preventing criminal offenses.

Nevertheless, when installing video surveillance, setting up

so-called private zones, i. H. the permanent hiding of areas in which

employees staying longer is required. The fewer opportunities to retreat

facilities available to employees in non-monitored areas

stand, the more their interests worthy of protection will prevail. the rising,

Processing or use of employees' personal data

through a video system, section 32 subsection 1 sentence 1

BDSG are supported. Open surveillance measures are conceivable

thereafter, however, in particular to fulfill the employer's duty to protect

towards the employees, if a video surveillance in particular

materials

hazardous work areas is required. However, in this

connection of the detection area to the safety-relevant area

to restrict and hide the employee as much as possible. One

Monitoring for the sole purpose of ensuring proper service flow

to ensure is not justified.

In order to detect criminal offences, personal data may

Employees according to § 32 paragraph 1 sentence 2 BDSG only collected, processed

be processed or used if actual to be documented in advance

indications justify the suspicion that the person concerned

has committed a criminal offense involving the collection, processing or

Use is necessary for detection and the legitimate interest of the

Employees to the exclusion of collection, processing or use

does not predominate, in particular the type and extent with regard to the occasion

are not disproportionate.

Video surveillance that takes place in rooms that are not accessible to the public

finds and is not related to the employment relationship,

is to be measured against the requirements of Section 28 Paragraph 1 Sentence 1 No. 2 BDSG

senior The use of video technology must be used to protect legitimate interests

sen of the employer may be required and legitimate interests of the

employees must not predominate. So can exceptionally

property interests of the employer justify video surveillance

gen if the employee is not the focus of the surveillance and not

is permanently recorded, e.g. B. the night security guard who the purpose

the prevention and investigation of theft video-monitored warehouse

checked rooms in which valuable goods are kept. But here too

it must be checked beforehand whether less drastic means are possible.

For the assessment of the admissibility of such a measure is supplementary

based on the case law of the Federal Labor Court5.

In a few exceptional cases, employees can then be monitored

using cameras permitted by the employer if they are open

takes place, so the employees know that their workplace is under video surveillance

becomes. The decisive factor is whether the employer has a legitimate interest in the

Camera recordings may be due to theft or vandalism

prevent staff. However, if he has one, this does not entitle him

easily for monitoring. Rather, his interest with the

legitimate interests of the employee, not in his personality

right to be hurt, to be weighed. Personal rights protect

the employees from a complete surveillance at the workplace

Video recordings that expose him to constant surveillance pressure,

from which he cannot escape. That is why the employee

interest in being spared such continuous surveillance,

if the employer with the monitoring only feared misconduct

wants to take preventive action against its employees, without having to do this in concrete terms

clues exist. In the consideration, it is also weighted whether the

employees at all a control-free and thus unobserved working

area remains. To control work performance, diligence and efficiency

Cameras are not allowed under any circumstances. Sensitive areas such as changing rooms,

sanitary facilities or break and lounge rooms are also

exempt from surveillance. A secret video surveillance is

only permissible in absolute exceptional cases, if less drastic

means of clarifying the suspicion have been exhausted, video surveillance

investigation is practically the only remaining possibility for enlightenment or for

Prevention of the grievance represents and in particular with regard to the

damage caused or to be prevented is not disproportionate.

Cannot collect and process data in the employment relationship

are based on a legal basis, the video surveillance is due

§ 4 paragraph 1 BDSG (ban with reservation of permission) inadmissible. Any

Consent obtained from the employee by the employer is irrelevant because

it in the employment relationship usually depends on the voluntary requirement

4a paragraph 1 sentence 1 BDSG is missing.

As far as the video surveillance complies with the legal requirements,

them through a company agreement that conforms to data protection law

be managed. The methods of collection, processing or use

personal data should be described in more detail. This includes

in particular:

– Object of data collection, processing or use

– earmarking

– Data avoidance and data economy

– Type and scope of the data collected, processed or used

– Recipients of the data

- Rights of the persons affected

– Deletion periods

– technical and organizational measures such as this

authorization concept

If a works council does not exist, the employer should

Create service instructions.

Approved procedures for video surveillance usually enable a

Assessment of the personality of the employees concerned including

240

materials

their abilities, their performance and their behavior. Therefore, according to § 4d

Paragraph 5 sentence 2 no. 2 BDSG to regularly carry out a preliminary check

(cf. no. 2.2.1 above).

5.

Other video surveillance by non-public bodies, in particular

Video surveillance by neighbors or landlords

When assessing the admissibility of video cameras installed on or in residential

attached to houses is based on the detection range of the cameras

to distinguish. The video surveillance of your own, used alone

property is permitted. However, it should be emphasized that the observation

authority of the owner of house rights in principle at the property boundaries

ends. Anyone who, in addition to their property, also has public space such as streets,

Walkways or parking lots are monitored, cannot rely on his domiciliary rights

based, as this right extends only to private land.

Legitimate interests, such as the protection of property, stand

in these cases behind the legitimate interests of the persons who

the detection area of the camera, such as neighbors, passers-by and

other road users, usually back. Those for monitoring and

Video surveillance used to protect your own property

ing technology must not result in the fact that – more or less incidentally –

also adjacent public paths and the people staying there

be monitored.

Provided the video surveillance on the property of the neighbor

extends without affecting a publicly accessible area

the applicability of the Federal Data Protection Act mostly therefore

no, because it is a personal or family activity in the sense

ne of § 1 Paragraph 2 No. 3 BDSG, which is subject to the scope of the

Federal Data Protection Act is excluded. This has the consequence that

the system is not subject to the control of the data protection supervisory authorities

lies. Video-monitored neighbors are, however, independent of this

civil law injunctive relief and defense claims. This

would have to go to civil court, if necessary, with the involvement of a

be asserted by a lawyer. In addition, observing

third-party property with a video system has criminal consequences

have, if so the most personal area of life of the observed

person is injured (cf. Section 201a of the Criminal Code).

For video surveillance in the interior of an apartment building

These are usually rooms that are not open to the public, which is why

the admissibility is not based on § 6b BDSG (cf. above no. 2.1.2). In

In these cases, § 28 BDSG applies, according to which similar requirements for a

Video surveillance applies as in the cases of § 6b BDSG. Besides that

in these cases there is also the possibility of dealing with civil law

claims for remission and defense against any interference with the

to act on personal rights. Thus, permanent monitoring in the

Interior of an apartment building, for example in stairwells,

in the elevator lobby or in the elevator itself, a serious intervention in

the general right of personality of those affected.

past civil law jurisprudence6 there is agreement that

an all-round surveillance of social life does not thereby justify

can be made that the landlord with the monitoring graffiti,

want to prevent contamination or one-time vandalism. In the

As a rule, therefore, the interests of the tenants and tenants, which are worthy of protection, prevail

visitors as victims.

6.

Checklist for the operator of video surveillance public

accessible spaces

Are you planning to install video cameras or do you already have one in place?

video surveillance system? You should ask the following questions for an allowable

surveillance measure can answer:

1. Which areas should be monitored?

– publicly accessible space (e.g. customer areas),

– staff rooms,

– public areas (e.g. sidewalks)

2. Serves video surveillance of

– observance of domiciliary rights or

– Safeguarding another legitimate

If yes, which one?

interest (purpose)?

– Is there a risk situation and what facts, e.g. B.

events in the past, is this based?

3. Has the purpose of video surveillance been established in writing?

4. Why is video surveillance suitable for the stated purpose

to reach?

5. Why is video surveillance necessary and why is it not available

milder means, which are less for the personal rights of those affected

are incisive?

242

materials

6. What legitimate interests of those affected do you have with which

chem result included in the weighing of interests?

Is an observation of the images on a monitor without recording

of the image data sufficient?

7.

If no, why not?

8. If recorded, when will the recordings be deleted? If

the deletion does not take place within 48 hours, please explain

later deletion.

9. At what times is the video surveillance carried out and who keeps

in the monitored area at this time?

10. If there's 24/7 video surveillance, why stop

You need them or why can't they be time restricted

become, e.g. E.g. after business hours or the night hours?

11. Are certain areas of surveillance hidden or

pixelated?

If no, why not?

12. What options does the video camera have and which of these

are not required for monitoring and may need to be deactivated?

– in terms of alignment, e.g. B. swiveling or variable, dome

camera

– in terms of functionality, e.g. B. zoom lenses, wireless cameras,

audio function

13. Has it been checked whether prior checking is necessary and, if so, has it been done?

carried out by the company data protection officer?

If not, why is prior checking not required?

14. Is the video surveillance pointed out in such a way that the person concerned

before entering the monitored area, the circumstance of the observation

can recognize?

15. Is the responsible body named in the notice?

16. Under what conditions is access to the recordings

taken?

By whom?

Were the persons authorized to access the data confidentiality

Is the logging of the inspection ensured?

obligated?

17. Have the technical and organizational measures to protect the

Data according to § 9 BDSG (and the annex to it) taken?

18. Does the company have a works council and has it become one?

Works agreement reached on video surveillance?

As a precaution, we would like to point out that dealing with these

Do not automatically ask about the admissibility of the video surveillance measures

me leads.

If you have specific questions about the operation of a video surveillance system,

you are welcome to contact the data protection supervisory authority responsible for you

listen. The seat of the operator is decisive. One

For example, you can get an overview of the contact details at http://

www.baden-wuerttemberg.datenschutz.de/die-aufsichtsbehorden-der-lander/.

1 LG Bonn, judgment of November 16, 2004-8 S 139/04; AG Lichtenberg, decision of 01/24/2008 –

10C156/07.

2 See the explanatory memorandum to the law, Bundestag printed paper 14/5793, p.

3 This refers to the restaurant within the meaning of the Restaurant Act (GastG), i. H. a business,

in which drinks and/or food are served for consumption on the spot and

which is accessible to everyone or certain groups of people (cf. § 1 GastG). among the

The concept of restaurants therefore also includes cafés, snack bars, fast food restaurants, etc.

4 Cf. AG Hamburg, judgment of April 22, 2008 – 4 C 134/08.

5 Cf. BAG, judgment of March 27, 2003 – 2 AZR 51/02; Resolution of June 29th, 2004 – 1 ABR 21/03;

Resolution of December 14, 2004 – 1 ABR 34/03; Resolution of August 26th, 2008 – 1 ABR 16/07; Verdict

from 06/21/2012 – 2 AZR 153/11.

6 See, for example, LG Berlin, judgment of May 23, 2005 – 62 S 37/05; KG Berlin, decision of

08/04/2008 – 8 U 83/08; AG Munich, judgment of October 16, 2009 – 423 C 34037/08

3.2

Guidance from the supervisory authorities on the processing of

personal data for direct marketing purposes

Validity of the General Data Protection Regulation (GDPR)

materials

balancing of interests

1.3.1 Practical cases balancing of interests

1.4.1 Using Existing Customer Email Addresses

1.4.2 Use of Telephone Numbers

Table of Contents

1.

General Data Protection Regulation (GDPR) and direct mail

1.1

Term of advertising within the meaning of the GDPR

Advertising or direct advertising within the meaning of the DS-GVO is on the one hand that of

companies, the self-employed, associations and clubs, etc

Commercial advertising to build and promote a business

drove. "Advertising" is defined in Art. 2 lit. a of the EU Directive 2006/114/EG

on Misleading and Comparative Advertising of 12/12/2006 defined as

"every expression in the exercise of a trade, trade, craft

or freelance with the aim of selling goods or providing services

of services, including immovable property, rights and

obligations to promote”.

The courts also lay down this far-reaching view of advertising

in their decisions and see e.g. B. thus also satisfaction

asking customers about a business deal, birthday and

Christmas mailings etc. as advertising.

On the other hand, advertising or direct mail within the meaning of the GDPR, but

also contact by parties, associations and clubs or ca-

ritative and social organizations with people concerned to achieve their goals

publicize or promote (see for the promotion of political

parties e.g. B. BVerfG decision of 01.08.2002, 2 BvR 2135/01).

1.2

There are no detailed regulations on this in the GDPR

With the GDPR, all detailed regulations of the previous Federal

data protection law (BDSG) for the processing of personal data

for direct advertising purposes (see in particular Section 28

Para. 3 and 4 as well as § 29 BDSG-old).

246

materials

Basis for assessing the admissibility of processing personal

The data collected for direct marketing purposes is set aside in the GDPR

of the consent of the data subject, a weighing of interests

Article 6 paragraph 1 sentence 1 lit. f GDPR. After that, processing must be carried out for compliance

the legitimate interests of the person responsible, provided that

not outweigh the interests of the data subject. clues for the

The weighing decision to be made is contained in Recital (Recital) 47

DS-GVO, which i.a. states: “The processing of personal data

for direct marketing purposes can be considered a legitimate interest

serving processing are considered.

1.3

balancing of interests

The DS-GVO requires a consideration in the specific individual case both in

With regard to the interests of those responsible or third parties as well as the

affected person. A mere focus on abstract or on comparable

bare cases without considering the individual case satisfies the requirements of

GDPR not.

In this respect, the weighing of interests results in, among other things, from recital 47 that the

reasonable expectations of the person concerned based on their relationship

the person responsible are to be taken into account. That's it too

to turn off the subjective expectations of the person concerned in individual cases.

In addition to these, however, one must also ask what objectively

can and may be. It is therefore also crucial whether the processing

personal data for direct marketing purposes in certain

areas of the social sphere is typically accepted or rejected.

The expectations of the data subject are taken into account when measures are taken to

Direct advertising also through the information according to Art. 13 and 14 DS-GVO

the purposes of data processing. Informs the person responsible

transparently and comprehensively about the intended processing of data

for direct marketing purposes, goes beyond the expectation of the data subjects

usually also to the effect that their customer data is used accordingly

become. However, through transparency, the legal balancing

Fact according to Art. 6 Para. 1 Sentence 1 lit. f GDPR not expanded at will

because the expectations are based on the objective standard of reason.

have to be measured.

The data processing must also be carried out as a whole with regard to the legitimate

interests may be required.

247

47th activity report on data protection

In addition, when weighing up the interests, the general ones that apply anyway

Principles from Art. 5 Para. 1 DS-GVO must be taken into account, i.e. in particular:

– fair process

– appropriate to the processing purpose

- in a way that is comprehensible for the person concerned (in particular

Naming of the source of the data if external data is processed)

1.3.1

Practical cases balancing of interests

Subject to the concrete consideration in the individual case and the supplementary

Statements on points 1.4 and 1.5 can be used for the following rough categories

consideration in practice become relevant:

Interests worthy of protection should not generally prevail if

Subsequent to an order all customers (without selection) by post

Promotional catalog or advertising letter to purchase other products from the

will be sent to those responsible.

If, based on a selection criterion, a classification into advertising

groups and there is no additional knowledge gain from the selection

results, the balancing of interests is usually also in favor of the

responsibility.

More intervention-intensive measures such as automated selection processes

to create detailed profiles, behavioral forecasts or analyzes that

lead to additional insights, on the other hand, suggest that a

Interest of the data subject in the exclusion of data processing

prevails. In these cases, it is profiling that no longer applies

Art. 6 (1) lit. f GDPR can be supported and thus the collection

requires consent prior to data processing. The counter

The right to appeal under Art. 21 GDPR is then not sufficient.

Also the creation of a profile using external data sources

(e.g. information from social networks) for direct marketing purposes

(Advertising scores) will usually result in a predominance of the protectable

interests of the data subject.

Regarding the transmission of data for advertising purposes to third parties as well

the use of third-party addresses, it must be checked whether the interest of the affected

be given a higher priority than the interests of the

Responsible for the transmission as well as the third party for the use of

External addresses for advertising. In this respect, recital Gr. 47 that the expectation

attitude of the person concerned is also determined by whether a relevant

248

materials

and appropriate relationship between the data subject and the

Responsible exists, e.g. B. if this customer is the person responsible.

The specifications of Art. 6 Para. 4 DS-GVO may have to be observed (point 1.5).

1.4

Specific regulations for different contact channels

Regarding the concrete forms of direct advertising, i.e. the contact route to the

affected persons (contact by telephone call, e-mail, fax etc.).

the competition law, § 7 of the law against unfair competition

(UWG), in which cases of unreasonable harassment of the advertised

to go out and advertising of this kind is inadmissible.

Because Art. 6 Para. 1 Sentence 1 lit. f GDPR requires the processing of personal data

Data only declared admissible to the extent that the interests or fundamental rights and

Basic freedoms of the person concerned do not prevail, are also at the

data protection assessment of the processing of personal data

Data for direct marketing purposes the ratings in the protection regulations

of the UWG must be taken into account for the respective form of advertising. If for the

advertisers a specific contact route to a data subject

Person is not allowed after that, the weighing of interests according to Art. 6

Paragraph 1 sentence 1 lit. f GDPR also not in favor of the admissibility of a

Processing of this contact data for direct marketing purposes fails.

1.4.1

Use of the e-mail addresses of existing customers

E-mail addresses directly from the persons concerned under

of a business relationship (existing customers), can

generally used for e-mail advertising if this purpose

E-mail advertising in accordance with Article 13 (1) (c) GDPR for those affected

was transparently explained to persons during data collection. Above-

overriding legitimate interests of the data subject pursuant to Art. 6

Paragraph 1 sentence 1 lit. f GDPR are not given in particular if

the requirements for electronic advertising contained in Section 7 (3) UWG

be respected.

1.4.2

use of telephone numbers

For calls to consumers for direct advertising purposes, the UWG

(§ 7 Para. 2 No. 2) no exception to the consent requirement, so that a

such use of telephone numbers without prior consent because of the

special effects of this form of advertising (more severe annoyance/disruption)

under data protection law in the overriding interests of the company worthy of protection

data subjects pursuant to Art. 6 (1) sentence 1 lit. f GDPR fails.

When advertising with a telephone call to another market part

2 no. 2 UWG

on the fact that his at least presumed consent is assumed

can be generated. In the B2B area, there is therefore a benefit of

Telephone numbers for advertising calls not from the outset in terms of data protection

overriding interests worthy of protection of those to be addressed by telephone

Traders according to Art. 6 Para. 1 Sentence 1 lit. f GDPR.

See the ban on telephone advertising to traders

additionally also BGH, judgment of 16.11.2006, Az. I ZR 191/03, and BGH,

Judgment of September 20th, 2007, Az. I ZR 88/05.

1.5

change of purpose

If personal data is used for advertising purposes,

data that were not (also) originally collected for advertising purposes

are, the regulations of Art. 6 Para. 4 DSGVO (change of purpose) apply

observe. A change of purpose can also occur in cases of transmission to

Third parties for advertising purposes and when using third-party addresses for advertising

Exercise be relevant if the data processing is not in the context

of the purpose of the survey.

In order to find out whether the advertising purpose is compatible with the original

mood is compatible, those responsible must have a so-called compatibility

perform audit.

2.

Information obligations1

2.1

Information on data collection

Personal data are collected directly from the data subject

raised, e.g. B. for purchase and service contracts, prospectus requirements

or competitions, this is comprehensive according to Art. 13 Para. 1 and 2 DS-GVO

etc. to inform about the purposes of the processing of the data. one already

planned or contemplated processing or use of the data

materials

for direct marketing purposes is therefore the person concerned from the start

to be presented transparently.

In the event of a subsequent change in processing, also for the purposes of

Art. 13 Para. 3 DS-GVO requires direct advertising to provide prior information

before. This information is accompanied by a reference to the right to object to advertising

to provide.

Basically, the person responsible at the time of data collection

to inform all topics according to Art. 13 Para. 1 and 2 DS-GVO. However

there is already practically not always the possibility of those affected

Person immediately complete all information from Art. 13 Para. 1 and 2 DS-GVO

to be able to give dig, e.g. B. with order postcards as a magazine insert,

for orders on the phone or for purchase contracts at vending machines. The

Regulators therefore support the Article 29 Group's proposal

(WP 260, p. 17) for a two-stage information model.

From the information requirements according to Art. 13 Para. 1 and 2 DS-GVO

the following basic minimum requirements (decisive

dend is always the need for information in individual cases), which regularly arises

have to be implemented in a first stage:

– Identity of the controller (name including

Contact details)

– Contact details of the company data protection officer (if named)

– Processing purposes and legal basis in keywords

– Indication of the legitimate interest, insofar as the processing is based on it

– Recipients or categories of recipients of personal data

Data

– Transmission to third countries

– Right of objection according to Art. 21 DS-GVO

– Reference to access to further mandatory information in accordance with Article 13

Paragraphs 1 and 2 of the GDPR (such as the right to information, the right to lodge a complaint), e.g. Belly

via QR code or Internet link

2.2

Time of information according to Art. 14 DS-GVO

If personal data of the data subject are to be used for the purposes of

Direct advertising is processed that was not collected by this person himself

were the information requirements according to Art. 14 Para. 1 and 2 DS-GVO

to note.

The law does not require immediate or separate information.

However, the information must be provided within a reasonable period of time, in any case

at the time an advertisement is sent, but no later than within

one month after processing. Does the information take place in

connection with the first advertising mailing, both components (internal

formation and advertising text) to be clearly separated from each other and the information

(including reference to the right to object to advertising) accordingly

to point out clearly.

2.3

Information on the portfolio (“old cases”)

Art. 13 and 14 DS-GVO produce the information requirements from the wording

seen initially on data collection after the GDPR came into effect

("Are personal data ... collected ...").

The Art. 29 group, however, with regard to recital 171 Sentence 2 (“Processing

which have already begun at the time of application of this Ordinance

should have, within two years of the entry into force of this

Regulation be brought into line with it.”) and the principles from

Article 5(1)(a) GDPR on transparency in the development of WP 260

assume that in future contacts with the persons concerned

implement the new information obligations in an appropriate manner or

are to be submitted later (see under No. 2.1, minimum information, reference,

where all the information can be easily obtained).

3.

Consent to the processing of personal data for the purposes of

direct mail

3.1

design of the consent

Consent is a legal requirement for processing

Processing of personal data in accordance with Article 6 Paragraph 1 Clause 1 Letter a GDPR

only effective if they are voluntary and - based on a specific case -

informed. Being informed also requires the type of

intended advertising (letter, e-mail/SMS, telephone, fax), the products or

Services to be advertised and the advertising companies

be called to comply with the transparency requirements of Art. 12

Paragraph 1 and Article 13 Paragraph 1 lit. c DS-GVO as well as the previously issued

to comply with jurisprudence (see e.g. BGH judgment of March 14, 2017,

Az. VI ZR 721/15).

252

materials

According to Art. 4 No. 11 and Art. 7 Para. 2 DS-GVO, an unequivocal

clearly given expression of will in the form of a declaration in a

clear and simple language or any other unequivocal affirmative

Act by which the data subject consents to processing

of the data concerning them.

The GDPR stipulates that consent under data protection law must be in writing

not as a rule. However, according to Art. 5 Para. 2

DS-GVO compliance with the legality requirements of the data

processing and according to Art. 7 Para. 1 DS-GVO also specifically the existence

to prove consent. In order to comply with this obligation

can, it is advisable for those responsible to regularly contact

approval in writing with a handwritten signature or at least

in text form (e.g. e-mail).

There is usually a separate text or section of text for consent

without using any other content. Should it be used together with other

ments (particularly contractual declarations) in writing or in a

be given in electronic format, consent under data protection law is

7 para. 2 sentence 1 DS-GVO in one of the other

to present facts in a clearly distinguishable manner.

3.2

Consent with delivery of business cards

Business cards presented by the persons concerned at trade fairs or other

Events expressly for the purpose of sending information or other

business contact can be left, in principle

represent an effective consent within the meaning of Art. 4 No. 11 DS-GVO,

if, as a result of other circumstances, the person responsible

availability of consent is given.

3.3

Double opt-in procedure for electronic consents

For the electronic declaration of consent is - to verify the

Declaration of intent by the data subject – the double opt-in procedure

offered (depending on the specific type of contact: e-mail or SMS), whereby the

Proof requirements of Art. 5 Para. 2 DS-GVO and the BGH (judgment

dated February 10, 2011, I ZR 164/09) must be taken into account when logging

are. The mere storage of the IP addresses of connection owners and

the assertion that they have given their consent is sufficient

BGH not. Proof of consent requires more, e.g. B. the protocol

ment of the entire opt-in procedure and the content of the consent.

However, such proof is not sufficient in the case of the intended use

phone numbers obtained through website listings for promotional calls

out of. By sending a confirmation e-mail, the post-

knows the identity of the person declaring the consent by e-mail

and the subscriber of the telephone number are not kept. One

written consent to the use of an email address and/or a

Phone number for promotional purposes is regularly the best way for

a later verifiability of a consent.

3.4

"Prohibition of coupling", Art. 7 Para. 4 DS-GVO

The previously existing linking ban for advertising can be found

also in the GDPR again, but is no longer dependent on whether a

other access to equivalent contractual services is possible. At

the assessment of whether the consent was given voluntarily depends on the circumstance

to the greatest possible extent whether, among other things, the

performance of a contract, including the provision of a service,

of consent to the processing of personal data

dependent, which is not necessary for the fulfillment of the contract (Art. 7

Para. 4 GDPR).

3.5

“Expiry” of Consent, Forfeiture

The civil courts see in the case of granted consent to advertising contact

admission partly not unlimited validity. The LG Munich I

with judgment of April 8th, 2010, Az. 17 HK O 138/10, decided that a

Consent to e-mail advertising that was granted 17 months ago and has not yet been used

"loses its topicality" and therefore no legal basis in this respect

is more.

3.6

No advertising use of special data categories without consent

Art. 9 DS-GVO does not contain any permission standard for the processing of special

Categories of personal data for advertising purposes. This is

only with the express consent of the person concerned

254

materials

allowed. This is relevant e.g. B. for companies and professions in

healthcare (pharmacies, medical supply stores, opticians, orthopaedists, etc.).

4.

Special circumstances in the processing of personal data for

Direct Marketing Purposes

4.1

Publication of contact details in telephone directories

Telecommunications service providers must ensure the admissibility of the publication

Publication of telephone numbers and other contact details of connection

holders take into account what the data subject is when concluding the contract

or later requested (no publication, publication only in

printed or in electronic directories). Other directories

Providers must do this when weighing up the interests of Art. 6 Para. 1

Sentence 1 lit. f DS-GVO observe the facts to be assessed.

Any further processing of such contact data in phone numbers

commercial directories would be inadmissible.

4.2

Data collection on the occasion of competitions, catalogues/

prospectus requirements

Processing of postal address data for the purposes of our own direct marketing

Exercise from the implementation of competitions and sweepstakes as well

Due to catalog and prospectus requirements, according to Art. 6 Para. 1

Sentence 1 lit. f DS-GVO permissible if about advertising data processing

was informed; a consent of the persons concerned is with such

circumstances then not required. The requirements from No. 2.1 are

to note.

4.3

No use of the data from the imprint

However, it is not permitted to read out the data from an online

Imprint for the purpose of advertising use. Although these data are

publicly accessible, but they are not voluntarily, but because of

legal obligation to identify providers according to § 5 TMG or

§ 55 paragraph 2 RStV published. In the absence of voluntary publication

regularly carries out the balancing of interests in accordance with Article 6 (1) (f) GDPR

to the fact that the advertising use of data collected in this way is inadmissible. To the

A provider can avoid advertising with this data

a website as a precautionary measure an advertising objection in its imprint

to record.

4.4

Naming of the person responsible for processing the data and the

Source of personal data for third-party address applications

Subject to the admissibility of data transmission to third parties

(Item 1.3 or Item 1.5) must be responsible for the personal data

Responsible, the advertising company and the source of the data

clearly emerge from an advertisement and be clearly visible. A responsible

is more literal than a concrete legal person or company with a summons

address including e-mail address. Abbreviations

(such as XY-Group) or PO box addresses meet the transparency requirements

Amendments to Article 12 Paragraph 1 Clause 1, Article 13 Paragraph 1 Letter a and Article 14 Paragraph 1

lit. a DS-GVO not.

4.5

Contractual information, which at the same time is also promotional information

included (“included advertising”)

If contractors contractual information and related

own or third-party advertising information can also be sent by letter

den, this is possible within the limits of Art. 6 Para. 1 Sentence 1 lit. f GDPR,

as long as the data subject does not object to advertising in accordance with Art. 21

Para. 2 DS-GVO is available.

In the case of e-mail advertising, the assessments of § 7 Para. 3 UWG must be observed,

according to which no simplifications apply to third-party advertising.

4.6

Direct marketing using postal address data obtained from third parties

("Refer a Friend")

A practice, further postal address data for customer and prospect visits

to collect data by interviewing third parties and for direct marketing purposes

to process, the principles of fair and transparent

pensions Processing of personal data in accordance with Article 5 Paragraph 1 Letter a and

Art. 12 para. 1 DS-GVO contrary.

256

materials

4.7

referral advertising

In a judgment of September 12, 2013, I ZR 208/12, the BGH sees unsolicited

sent recommendation emails as unsolicited promotional emails to (a company

take had set up the possibility on its website for users who

Enter a friend's e-mail address in order to send them an unsolicited

so-called recommendation e-mail). It comes for classification

as advertising does not indicate that the sending of the recommendation e-mails

of a company is ultimately based on the will of a third party.

The Federal Court of Justice ruled on January 14th, 2016, Az. I ZR 65/14, that the dispatch of

e-mails generated by Facebook in connection with the registration

procedure "find friends" as unreasonably annoying and therefore illegal

Classified as advertising because these e-mails were sent without prior express consent

be sent with the consent of the addressee.

This makes it clear from the courts that such constructs

Referral advertising the applicable consent requirement in e-mail

Practice according to § 7 Abs. 2 Nr. 3 UWG outside of existing customer relationships

within the meaning of § 7 para. 3 UWG cannot be circumvented.

4.8

Possible useful life of contact data of the data subject for

Direct Marketing Purposes

The question of how long contact data will last cannot be answered unequivocally

the last active business or direct marketing contact with an affected person

person for the advertising purposes of reactivation, recovery, etc.

may still be used, or from when according to Art. 6 Para. 1 Sentence 1 lit. f

DS-GVO overriding interests of the data subject worthy of protection

stand in the way of longer-lasting advertising use.

The legislator has not stipulated a specific deadline.

The decisive factor is whether another one is due to the type of business relationship

Necessity for further use of the data for purposes of direct marketing

exercise can be explained in a comprehensible manner by the person responsible.

If, according to the case law, a granted 17 months ago and so far

unused consent to e-mail advertising "loses its relevance" and

therefore there is no longer any legal basis in this respect (see under 3.5),

This time scale can also be used in the weighing of interests according to Art. 6

Paragraph 1 sentence 1 lit. f GDPR to the reasonable expectations of those affected

Provide guidance to the person when after a long "commercial break" the

Contact details of the person are suddenly processed again for an advertising mailing

become. Also, no overriding legitimate interests of the

data subjects oppose advertising use. So can

e.g. B. the condition query at a funeral home does not

justify the long-term use of data for advertising purposes.

5.

Notes on Art. 21 Para. 2 to 4 GDPR

5.1

Objection to advertising and request for data deletion

In case of doubt, the affected

Clarify the person or clarify with them what they are doing with their declaration of intent
want to effect. Would you like it primarily from an advertising approach
be spared by the company is for the inclusion of their
Contact data in an advertising blocking file at this company is the right one
Means of taking their will into account. When using third-party data
can then be ensured by comparison with the advertising blocking file,
that the contact details of this data subject will not be used.
Such advertising blocking files are therefore prohibited on the basis of Art. 21 Para. 3, Art. 17
Paragraph 3 lit. b and Art. 6 Paragraph 1 Sentence 1 lit. f GDPR to take into account the
Advertising objections from data subjects permissible (for the necessary
Ensuring compliance with the asserted legal claim).
The persons concerned must be in connection with the notification
(Art. 12 Para. 3 DS-GVO) about the observance of your advertising objection
also about the sense and purpose of including your data in a blocking file
be taught.
If a data subject expressly and solely requests a deletion of all
data, they should be advised that they will be used in a future
- legally permissible - use of third-party data may again be advertising
can get.
The advertising objection of a person concerned can, depending on their
Declaration of intent, data protection law against the data owner and/or
address the advertiser as responsible according to Art. 4 No. 7 DS-GVO. At-
de may have to take this advertising objection into account in the future (by
inclusion in an advertising blocking file). With regard to Art. 12 Para. 2 Sentence 1
DS-GVO have those responsible for the effective enforcement of the
the data subject's right to object (e.g.

transfer of the objection).

258

materials

In addition, a reference to the so-called Robin

advertising industry lists can be helpful, see e.g. B. at www.ichhabe-

diewahl.de or www.robinsonliste.de.

5.2

Information about the right to object to advertising

Art. 21 Para. 4 DS-GVO requires that the data subject intelligible

and separate form from other information on their right to object

against the processing of your personal data for the purposes of

Direct marketing, including any related

must be informed of the profiling. For traceability reasons

it is advisable to include the reference to the right of objection with each advertising

to attach the shipment.

Only then is it effective information within the meaning of the law

to assume if a person concerned in the usual handling of the

Advertising or with contract information from the reference to the

right to claim knowledge. The "hiding" of information in long

Terms and conditions or in extensive promotional materials does not constitute a reference within the meaning

of Art. 21 Para. 4 DS-GVO.

Within the meaning of Art. 12 Para. 2 Sentence 1 DS-GVO, the insertion of the advertising

objection to also offer an electronic communication option.

5.3

Implementation period of the advertising objection according to Art. 21 Para. 3 DS-GVO

The implementation of the objection to the future processing of the

Contact details of a data subject for direct marketing purposes

eventually to any related profiling

take place immediately in the company concerned.

If concrete advertising campaigns have started and the contact details of the

affected person are already in the technical processing, it can

be unreasonable for the company in individual cases, temporarily

received objection to advertising with considerable effort

set, e.g. B. a certain already addressed letter from a large

to sort out the crowd.

Here, too, the people affected are largely unaware that

"Started" advertising campaigns are regularly no longer stopped without further ado

can become.

To avoid unnecessary complaints, advertisers should

the persons concerned in an individual reply letter first

on the observance of the advertising contradiction and secondly on the fact

that they remain for as short a period of time as possible, to be named as precisely as possible

may receive advertising.

1 See also the WP 260 of the Art. 29 group at http://ec.europa.eu/newsroom/

article29/news-overview.cfm

3.3

Sample text for manufacturer information on data processing in the vehicle

The independent federal and state data protection authorities have

together with the German Association of the Automotive Industry (VDA).

Sample text for data processing in the vehicle developed:

“Electronic control units are installed in your vehicle. tax

councils process data that they receive from vehicle sensors, for example

received, self-generated or exchanged with each other. Some

Control units are required for the safe functioning of your vehicle

derlich, others support you when driving (driver assistance systems),

others enable convenience or infotainment features.

Below you will find general information on data processing

in the vehicle. Additional information, what specific dates

for what purpose collected, stored and transmitted in your vehicle

are transmitted to third parties can be found under the keyword data protection

in direct connection with the information on the persons concerned

Functional features in the respective operating instructions. These are too

Available online and, depending on equipment, digitally in the vehicle.

personal reference

Each vehicle is marked with a unique chassis number

draws. This vehicle identification number is in Germany

via information from the Federal Motor Transport Authority on the current one

and former owner of the vehicle traceable. There are others too

Ways to transfer data collected from the vehicle to the owner or

driver attributed, e.g. B. on the license plate.

260

materials

The data generated or processed by control units can

therefore be personal or under certain conditions

become personal. Depending on the vehicle data

gene, if necessary, conclusions z. B. on your driving behavior, your

Location or your route or on the usage behavior possible.

Your rights in relation to data protection

You have certain rights under applicable data protection law

to such companies that collect your personal data

process. You will then receive a free and comprehensive

Right to information from the manufacturer and third parties (e.g. commissioned

carried breakdown services or workshops, providers of online services

in the vehicle) to the extent that this personal data is provided by you

have saves. You may request information about which

Your personal data is stored for what purpose and where it comes from

data come from. Your right to information also includes the transmission

of the data to other places.

Learn more about your legal rights against the

Manufacturer (e.g. your right to erasure or rectification of

data) can be found in the applicable data protection information

the manufacturer's website (including contact details of the manufacturer and

his data protection officer) (Footnote 1: Here is a direct link

to the data protection notices on the manufacturer's website).

Data that is only stored locally in the vehicle can be

expert support e.g. B. in a workshop against

have a fee read out.

Legal Requirements for Disclosure of Information

As far as legal regulations exist, manufacturers are fundamentally

Lich obliged to respond to requests from government agencies in the

required extent of data stored by the manufacturer in individual cases

to be released (e.g. when investigating a criminal offence).

Government agencies are also required to do so within the framework of applicable law

authorized to read data from vehicles themselves in individual cases. so can

information from the airbag control unit, for example, in the event of an accident

are read out, which can help to clarify this.

261

47th activity report on data protection

Operating data in the vehicle

Control units process data to operate the vehicle. In addition

include for example:

– Vehicle status information (e.g. speed, movement

deceleration, lateral acceleration, number of wheel revolutions, display

closed seat belts),

– Ambient conditions (e.g. temperature, rain sensor, distance

sensor).

As a rule, this data is volatile and is not passed on to the

stored beyond the operating time and only processed in the vehicle itself.

Control units often contain data memory (including the

vehicle key). These are used to collect information about

Vehicle condition, component stress, maintenance requirements and technical

Document niche events and errors temporarily or permanently

to be able to

Depending on the technical equipment, the following are stored:

– Operating states of system components (e.g. fill levels, tire

pressure, battery status)

– Malfunctions and defects in important system components (e.g. light,

brakes)

– Reactions of the systems in special driving situations (e.g. triggering

an airbag, deployment of the stability control systems)

– Information on vehicle-damaging events

– Estimated state of charge of the high-voltage battery for electric vehicles

Range

In special cases (e.g. when the vehicle detects a malfunction

hat) it may be necessary to store data that is actually only

would be fleeting.

If you require services (e.g. repairs, maintenance work

ten) can, if necessary, use the stored

ten operating data together with the vehicle identification number

be read and used. Employees can read it out

the service network (e.g. workshops, manufacturers) or third parties (e.g. pan-

services) from the vehicle. The same applies to guarantee cases

and quality assurance measures.

Reading is usually carried out via the legally prescribed

a connection for OBD (“on-board diagnosis”) in the vehicle. The

The operating data that has been read document the technical conditions of the

materials

vehicle or individual components, help with fault diagnosis,

compliance with warranty obligations and quality

improvement. This data, in particular information about construction

partial stress, technical events, incorrect operation and others

Errors, together with the vehicle identification number

if necessary, sent to the manufacturer. In addition, subject

the manufacturer of product liability. The manufacturer also uses this for this

Operating data from vehicles, for example for recall campaigns. These dates

can also be used to assert customer claims for

check warranty and guarantee.

Fault memories in the vehicle can be used as part of repair or

Service work or, at your request, by a service company

be reset.

Comfort and infotainment functions

You can make comfort settings and customizations in the vehicle

save and change or reset at any time.

These include, depending on the respective equipment, e.g. e.g.:

– Seat and steering wheel position adjustments

– Suspension and climate control settings

– Customizations such as interior lighting

Within the scope of the selected equipment, you can enter data yourself in info

Bring in the vehicle's tainment functions.

These include, depending on the respective equipment, e.g. e.g.:

– Multimedia data such as music, films or photos for playback in one

integrated multimedia system

– Address book data for use in connection with an integrated

speakerphone or an integrated navigation system

– Entered navigation destinations

– Data on the use of Internet services

This data for comfort and infotainment functions can be stored locally in the

vehicle or they are located on a device that

you have connected to the vehicle (e.g. smartphone, USB stick

or MP3 player). If you have entered data yourself, you can

you can delete them at any time.

A transmission of this data from the vehicle takes place

finally at your request, in particular within the framework of the use of

online services according to the settings you have chosen.

[Smartphone integration e.g. B. Android Auto or Apple car play

If your vehicle is equipped accordingly, you can use your smart

connect phone or another mobile device to the vehicle,

so that you can do this using the controls integrated in the vehicle

can control. The picture and sound of the smartphone can be transmitted via

the multimedia system can be output. At the same time your

Smartphone transmit certain information. These include depending on

Type of integration such as position data, day/night mode and

other general vehicle information. Please inform yourself in

the owner's manual of the vehicle/infotainment system.

The integration enables the use of selected smartphone apps

no, such as B. navigation or music playback. Another interaction

between smartphone and vehicle, in particular active access

on vehicle data, does not take place. The type of further data processing

is determined by the provider of the app used in each case. Whether and

which settings you can make for this depends on the

ligen app and the operating system of your smartphone.]

Online services

If your vehicle has a radio network connection, this is possible

these exchange data between your vehicle and others

systems. The radio network connection is provided by an on-board sensor

de and receiving unit or via a mobile you have brought in

End device (e.g. smartphone) allows. Via this wireless network connection

online functions can be used. This includes online services

and applications/apps provided to you by the manufacturer or by others

providers are provided.

Manufacturer's Services

In the case of the manufacturer's online services, the respective functions are indicated

appropriate place (e.g. operating instructions, manufacturer's website).

described the manufacturer and the associated data protection regulations

given information. To provide online services

personal data are used. The data exchange for this

materials

takes place via a protected connection, e.g. B. with the designated

manufacturer's IT systems. One about providing services

additional collection, processing and use of personal data

Data takes place exclusively on the basis of legal permission, e.g. B.

with a legally required emergency call system, a contractual

Agreement or based on consent.

You can use the services and functions (some of which are subject to a fee) and

in some cases also the entire radio network connection of the vehicle

activate or deactivate. Exceptions to this are by law

mandatory functions and services, such as an emergency call system.

Third Party Services

If you make use of the opportunity, online services of others

providers (third parties), these services are subject to the responsibility

tion as well as the data protection and terms of use of the respective

provider. The manufacturer has access to the content exchanged here

regularly no influence.

Therefore, please inform yourself about the type, scope and purpose of the

Collection and use of personal data within the framework of

Third-party services from the respective service provider.

Berlin, February 2018”

265

266

materials

4. Short Papers

materials

4.1

Short Paper No. 12

Data protection officer at responsible persons and

processors

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the

DSK the General Data Protection Regulation (GDPR) in practice

should be applied. This view is subject to a

future - possibly deviating - interpretation of the European

Data Protection Board.

The following explanations on the data protection officer (DSB) apply

for both controllers and processors.

Appointment of the DPO

An obligation to designate a DPO can result from both the GDPR and

also result from national law. A designation obligation can apply to

the person responsible, for the processor or for both,

depending on who through his activity himself the conditions for this

Duty accomplished. Anyone who previously had to order a DSB usually has to

continue to appoint a DPO.

Appointment of the DPO according to Art. 37 DS-GVO

According to Art. 37 Para. 1 lit. a to c DS-GVO, a DPO must be named in any case.

if one of the following conditions is met:

– Authority or public body (with the exception of courts

act within the framework of their judicial activities)

– Core activity with extensive or systematic monitoring of

persons

– Core activity with extensive processing of particularly sensitive data

(Article 9, 10 GDPR)

"Core activity" is the main activity of a company, which is inseparable from it

characterizes, and not the processing of personal data as a secondary activity

(Recital 97 of the GDPR). The core activities then also include all of them

Operations that are an integral part of the main activity of the person responsible

represent. This does not include those that support the core business

activities such as B. the processing of employee data of their own

Employees.

For the definition of the term "extensive" can be taken from recital 91 of the DS-

GMO the following factors are used:

– Amount of personal data processed (volume)

– Processing at regional, national or supranational level (geo-

graphic aspect)

– Number of persons affected (absolute number or as a percentage of the

relevant reference value)

– Duration of processing (time aspect)

If several factors are high, this can mean “extensive” monitoring

ment or processing.

If patient or client data is processed by a

an individual doctor, other healthcare professional or

Lawyer, it is regularly not a case of the designation

obligatory extensive data processing (see recital 91). Under

Taking into account the circumstances of the individual case and the concrete elements

an extensive processing within the meaning of ErwGr. 91 – for example

in the case of a number of those affected that is significantly greater than the group of those affected

an average, by Rec. 91 sentence 4 privileged individual doctor

goes beyond - there may be extensive processing, so that

a DPO is to be named. Notwithstanding, the naming is general

recommended to comply with data protection regulations

to facilitate and thus, if necessary, regulatory measures

to avoid.

The regulation of Art. 37 Para. 4 S. 1 DS-GVO provides that DSBe also

can be named on a voluntary basis. If there is no obligation to

designation of a DPO is available, a voluntary designation of a DPO

be recommended.

Appointment of the DPO to other responsible persons and

Contract processors according to § 38 BDSG-new

The EU Member States have the option of making the designation mandatory

of a DPO in their national implementing laws to other bodies

stretch (Art. 37 Para. 4 S. 1 DS-GVO). The federal legislature has this

Regulatory leeway used to specify the duty to designate operational

materials

To adjust DSB to the "status quo" existing in Germany (cf. § 4f

BDSG-old and § 38 BDSG-new).

Accordingly, the designation of a DPO is also required in the following cases:

- usually at least ten people are constantly with the

automated processing of personal data employed or

- processing is carried out that is subject to a data protection

assessment according to Art. 35 DS-GVO or

– personal data is processed commercially for the purpose of

Transmission, anonymized transmission or for purposes of

market or opinion research processed;

then must be independent of the number of people engaged in processing

Persons are named a DPO.

Common DPO

A group of companies may appoint a joint DPO (cf.

Art. 37 Para. 2 GDPR). The prerequisite for this is that the data protection officer of each

Branch can be easily reached from. This is also the case

recognized that under German law there is an obligation to appoint a DPO
exists and this DPO outside of Germany for German branches
gene is named. In this context, however, it is recommended that
DSB to settle in the European Union in order to be able to carry out the tasks in
to facilitate reference to the GDPR.
Authorities or public bodies have the option of
authorities or bodies, taking into account their organizational structure and
to appoint a common data protection officer based on their size (Article 37 (3) GDPR).
The reference to organizational structure and size also means that the
Controller must ensure that the common DPO is able
is to carry out the tasks assigned to him in relation to all authorities or
public bodies have been transferred.
Easy access to the DSB
Precautions must be taken to ensure that the persons concerned or
enable other bodies to reach the DPO easily (e.g. facility
a hotline or a contact form on the homepage). The DSB
communication must be possible in the language required for the correc-
Discussion with supervisory authorities and data subjects is necessary.

Professional qualifications and expertise
The DSB is based on his professional qualifications and in particular
his expertise in the field of data protection law and data
protection practice and his ability to carry out the tasks according to Art. 39 DS-GVO
to fulfill, named.
Internal and external DPO

The DPO can be an employee of the company or the authority (in-

internal DPO) or his tasks based on a service contract

(external data protection officer, Art. 37 Para. 6 DS-GVO).

form of naming

Since the GDPR only speaks of naming the DPO, a

Written form - in contrast to § 4f Abs. 1 S. 1 BDSG-old - no longer required

wrote. For reasons of proof with regard to the obligation to provide evidence according to

Art. 24 Para. 1 DS-GVO and Art. 5 Para. 2 DS-GVO and for legal certainty

however, it is advisable to appoint a DPO in an appropriate form

to document. The already before the validity of the DS-GVO and the BDSG-new

against this background, the signed order documents continue to apply. The

Certificate and any additional agreements and tasks contained therein

Assignments should be checked for compatibility with the new regulations

of the GDPR can be checked and adjusted if necessary.

Position of the DPO and obligations of the person responsible or the

processor

The person responsible or the processor must be free from instructions

of the DPO in the fulfillment of his tasks. The DSB may because

not be dismissed or disadvantaged in fulfilling his duties.

The special protection against dismissal and dismissal for DSB according to § 4f

Paragraph 3 sentences 4 to 6 of the old BDSG has been retained in the new BDSG (Section 6 Paragraph 4

i. V. m. § 38 paragraph 2 BDSG-new). The DSB reports directly to the highest

Management level (Article 38 (3) sentence 3 GDPR).

According to Art. 38 DS-GVO, it must be ensured that the data protection officer

is involved in all data protection issues in an appropriate and timely manner. The

DSB must be assisted in fulfilling his duties by giving him

The following is provided:

270

materials

– the resources required for the fulfillment of its tasks (a

finally staff),

– access to personal data and processing operations

as well as

– the resources needed to maintain its expertise.

The DPO is in the fulfillment of his duties to maintain confidentiality

or bound to confidentiality. The BDSG-new additionally regulates for DSB

the obligation to maintain secrecy about the identity of the data subject,

who consults the DPO and the circumstances from which conclusions can be drawn

allow the person concerned. In addition, § 6 para. 6 i. V. m.

§ 38 para. 2 BDSG-new the obligation to maintain secrecy and

Confidentiality on the right to refuse to give evidence.

The person responsible can transfer further tasks to the DPO,

whereby he must ensure that no conflicts of interest arise. This

is to be assumed in particular when holding positions of senior

management are perceived or the fields of activity

definition of purposes and means of data processing.

Tasks of the DSB

According to Art. 39 GDPR, the DPO has the following tasks:

– Informing and advising the person responsible and the employees,

carry out the processing with regard to their data protection obligations

(lit. a)

– Monitoring compliance with data protection regulations and the

tegies of the person responsible for the protection of personal data

including assignment of responsibilities, raising awareness

and training of the employees involved in the processing operations

and the related reviews (lit. b)

– Advice in connection with the data protection impact assessment

according to Art. 35 GDPR and monitoring of their implementation (lit. c)

– Cooperation with the supervisory authority (lit. d) and activity as an

point of contact for the supervisory authority (lit. e)

In addition, the persons concerned are advised on all

processing of your personal data and with the perception of your

Rights under the GDPR related issues (Art. 38

Para. 4 GDPR).

Risk-oriented task fulfillment by the DPO

The DPO takes its tasks according to Art. 39 Para. 2 DS-GVO risk-oriented

true. In fulfilling his tasks, he contributes to the processing

risk involved in the operations, taking into account the nature of the

The scope, circumstances and purposes of the processing are taken into account.

Responsibility for compliance with the GDPR

The DS-GVO expressly clarifies in Art. 24 Para. 1 DS-GVO that it is the

Obligation of the person responsible or the processor - and not the

of the DSB - remains to ensure and prove that the data processing

are in accordance with the provisions of the GDPR. nevertheless

the DPO should adequately document its activities,

in order to be able to prove, if necessary, that he has fulfilled his tasks (in particular

information and advice) has been duly complied with.

Obligations to publish and notify the contact details

of the DSB

The contact details of the DPO are to be published in accordance with Art. 37 (7) GDPR

and notify the supervisory authority. The supervisory authorities will

reporting bodies a form for communicating the contact details

of the DSB.

Legal Consequences in Case of Violation

Violations of the provisions on the DPO from Art. 37 to 39 DS-GVO (e.g.

Non-naming or insufficient support of the DPO) are after

Art. 83 (4) lit. a GDPR threatened with a fine.

Notice

The Article 29 Working Party has to clarify the Art. 37

to 39 DS-GVO now "Guidelines in relation to data protection officers"

(Working Paper 243).

materials

4.2

Short Paper No. 13

Order processing, Art. 28 GDPR

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the

DSK the General Data Protection Regulation (GDPR) in practice

should be applied. This view is subject to a

future – possibly different – interpretation of the European

Data Protection Board.

Processor concept

According to Art. 4 No. 8 DS-GVO, the processor is a body that processes personal related data processed on behalf of the person responsible. The term of the person responsible and subsequently the relevant distinction between controller and processor is not in the DS-GVO completely congruent with the wording of the BDSG-old. Responsible is, according to Art. 4 No. 7 DS-GVO, the body that alone or together with others about the means and purposes of processing personal data data decides. This is where the decision comes in the processing purposes, while the decision on the technical organizational issues of processing also on the processor can be delegated (cf. already WP 169 of the Article 29 group, p. 17 f.). This working document does refer to the legal situation under the EU Data Protection Directive 95/46/EG [DS-RL], the basic However, considerations on these questions are also relevant for the interpretation of the DS-GVO.1

Under the old BDSG, it was often differentiated from order (data) processing the figure of the so-called function transfer is used. When the function transmission became a transmission instead of an order (data) processing personal data to third parties in the course of outsourcing such “Functions”/tasks that go beyond mere data processing go out as such and where the recipient at least certain Decision-making scope for task fulfillment was transferred. The However, the transfer of functions is not provided for in the GDPR. This results from the overall system, in particular from the special

regulated figure of the jointly responsible (Art. 26 DS-GVO) as well as

from the fact that certain decision-making leeway of a representative

- within the framework set by the person responsible - with regard to

lich the means of processing with regard to the technical and organizational

Questions that do not rule out order processing (WP 169, p. 17 f.).

Continued special regulation for processing of

personal data in the order

As before, there is also a special regulation under the GDPR

for processing of personal data on behalf of However

the GDPR will place more responsibility on processors in the future and

more duties.

According to Art. 29 DS-GVO is the service provider working on the basis of an order

bound by instructions. He therefore does not carry out the processing for the client

as third i. s.d. Art. 4 No. 10 GDPR through. Rather, it is between

the controller issuing the order and its processor

an "internal relationship". The processing by the processor is

therefore generally attributed to the person responsible.

It should be noted that the data processing in the order will also not be possible in the future

Permission to disclose data to the processor that is based on

statutory confidentiality obligations or professional or special

Official secrets that are not based on legal regulations are confidential

are to be treated in a legal manner (cf. § 1 Para. 2 S. 3 BDSG-new). With the "Law on

New regulations for the protection of secrets when third parties are involved

the professional exercise of confidential persons" however, various

which amends laws on professional secrecy. So now u. the

in § 203 Abs. 1 or 2 StGB specified professional secrecy for example

external service providers who are involved in their professional or official activities

participate, secrets under the conditions of § 203 paragraph 3 and

4 StGB reveal. In return, the processor is subject to

Section 203 (4) of the Criminal Code is now also sanctioned under criminal law

duty of confidentiality.

For the transfer of personal data to the processor

and the processing by the processor requires it regularly

no other legal basis within the meaning of Art. 6 to 10 DS-GVO as

those on which the controller itself bases the processing.

According to the GDPR, order processing by service providers is also possible.

providers outside the EU/EEA area if the additional requirements

of Art. 44 et seq. GDPR for processing in third countries

(adequate level of protection in the third country, suitable guarantees under Art. 46

GDPR such as B. Standard data protection clauses or exceptions

according to Art. 49 GDPR). Processors are recipients within the meaning of

274

materials

Art. 4 No. 9 GDPR. The property as recipient leads to separate

Information (cf. inter alia Art. 13 Para. 1 lit. e GDPR) and notification obligations

(Art. 19 DS-GVO) of the person responsible as well as to information rights (Art. 15

DS-GVO) of the data subject to the person responsible. recomm.

Data catchers must be included in the record of processing activities (cf.

Art. 30 Para. 1 lit. d GDPR).

Regulations for order processing in Art. 28 DS-GVO

The central provision for processors in the GDPR is Art. 28, where

according to the person responsible according to paragraph 1 before awarding the contract first

an examination of the suitability of the processor is imposed. The

According to this, the person responsible may only use such processors

which offer sufficient guarantees that they have appropriate technical

and organizational measures for adequate data protection

apply, so that the processing takes place in accordance with the GDPR

and ensuring the protection of the rights of data subjects. For the

Evidence of such guarantees may also be approved by the Code of Conduct

Processor according to Art. 40 DS-GVO or certification according to Art. 42

GDPR can be used as factors.

Contract with the processor

As under the previous legal situation, the person responsible must

Processor a contract for the instruction-bound activity

close, which is in writing or in an electronic format

can be. Individual arrangements can be made for this

also by the EU Commission or by the competent supervisory authority

adopted standard contractual clauses are used. for the emergency

The flexible content of the contract is largely the same as before. The

existing contracts can therefore continue to apply if they meet the requirements

correspond to or go beyond the GDPR. For example, must

a contract for order processing a regulation for the provision of the

Data include and compliance with the special conditions for the

regulate the use of subcontractors. Among other things, the contract must

also provide for order processing that the order processor

takes the necessary measures in accordance with Art. 32 DS-GVO. Since the responsible

literally responsible for the lawfulness of the processing as a whole

is and remains (see Art. 24 DS-GVO), it is still advisable that at least

to present the necessary technical and organizational measures.

Subcontracting

If the processor wants to provide the agreed service

service subcontractors as additional processors, see above

this requires prior (written or electronic) approval

by the person responsible (Art. 28 Para. 2 DS-GVO). later intended

Changes to the subcontractors used must be

workers to inform the client in advance as the person responsible, whereby it

reserved for the person responsible, against the planned inclusion

to object to a subcontractor. Can after the appeal

no agreement between the controller and the processor

are achieved, the person responsible has the sub-contracting by instruction

prevent or terminate the order processing.

The contract between the processor and the subcontractor

must contain the same contractual obligations that the order

has taken over in favor of the customer.

New responsibilities and obligations for processors are

in particular:

The overall responsibility for data processing and the obligation to provide proof of

Responsible according to Art. 5 Para. 2 DS-GVO also includes the processing

by the processor. The person responsible cannot get away from this

by commissioning a processor.

If a processor violates the obligation to be bound by instructions

Processing by using the client's data in violation of the regulation for

own purposes or purposes of third parties, it applies according to Art. 28 Para. 10

DS-GVO in this respect as the person responsible - with all the legal consequences,

e.g. B. also the obligation to fulfill the rights of those affected. newly added

Art. 82 GDPR also contains special liability regulations for

data breach processors. So now threaten

Contract processors in the event of violations of the data specified in the DS-GVO

Obligations imposed on processors Claims for damages by

affected persons.

Furthermore, there is a new obligation for processors, also in the future

a list of processing activities according to Art. 30 Para. 2 DS-GVO

for all categories of data carried out on behalf of a person responsible

carry out processing activities. The register must

authority on request according to Art. 30 Para. 4 DS-GVO, e.g. B. for controls, for

Will be provided.

276

materials

According to Art. 33 Para. 2 DS-GVO, a processor must have a violation

of the protection of personal data immediately after becoming known

report to the person responsible.

maintenance and remote access

Is the subject of the contract between the person responsible and the

IT maintenance or remote maintenance (e.g. error analyses, support

Working in the client's systems) and exists within this framework

for the processor the need or possibility of access

on personal data, it is with regard to the broad

Definition of a processing in Art. 4 No. 2 DS-GVO (e.g. reading, query

gene, use) also to a form or part of an order

processing and the requirements of Art. 28 GDPR - such as the

Conclusion of a contract for order processing - must be implemented.

This is different with purely technical maintenance of the IT infrastructure

by service providers (e.g. work on electricity supply, cooling, heating) who

not to a qualification of the service provider as a processor and

an application of Art. 28 DS-GVO.

consequences of violations

Likewise, the comprehensive provisions on fines in Art. 83 Para. 4,

5 and 6 DS-GVO to be taken into account (in the event of violations of the specifications of the

Art. 28 DS-GVO can fines of up to 10,000,000 euros or up to

2% of the total worldwide annual turnover of the previous one

financial year of a company). These sanctions

In the event of violations, not only the responsible persons themselves, but also

meet the processor, e.g. B. in the event of violations by the processor

against his obligations under Art. 28 Para. 2 to 4 DS-GVO.

Attachment:

Appendix A

Order processing can regularly e.g. B. the following services:

– IT work for payroll accounting or the

Financial accounting through computer centers

– Outsourcing of personal data processing within the framework of

Cloud computing without the cloud

operator is required

– Advertising address processing in a letter shop

– Processing of customer data by a call center without significant

own scope for decision-making there

– Outsourcing of e-mail administration or other data services

Websites (e.g. maintenance of contact forms or user inquiries)

– Data acquisition, data conversion or scanning of documents

– Outsourcing of backup security storage and other archival

ments

– Data carrier disposal by service providers

– Testing or maintenance (e.g. remote maintenance, external support)

ated procedures or data processing systems, if these

activities, access to personal data cannot be ruled out

can be

– Centralization of certain “Shared Services” within

of a group, such as business trip planning or travel expense accounting

ments (at least insofar as there is no case of joint responsibility

Art. 26 GDPR exists)

Appendix B

No order processing, but the use of external specialist services

obligations with an independent controller, for the processing

(including transfer) of personal data has a legal basis

according to Art. 6 DS-GVO are, for example, as a rule

the inclusion of one

– Persons subject to professional secrecy (tax consultants, lawyers, external business

doctors, accountants),

– Debt collection agencies with assignment of claims,

– banking institution for money transfer,

– Postal service for the transport of letters

and much more.

Appendix C

Furthermore, there is no order processing if joint controllers

according to Art. 26 DS-GVO, i. H. if several responsible persons

jointly decide on the purposes and means of processing. below

Depending on the design, there may be a number of processing

len were classified under BDSG-old as a so-called functional transfer, for example

278

materials

– clinical drug trials when multiple contributors (e.g. sponsor,

Study centers/doctors) each in sub-areas decisions about the

meet processing,

– joint management of certain categories of data (e.g. “master

data”) for certain parallel business purposes of several con-

company.

1 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/

files/2010/wp169_en.pdf

4.3

Short Paper No. 14

Employee data protection

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the
DSK the General Data Protection Regulation (GDPR) in practice
should be applied. This view is subject to a
future – possibly different – interpretation of the European
Data Protection Board.

Old law = new law?

In § 32 Federal Data Protection Act-old was the employee data protection
specially regulated. There was no comprehensive employee data protection law
however. The GDPR also does not contain any concrete, area-specific
fishing regulations. Rather, the focus is on employee data protection
initially according to the general regulations of the DS-GVO, which apply to each
legal relationship apply. However, Article 88 paragraph 1 DS-GVO contains for
a so-called opening clause for employee data protection. She he-
allows Member States to set specific rules for processing
to enact personal data in the employee context that
correspond to the content requirements of Article 88 paragraph 2 DS-GVO
must. A hitherto higher national level of data protection can therefore be
be maintained in this area. The German legislator has
this opening clause through the enactment of Section 26 of the new Federal Data Protection Act
made use of.

For employees and employees of authorities and public bodies of the
Federal and state governments - including local authorities - apply special

Federal and state-specific regulations (e.g. civil service law
regulations). The regulations of § 26 BDSG (Federal Data Protection Act)

then do not apply.

Content § 26 BDSG-new

I) Data processing for the purpose of the employment relationship

1st principle, § 26 paragraph 1 sentence 1, 1st clause BDSG-new

§ 26 paragraph 1 sentence 1 BDSG-new largely corresponds to the previous one

Regulation of § 32 paragraph 1 sentence 1 BDSG-old. According to both rules

may personal data of employees be used for employment

contractual relationship are processed, insofar as this is necessary for the justification,

Implementation or termination of employment required

is. In this respect there is no difference between the old and the new

legal position.

2. Collective/company agreements, § 26 paragraph 1 sentence 1 and paragraph 4

BDSG-new

In § 26 paragraph 1 sentence 1 and paragraph 4 BDSG-new is now expressly

regulated that the processing of employee data on the basis

of collective agreements is permitted. This includes collective bargaining agreements as well

Company and service agreements (compare recital 155 on

GDPR). The negotiating partners have the substantive specifications of the

Article 88 paragraph 2 GDPR must be observed. Accordingly, are appropriate

and special measures to safeguard human dignity, the

legitimate interests and fundamental rights of the data subject

seize. These requirements ensure that collective agreements do not

lower the level of protection of the GDPR.

Employee data may also be processed to the extent necessary for the rights

and obligations of employee representative bodies

– regardless of whether this relates to a law, collective agreement

tion of a company or service agreement (§ 26 Paragraph 1

Clause 1 clause 2 BDSG-new).

280

materials

II) Consent

In the employment relationship comes a voluntary and therefore effective

Consent based on the existing superior/subordinate relationship

regularly not considered. However, knew neither the BDSG-old nor

Do the BDSG-new or the DS-GVO know a basic

the exclusion of consent in the employee context. The specific

Regulation of § 26 paragraph 2 BDSG-new now contains restrictive ones

Regulations on the question of the voluntariness of consent. employees can

You then voluntarily consent to data processing if for

the employees gain a legal or economic advantage.

The same applies if the employer and employees have the same interests

pursue.1 With regard to these legal rule presumptions are due

However, the super-/subordination relationship places high demands on the

To provide the purpose of the consent, if processing is required in individual cases

to be supported by employee data.

In practice, consent is therefore mainly given in constellations

be possible, which is not the employment relationship as such, but additional

relate to benefits provided by the employer (e.g. when permitting

private use of company vehicles, telephones and IT equipment; introduction

a company health management for health promotion;

inclusion in birthday lists).

The written form is generally required for consent in order to

informational self-determination of the employees concerned

chern. At the same time, this means that the employer's obligation to provide evidence is taken into account

of Article 7 Paragraph 1 DS-GVO. In addition, there is the obligation of

Employer for clarification in text form about the purpose of data processing

tion and the possibility of revocation at any time by the employees as well as the

associated consequences according to Article 7 Paragraph 3 DS-GVO.

III) To detect criminal offenses

Section 32, paragraph 1, sentence 2 of the old BDSG was adopted as Section 26, paragraph 1, sentence 2

BDSG-new. According to this, data for the detection of criminal offenses may be processed

if there are factual indications to be documented that

the person concerned has committed a criminal offense in the employment relationship.

The processing must be necessary for detection and the protection-worthy

ge interest of the employee in the exclusion of processing

must not predominate. In particular, the type and extent with regard to

not be disproportionate to the occasion. This corresponds to § 26 paragraph 1

Sentence 2 BDSG-new of the previous legal situation.

281

47th activity report on data protection

The processing may only take place after the indications are available.

Precautionary processing "in advance" is therefore not permitted. Employer

are therefore not allowed to collect data in the event that a criminal offense is later committed in the

employment relationship could be committed. In addition, they have to

Take action against specific suspected employees, not against

larger groups of workers.

IV) Special categories of personal data

The processing of special categories of personal data

same Article 9 Paragraph 1 DS-GVO) is in the employee context under the
Prerequisites of § 26 Paragraph 3 Clause 1 BDSG-new possible. According to § 26
Paragraph 3 sentence 2 BDSG-new can also be an effective consent
Article 9 paragraph 2 letter a DS-GVO in connection with § 26 paragraph 2
BDSG-neu extend to these types of data, provided that the consent
expressly referred to this data. According to § 26 paragraph 4 BDSG-new
Collective agreements can also form legal bases for processing
represent special categories of personal data. Have along
the negotiating partners the substantive requirements of Article 88 paragraph 2
GDPR to be observed. A reference to Article 5 GDPR (processing
principles) contains § 26 paragraph 5 BDSG-new. This is particularly
emphasized that when processing employee data, appropriate
measures are to be taken. The explanatory memorandum explains
that in this way at the same time the requirements of Article 10 DS-GVO
(Processing of personal data relating to criminal offenses)
should be gene.

V) Processing outside of file systems

According to § 26 paragraph 7 BDSG-new, the entire § 26 also applies to such data,
that are not and should not be stored in a file system. With that is
the substantive scope of application of the GDPR has been expanded by the legislature
been. On the existence of at least a structured collection
of data (file system) within the meaning of Article 4 No. 6 DS-GVO
therefore not on. All forms of processing will therefore continue to be subject in the future
of personal data in the employment relationship - paper-based
dene as well as oral forms, but also purely actual actions -
the data protection regulations (compare, for example, judgment

of the Federal Labor Court of June 20, 2013, file number 2 AZR 546/12). This can for

Example, be handwritten notes by the employer about employees.

282

materials

VI) Definition of “employees”

The definition of the term “employees” in § 26 Paragraph 8 BDSG-new

basically speaks of the previous one. was explicitly included

clarifying that the employee status of agency workers also

in relation to the borrower - i.e. not only to the lender.

Applicability GDPR otherwise

I) General

The range of § 26 BDSG-new and thus the remaining applicability

the DS-GVO in the employee context must be checked in each individual case.

This is also related to the meaning and purpose of Article 88 GDPR

with § 26 BDSG-new to be considered.

II) Change of purpose

In the employee context - from individual cases on the basis of a voluntary

Apart from consent - the collection and (further) processing of

Data mainly according to § 26 BDSG-new, i.e. on a special basis

legal basis. In addition, the processing takes place within the framework of a

superior/subordinate relationship. Both the evaluation of the criteria of

Article 6 paragraph 4 DS-GVO as well as the balancing of interests according to Article 6

Paragraph 1 letter f DS-GVO is therefore basically the result

must come that also for new uses still an inner

connection to the employment relationship in the broadest sense

must. A use for completely different purposes (e.g.

purchase to third parties for advertising purposes) will therefore be excluded; a

such purpose is incompatible with the original one respectively

in such constellations, interests, fundamental rights and

fundamental freedoms of those affected. Incidentally, in this regard

also § 24 BDSG-new ("Processing for other purposes by non-public

relevant bodies").

III) Legal Consequences in Case of Violation

A violation of the obligations of § 26 BDSG-new is according to Article 83

Paragraph 5 letter d DS-GVO with a fine of up to 20

million euros (or 4% of global annual sales)

sanctioned. Section 42 of the new BDSG contains criminal regulations.

283

47th activity report on data protection

outlook

The legislature has reserved the right to issue more specific regulations on employment

to enact mandatory data protection. Such an employee data protection law

could include the right to ask questions when recruiting female applicants

and applicants, the limits of permissible checks on employees who

Limitation of localization (GPS) and the use of biometric

have authentication and authorization systems as their subject.

1 In the area of public bodies, the consent in the service and employment relationship is the same

only be considered under narrow conditions, especially if a

Consent-based data processing is explicitly provided for in the State Civil Service Act.

4.4

Short Paper No. 15

Video surveillance according to the General Data Protection Regulation

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the

DSK the General Data Protection Regulation (GDPR) in practice

should be applied. This view is subject to a

future – possibly different – interpretation of the European

Data Protection Board.

Video surveillance will continue after May 25, 2018 for both the

supervisory authorities as well as for the operators of corresponding systems

Topic with considerable practical relevance remain: the GDPR itself

does not contain any specific regulation on video surveillance. Thus is not

clear to what extent the previous data protection assessments

can be maintained in practice. The one from May 25, 2018 as well

§ 4 of the Federal Data Protection Act (BDSG-new, cf. Art. 1

DSAnpUG-EU) contains a regulation on video surveillance in public

accessible spaces. Whether and to what extent this regulation is due

of the application priority of the GDPR can be applied remains

subject to a decision in each concrete individual case.

materials

Which regulations of the DS-GVO are for video surveillance

relevant?

For examining the legality of (data) processing by non-

public bodies is initially on the "general clause" in Art. 6 para. 1 sentence 1

lit. f GDPR. Thereafter, the processing is lawful to the extent

they 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. With Art. 2 Para. 2 lit. c

DS-GVO the previous so-called household privilege will continue to exist. The Ordinance

therefore does not apply to the processing of personal data,

by a natural person to exercise exclusively personal

or family activities and therefore not related to a professional or

economic activity is carried out (Recital [Recital] 18).

In certain cases, Article 6 (1) sentence 1 lit. e,

Para. 3 DS-GVO in connection with a national law as a legal

basis to be considered.

Should video surveillance be based on consent within the meaning of Art. 7 DS-

However, the requirements of this provision should be supported by GMOs

only be fulfilled in rare individual cases. In particular, entering the

marked detection area of a video camera as "clear

confirmatory action" and also not as informed consent i. s.d.

Art. 4 No. 11 GDPR.

A processing of biometric data (Art. 4 No. 14 DS-GVO) to clearly

9 Para. 1 DS-GVO

generally prohibited. Even the mere suitability of video recordings for

a biometric analysis is involved in risk assessment and selection

of the technical and organizational measures must be taken into account.

Insofar as biometric data is used in video surveillance for the purpose of

unique identification or authentication of a natural person

processed (e.g. with face recognition software) apply to

such processing the narrow exceptional circumstances of Art. 9 Para. 2

GDPR. Detailed information on this can be found in Short Paper No. 19 “Special

Categories of personal data”.

Which content-related requirements will arise in the future for a

video surveillance system?

The test to be carried out in accordance with Article 6 Paragraph 1 S. 1 lit. f GDPR follows in

Essentially the criteria already known from the BDSG:

– Protection of legitimate interests

– Necessity

– balancing of interests

With regard to the factual element of "legitimate interest".

the previous casuistry can continue to be followed. New is from German

View, however, the consideration of the so-called "third party interest". As a "third party"

according to Art. 4 No. 10 DS-GVO both private and legal

persons under consideration. For example, one could think of the typical

Constellation in shopping centers where the landlord has video surveillance

also in the interest of his (shop) tenants, who in a large number of cases do not

are themselves affected, operates.

As part of the necessity test, it is still necessary to ask whether the

specific video surveillance is suitable for achieving the purpose and whether al-

ternative measures that are not or less deeply rooted in the right to protection

intervene in personal data are preferable in specific individual cases.

When weighing up the interests, Rec.Gr. 47 a relativization

of the hitherto strictly objective approach, since the "ver-

reasonable expectations of the person concerned, based on their relationship

based on the person responsible are to be taken into account". So that's first

on the subjective expectations of the person concerned in the individual case

deliver. In addition to these, however, one must also ask what an objective third party is

can and should reasonably expect. It will therefore also be decisive

be whether video surveillance in certain areas of the social sphere

typically accepted or rejected.

In the employment relationship in particular, a stricter standard will be applied

be as if the person concerned as a customer, guest or passer-by of a

deodorant monitoring is recorded. In general not expected and in this

Therefore, video surveillance, e.g. B. in

neighborhood context as well as in individual areas such as living, sports

exercise/fitness or medical treatment and waiting rooms. without exception

Video surveillance in sanitary and sauna areas is not accepted.

This makes the test significantly more complex.

The DS-GVO requires a consideration in the specific individual case both in

With regard to the interests of those responsible or third parties as well as the

concerned. A mere reference to abstract or comparable cases

286

materials

Without consideration of the individual case, the requirements of the DS-GVO are met

therefore not.

Transparency requirements and information signage

In addition to the lawfulness of the processing, the GDPR requires Art. 5

Paragraph 1 lit. a further that the personal data in a for the

data subject must be processed in a comprehensible manner.

With this regulation as well as the resulting from Art. 12 ff. DS-GVO

requirements, the transparency obligations have increased significantly. From the

Information obligations according to Art. 13 Para. 1 and 2 DS-GVO arise as follows

minimum requirements:

– Circumstance of observation – pictogram, camera icon

- Identity of the person responsible for video surveillance - Name incl.

Contact details (Art. 13 Para. 1 lit. a GDPR)

- Contact details of the company data protection officer - if named,

but then mandatory (Art. 13 Para. 1 lit. b DS-GVO)

– Processing purposes and legal basis in keywords (Art. 13

Paragraph 1 lit. c GDPR)

- Statement of legitimate interest - insofar as the processing is based on Art. 6

Paragraph 1 sentence 1 lit. f GDPR is based (Art. 13 Paragraph 1 lit. d GDPR)

– Duration of storage (Art. 13 Para. 2 lit. a GDPR)

– Reference to access to further mandatory information in accordance with Article 13

Paragraphs 1 and 2 of the GDPR (such as the right to information, the right to lodge a complaint,

catcher of the data)

The other mandatory information is also available at the location of the video surveillance

information at a point accessible to the person concerned or

to be made available, for example as a complete information sheet

(notice).

consequence

A non-transparent video surveillance is not in line with the DS-

GVO (Art. 5, 13 DS-GVO). According to Art. 58 Para. 2

lit. d DS-GVO instruct the person responsible to remedy the defect or

according to Art. 58 Para. 2 lit. f DS-GVO the video surveillance temporarily

or finally limit or prohibit. There is a lack of transparency

in addition, a fine according to Art. 83 Para. 5 DS-GVO.

Storage duration/deletion requirement

The video surveillance data must be deleted immediately if they are

Achievement of the purposes for which they were collected are no longer necessary

are (Art. 17 Para. 1 lit. a DS-GVO) or legitimate interests of the data subject

against further storage. Whether a backup of

Material is necessary should generally be available within one to two days

can be clarified. Taking into account Article 5 Paragraph 1 lit. c and e

DS-GVO - "data minimization" and "storage limitation" - should therefore

in principle, as before, deletion can take place after 48 hours.

Secure and privacy-friendly design

When procuring, installing and operating video surveillance

monitoring systems is based on the secure (Art. 32 DS-GVO) and data protection

friendly (Article 25 GDPR) design. In particular, the

Those responsible check to what extent video surveillance is timed

can be restricted and which areas of surveillance are hidden

or can be pixelated. Even when purchasing the video technology

Pay attention to "built-in data protection". Unneeded functionality

(e.g. free pivoting, comprehensive surveillance via dome camera,

zoom capability, radio transmission, internet publication, audio recording)

should not be supported by the technology procured, or at least at the

commissioning can be deactivated.

Special case: video observation in real time

Real-time video surveillance (direct transmission of image data to a

Monitor without saving the collected data - camera monitor principle)

constitutes fully or partially automated processing of personal data

data and must also be assessed according to the GDPR.

What other formal requirements must be observed?

In the processing directory to be created in accordance with Art. 30 Para. 1 DS-GVO

should the video surveillance be identified and documented, which

the purpose of the processing.

Furthermore, according to Art. 35 DS-GVO, a data protection impact assessment

carry out when the video surveillance poses a high risk to the rights

and freedoms of natural persons. This applies according to Art. 35

Paragraph 3 lit. c GDPR, in particular in the case of a systematic extensive

(Recital 91: wide-ranging) surveillance of publicly accessible areas.

288

materials

On the content of data protection video surveillance according to the basic data protection

ordinance impact assessment is referred to the corresponding brief

No. 5 referenced.

Our recommendation:

The formal and material requirements for using a video

monitoring will be compared to the BDSG when the GDPR comes into force

not be lowered. Rather, they remain high and still complex.

Therefore, operators of video surveillance systems should already

deal intensively with the new legal situation at this point in time and

check whether ongoing video surveillance meets the changed requirements

correspond and can be continued. This applies in particular to the

increased demands on transparency and the design of the

data processing.

In case of doubt, the supervisory authority will help.

4.5

Short Paper No. 16

Joint controllers, Art. 26 GDPR

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the

DSK the General Data Protection Regulation (GDPR) in practice

should be applied. This view is subject to a

future – possibly different – interpretation of the European

Data Protection Board.

concept of joint responsibility

Art. 26 of the GDPR regulates the “joint responsibility for processing

ly". This legal institution was already in the EC data protection directive

(RL 95/46/EG) but not detailed and played there

in Germany so far - if at all - only an extremely small role, since

it was not expressly mentioned in the old BDSG. Therefore, the express

Regulation of joint responsibility in the GDPR, especially for

practice in Germany have a significant impact.

289

47th activity report on data protection

An objective existing joint responsibility are in the future

Obligations are attached, non-compliance with which is sanctioned with a fine

(cf. Art. 83 Para. 4 lit. a).

According to Art. 26 Para. 1, several bodies are “joint for the processing

Controllers” when they share the purposes of and the means of

Specify processing. This definition builds consistently on Art. 4 No. 7,

according to which the person responsible is the body that alone or jointly with

others about the purposes and means of processing personal data

data decides

No “privilege effect” of joint responsibility

Responsibility is not a power to process data. She just makes it clear

who has to fulfill which tasks from the DS-GVO. Art. 26 therefore provides

neither a legal basis for processing by several responsible

literal, nor does it need a legal basis for several

bring together those responsible. As far as the respective person responsible

in the context of joint responsibility personal data

processed, he needs his own legal basis for this processing

according to Art. 6 Para. 1 and, insofar as special categories of personal

Data are processed according to Art. 9 Para. 2.

Joint controllers are also recipients among themselves

of Art. 4 No. 9 and can therefore be subject to information obligations

be. The transmission of personal data under joint responsibility

literal is a separate processing operation within the meaning of Art. 4 No. 2

DS-GVO and as such requires a legal basis. Should a processing

tion by several jointly responsible parties, for example, to consent

according to Art. 6 (1) lit. a GDPR, the consent must be supported

therefore unequivocally the processing by all jointly responsible

literal and therefore also the corresponding transfer to the or the

include other joint controllers. Starts the transmission

another joint controller represents a change of purpose,

must also be checked according to Art. 6 Para. 4 whether the change of purpose

allowed is.

The Institute of Joint Responsibility serves, among other things,

To regulate liability issues in cases where a body together with

at least one other body determining the purposes and means of the

processing (see WP 169 of the Article 29 Group, p. 39). So should ver-

prevented that the individual involved in data processing

relieved of his data protection responsibility and liability,

290

materials

if he is not solely responsible for the purposes and means of processing

decides, but has an actual influence alongside other stakeholders

on the purposes and the essential elements of the means of processing

exercises (see also the Opinion of the Advocate General at the ECJ in the

Case C-210/17, paragraph 54). The enforcement of civil claims is

joint and several liability according to Art. 26 Para. 3 for the persons concerned

person relieved.

differentiation from other cases

Joint responsibility must be distinguished in particular from

Order processing according to Art. 28 and of a transmission of personal

drawn data to a person responsible, where the parties involved the purposes

and means of processing do not jointly determine.

For Germany there is also a need for clarification regarding the so-called radio

tion transmission, a previous German "special feature". as radio

tion transmission was under BDSG-old in differentiation to order (data)

processing means the outsourcing of a "function"/task that is processed via

the outsourcing of data processing as such goes beyond that by dem

recipient a certain scope for decision-making with regard to the tasks

fulfillment is granted. The body taking over the "task" was in

in this case under BDSG-old as own responsible; however

was usually - as far as can be seen - usual in this context

Unfortunately, shared responsibility is rarely ever assumed.

Under the GDPR there is no longer any room for the so-called transfer of functions.

On the one hand, this follows from the common law regulated in detail in Article 26

responsibility, on the other hand from the fact that certain decision-making

clear one within the framework set by the person responsible

Commissioner regarding the means of processing the order processing

do not exclude. Processing previously known in Germany as so-called

Functional transfer assessed under the GDPR - depending on

case – as order processing (Art. 28), as joint responsibility

(Art. 26) or as a "normal" transmission to another responsible

ally (without joint responsibility). Which case

is available in each case, is judged solely on the basis of who has the purposes and (at least

least essential elements of the means of data processing.

Joint decision on purposes and means of processing

A "joint decision" on the purposes and means of processing

assumes that each of those involved has a determining actual

influences data processing. A determining influence can

Express themselves that, for different purposes, by the respective

parties are pursued, a pursuit of a purpose within the framework of this specific

ten data processing is not possible without the other. A determining one

However, influence does not require each of those involved to have the comprehensive

has control over all circumstances and stages of processing. also is

full peer control by all parties involved is not required.

Rather, the involvement of the parties in determining the purposes

and means take very different forms and need not be uniform

be distributed. The existence of a shared responsibility means

not necessarily equal responsibility. The different for

those responsible for processing can be involved in the processing of personal

extracted data at different stages and to varying degrees

be included.

It is conceivable that the data-processing offices involved only in certain

Phases of data processing, such as data collection, together

are responsible. Who takes what role in processing and

who is responsible for what must be specified in the agreement pursuant to Art. 26 Para. 1

be precisely defined.

For example, the provider of an IT application or platform

and the user body jointly responsible for the collection

personal data of the end user, in particular if

the provider plans to use the data (also) for its own purposes and

insofar as one or more intended uses have been determined in advance.

Those involved must identify the means and the (possibly differentiated) purposes

mutually accept the terms of processing. A decision

the user body about the purposes and means of processing

be given even if they are specified in advance by the provider

accepts or joins the ends and means. A complete

The purposes pursued by the parties involved are not congruent

required if the purposes are closely related. The mere combination

However, the work of several bodies within a chain leads as such

not necessarily a shared responsibility.

Joint responsibility is not possible in the way that one

of the participants in an already existing (individual or joint)

working for the past "joins". For future processing

However, other responsible persons can join, provided that all parties involved

with a view to the future together the purposes and means of processing

establish. In this case, all data subjects must, in accordance with Art. 26

Para. 2 or Art. 13 Para. 3 will be informed again.

292

materials

A designation chosen by the participants themselves or any

tragic agreements can (only) as an indication of the actual

distribution of roles (see WP 169 of the Article 29 Group, p. 14, concluding

applications of the Advocate General to the ECJ in case C-210/16, para. 60).

Joint responsibility can also exist in such cases

in which the participants declare the relationship as order processing,

however, the purposes and means of processing also or even largely

are specified by the "contractor".

Those responsible are also liable without an agreement under Art. 26

Paragraph 1 jointly.

Joint responsibility can also exist if individual participants

separately responsible for certain parts or phases of processing

are, however, the data is collected via a common platform
(WP 169 of Article 29-
Group, p. 25). However, joint processing is then limited
on the operation of the platform. For the separate areas of responsibility
the platform itself does not have to be between the individual anymore
separate joint responsibility.

Specific Obligations Joint Controller

Art. 26 imposes specific obligations on the joint controllers who
about the obligations applicable to every person responsible under the GDPR
go out. This is intended to increase transparency and law enforcement for the
affected persons are improved.

The joint controllers must enter into an agreement
in which they specify in a transparent form which of them is which in the DS
GMO-regulated obligations fulfilled, in particular the rights of data subjects
and the information requirements according to Art. 13 and 14. This agreement must
the actual relationships of those jointly responsible
data subjects "duely reflect" and the "essentials"
of this agreement must be made available to data subjects
become. The provision supplements the actual obligation to provide information
mation of the persons concerned in accordance with Art. 13 and 14. "Essential" and
thus making available to the data subjects is at least one
comprehensible description of the interaction and the roles of the
involved and their respective relationship to the data subject as well as the
Specification of which of the joint controllers has which data subject rights
and to fulfill information obligations. In principle, it should be sufficient
these essential elements of the agreement according to Art. 26 on one

to provide the website (see recital 58). Notwithstanding the
The division of tasks made by the responsible persons in this agreement
However, data subjects can always assert their rights with and towards
each of the joint controllers (Article 26(3)). One good
elaborated contractual relationship to the respective responsibilities
as the basis of the transparent agreement is therefore also in the interest
the person responsible to clarify the liability issues internally.
Whether the parties involved have concluded an agreement that meets the
changes of Art. 26 is irrelevant for whether a common
responsibility exists. The latter is measured solely according to the
criteria shown.
There is a joint responsibility without an agreement
according to Art. 26 DS-GVO, fines can be imposed for this
Article 83(4)(a) may be imposed.
Other special features
In addition, in the case of joint responsibility, special
to be observed in some other regulatory areas of the GDPR:
Each of the jointly responsible persons is liable according to Art. 82 Para. 4 in connection
tion with paragraph 2 sentence 1 in the case of unlawful processing for the entire
damage unless he can prove that he was not at fault
(Art. 82 para. 3). Those responsible are liable even without an agreement
according to Art. 26 Para. 1 jointly. However, this helps with the balancing of liability
internally according to Art. 82 Para. 5.
Cases of joint responsibility can not infrequently lead to an increase

of risks to the rights and freedoms of data subjects, so that

Under certain circumstances, the implementation of a data protection impact assessment

Art. 35 is required.

Use cases:

Shared accountability may be more modern given the complexity

Data processing operations in very different cases

come into consideration. It is not possible to provide an exhaustive list

create, rather it requires a certain flexibility to create an effective

to ensure the protection of the rights and freedoms of data subjects.

A few cases are listed below without any claim to completeness

shown, in which - depending on the design - possibly joint responsibility

can be considered:

materials

– clinical drug trials when multiple contributors (e.g. sponsor,

Study centers/doctors) each in sub-areas decisions about the

meet processing,

– joint administration of certain data categories (e.g. address data)

for certain parallel business processes of several group companies

company,

– Joint construction of an infrastructure on which several participants can build their

pursue individual purposes, e.g. B. joint operation of a

Internet-based platform for travel reservations by a travel agency,

a hotel chain and an airline,

– E-government portal where several authorities can retrieve documents

provide by citizens; the operator of the portal and the respective

Authority are joint controllers (WP 169 of the Article 29 Group,

Example #11),

– Recruitment service provider working for an employer X applicants

examines and also includes applications received by him,

which are not aimed specifically at jobs with employer X (WP 169,

Example #6),

- (depending on the design, if necessary) common information pool/warning file

rerer responsible (e.g. banks) about defaulting debtors (WP 169,

Example #13).

4.6

Short Paper No. 17

Special categories of personal data

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the

DSK the General Data Protection Regulation (GDPR) in practice

should be applied. This view is subject to a

future – possibly different – interpretation of the European

Data Protection Board.

Qualification as a special category of personal data

As before, special categories will also become more personal in the future

data that require special protection. To the ones so far

Categories mentioned in the Federal Data Protection Act - information about the

racial and ethnic origin, political opinions, religious beliefs

generations, trade union membership, health (cf. Art. 4 No. 15
DS-GVO, recital 35) or sex life - now also occur in Art. 9 GDPR
genetic information and biometric data (Art. 4 No. 13 DS-GVO, Er-
wGr. 34; Art. 4 No. 14 GDPR, recital 51) for clear identification
one person. Were previously also considered philosophical beliefs
classified as particularly vulnerable, this category now falls under the
Term of "ideological" beliefs without being substantive
changes would be involved.
All information that directly or indirectly informs
provide information on the data categories specified in Art. 9 DS-GVO
(e.g. taking medication, physical or mental condition,
regular attendance at a particular church). On the other hand, too
in the future, not any indirect information on the special categories per-
personal data the application of special (strict) processing
entail provisions – e.g. B. is mere alcohol consumption in the
Unlike an alcohol addiction no health date pure
geographic place of birth no indication of racial or ethnic
Origin and the one-time visit to a sacred building contain no statement
about a religious belief. It is more difficult to classify light
pictures. They are only to be qualified as biometric data if
they are processed with special technical means that are unique
enable identification or authentication of a natural person
(Recit. 51). The suitability of photographs for identification by way of bio-
metric analysis method is in risk assessment and selection
of the technical and organizational measures must be taken into account.
Prohibition of processing with reservation of exception

Art. 9 para. 1 DS-GVO stipulates a general ban on processing

of data in these categories. However, Art. 9 Para. 2 lit. a to j

DS-GVO also regulates extensive exceptions to this principle,

so that there are some changes compared to the previous legal situation

are to be observed, but the practical application of the standards only a few

adjustments may result.

In addition to the express consent (Art. 9 Para. 2 lit. a DS-GVO).

special legal provisions or special circumstances in individual cases

Justification for the processing of particularly sensitive information

Considering: The above Prohibition of processing therefore applies according to Art. 9 Para. 2

furthermore not if the processing (lit. b to lit. j)

296

materials

b) for the exercise of rights and obligations arising from work or social

cial law is required; such processing may only then

take place when required by law; of that

also includes collective agreements such as works agreements;

the legislation must provide appropriate safeguards for fundamental rights

and take into account the interests of the data subjects (see also recital 52);

c) is necessary to protect the vital interests of a person and

this person is physically or legally unable to consent;

d) on the basis of suitable guarantees by a political, ideological

political, religious or union-oriented foundation/association/

Organization takes place without the intention of making a profit and is exclusively

refers to current or former members or to persons

who have regular contacts with the body in connection with their

Maintain purpose of activity, and not after the data without consent

be passed on to the outside;

e) relates to data that the data subject has obviously made public

has;

f) for legal prosecution or for the fulfillment of the tasks of the courts in

is necessary within the scope of their judicial activities;

g) on a legal basis for reasons of significant public

interest is required;

h) for purposes of health care, care or treatment

in the health or social sector is required by professional secrecy

nisträger takes place and on a legal basis or due to a

contract with a healthcare professional;

i) for reasons of public interest in the area of public

health, e.g. B. to prevent epidemics or to guarantee

drug safety, is required on a legal basis;

j) on a legal basis for archiving in the public interest

purposes, for scientific research purposes or for statistical purposes

Purposes according to Art. 89 Para. 1 DS-GVO is required.

From the opening clauses named in Art. 9 Para. 2 lit. b, g, h, i and j DS-GVO

The federal legislature has seldom in §§ 22 para. 1, 27 and 28 BDSG-new

in connection with the respective concrete special legal regulations

made use of. Section 22 (2) of the new BDSG also contains examples

enumerated measures to safeguard the interests of those affected

People who are responsible for everyone and thus everyone who has special

categories of personal data processed.

297

Whether and if so how far the regulations of the BDSG-new to the restriction

of the rights of those affected because of the existing priority of application

DS-GVO can be applied, remains a decision in the respective

reserved for specific individual cases.

Other data processing requirements

In addition to the special requirements for processing special

Categories of personal data should be according to ErwGr. 51 the general

n principles and other provisions of the GDPR, in particular

regarding the conditions for lawful processing. At

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 repressed, but its prerequisites in addition to those of the

Art. 6 GDPR must be present.

Automated decisions based on categories of special data,

are only permitted if the person concerned has expressly consented

or the processing takes place on a special legal basis and from

Reasons of substantial public interest is required (Article 22

Para. 4 GDPR). The federal legislature has in § 37 para. 1 No. 2 BDSG-neu

such a scheme to make decisions based on the application

binding payment regulations for medical treatments. So far the

The decision is based on the processing of health data

Responsible according to § 37 paragraph 2 BDSG-new appropriate and specific

Measures to protect the interests of the data subject

§ 22 para. 2 sentence 2 BDSG-new.

Responsible persons who process special data categories have in each

If a list of all processing

activities (Article 30 (5) GDPR).

In the case of extensive processing of special categories of personal

related data must regularly undergo a data protection impact assessment

be carried out (Art. 35 Para. 3 lit. b DS-GVO) and it is also

appoint a data protection officer if in this extensive

processing the core activity of the person responsible or the

worker (Art. 37 Para. 1 lit. c DS-GVO). Detailed information

the short paper “Data protection officers for those responsible and

processors”.

298

materials

Requirements for the data processing persons

In principle, in compliance with Art. 9 Para. 2 DS-GVO

Prerequisites all eligible persons from Art. 9 Para. 1

process the data collected under the GDPR. As far as such data, however

for the purposes specified in Art. 9 Para. 2 lit. h GDPR (in particular

health care and medical care) are processed,

Art. 9 Para. 3 DS-GVO standardizes specific requirements for the staff.

This is a mandatory prerequisite for permissible processing

Existence of a special confidentiality obligation (professional secrecy or

Confidentiality regulation) to which the processor must be subject.

4.7

Short Paper No. 18

Risk to the rights and freedoms of individuals

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the

DSK the General Data Protection Regulation (GDPR) in practice

should be applied. This view is subject to a

future – possibly different – interpretation of the European

Data Protection Board.

The aim of this short paper is to define the risk in the context of the GDPR

and to show how risks to rights and freedoms become more natural

Persons are determined and assessed with regard to their legal consequences

can. The containment of risks by taking appropriate technical

shear and organizational measures is not the subject of the paper.

I. Rights and freedoms of natural persons under the GDPR

(disambiguation)

“Rights and freedoms of natural persons” is a key concept in the

GDPR. The aim of the GDPR is, according to Art. 1 Para. 2 GDPR, the fundamental rights

and to protect fundamental freedoms of natural persons. These determine

adhere to the Charter of Fundamental Rights and Freedoms of the European Union

Union (Charter of Fundamental Rights - GrCh) and the European Human Rights

convention (ECHR). The concept of rights and freedoms of natural persons

also includes individual rights under ordinary law. He is within the

European legal context and not according to a purely national

increase The starting point for the interpretation of this term is the fundamental right

on protection of personal data according to Art. 8 GrCh, but it includes

in principle, all fundamental rights that are guaranteed by data protection law at least
be protected indirectly. The provisions in Art. 5 also serve to a particular extent
DS-GVO standardized principles for the processing of personal data
Data and the regulations on the rights of data subjects (Art. 12 et seq. GDPR)
this protection.
The rights and freedoms of natural persons are central to assessing
of a risk in accordance with the GDPR. Any processing of personal
data is at least an impairment of the fundamental right
the protection of personal data by a legal basis
must be justified (Art. 8 GrCh and Art. 6 GDPR).

II. Risk according to the GDPR (disambiguation)

The concept of risk is not explicitly defined in the GDPR. Out of
the recital 75 and 94 sentence 2 DS-GVO, the following definition can be derived
become:
A risk within the meaning of the GDPR is the possibility of
Occurrence of an event that itself causes damage (including
justified impairment of rights and freedoms of natural
persons) or to further damage to one or more
natural persons can lead.
It has two dimensions: first, the severity of the damage, and second
the probability that the event and the consequential damage will occur.
According to recital 75 are among the possible damages physical, material and
classify non-pecuniary damage. Unjustified impairments of
Rights and freedoms of natural persons (violations of fundamental rights)
are to be counted among the immaterial damages. Accordingly, in
Speaking generally of damaging events below and below

also the occurrence of an unjustified impairment of rights

and freedoms of natural persons. A damaging event can

give rise to further risks. unlawful processing

ment activities or processing activities that do not comply with the principles

of Art. 5 DS-GVO are in themselves impairments of the basic

right to data protection and therefore already represent a damaging event.

They can also take additional risks, such as natural discrimination

people.

300

materials

An example of this is an erroneous entry in a ban file

or misrepresentation of creditworthiness – a breach of

the principle of correctness in accordance with Article 5 (1) (d) of the GDPR

can also lead to financial consequential damage and damage to reputation.

Basically, damage can result from:

a. the planned processing itself,

b. responsible and

c. Externally caused deviations from the planned processing (e.g.

Third-party effects, natural disasters, hardware defects ...)

III. risk and legal consequences

The GDPR uses the distinctions "risk" and "high risk"

(e.g. recital 76). In addition, the wording “probably not to

a risk" (Art. 27 Para. 2 lit. a and Art. 33 Para. 1

GDPR). Since there cannot be completely risk-free processing,

the phrase "do not become a risk" is deprived of its meaning and purpose

starting out as leading “only to a small risk”. goal of

Risk assessment is therefore to classify the risks as “low

risk”, “risk” and “high risk”.

The risk with regard to legal consequences under the GDPR is relevant in particular

special at:

– Responsibility of the controller (Art. 24 para. 1

GDPR)

– Data protection through technology design (Article 25 (1) GDPR)

– Security of processing (Article 32 GDPR)

– Dealing with a personal data breach

(Art. 33, 34 GDPR)

– Data protection impact assessment and prior consultation (Art. 35,

36 GDPR

IV. Risk Assessment

The phases described below are to be used for the risk assessment

run through:

1. Risk Identification

2. Estimation of the probability of occurrence and severity of possible

damage

3. Assignment to risk classifications

A risk assessment must be based on a concrete description of the

underlying facts for which the risk is to be assessed.

1. Risk Identification

To identify data protection risks, it is advisable to use the following

questions to go out:

a. What damage can be based on natural persons

of the data to be processed?

b. by what, i.e. H. What events can cause the damage?

c. What actions and circumstances can lead to this

events coming?

to a.) Damage to natural persons

According to the GDPR, damage can be physical, material or immaterial

be nature (recital 75, first sentence). The concept of damage is thus in a

to be understood in the broadest sense and not to damage that can be quantified in monetary terms

limited.

It must be considered the negative consequences of the planned processing itself

become. This includes restrictions on rights and freedoms,

for example, if affected persons for fear of disadvantages on the

refrain from exercising their rights (e.g. refraining from participating in a

demonstration due to extensive surveillance).

Also negative consequences of deviations from the planned processing

must be considered (e.g. data access by unauthorized persons

or bodies, unauthorized disclosure or association of data, accidental

Destruction of data, failure or limitations of those provided

processes, accidental or intentional unauthorized modification of

data, failure to fulfill a right to information). The deviations can

to an unlawful one or one that violates data protection principles

lead processing.

Every processing of personal data takes place at least one

Impairment of the fundamental right to protection of personal data

(cf. Art. 8 GrCh). In addition, other fundamental rights may be affected, such as

e.g. B. respect for family life in Art. 7 GrCh or the opinion and

Freedom of assembly in Art. 11 and 12 GrCh or the right to non-

302

materials

criminalization in Art. 21 GrCh. These impairments lead to damage

if they are not justified.

Ultimately, all conceivable negative consequences of data processing must be eliminated

for the rights and freedoms of natural persons, their economic,

financial and immaterial interests, their access to goods or

services, for their professional and social standing, for their

health condition and for any other legitimate interests

to be viewed as.

Examples of possible damage include:

– Discrimination

– Identity theft or fraud

- financial loss

– damage to reputation

– economic or social disadvantages

– Making it more difficult to exercise rights and preventing control

affected people

– Exclusion or limitation of the exercise of rights and freedoms

– Profiling or use by assessing personal aspects

– bodily harm as a result of actions based on incorrect

liable or disclosed data

to b.) Events

For each potential damage already identified, the events

determined that could lead to its realization. These consist in the

Non-compliance with the data protection principles according to Art. 5 Para. 1 DS-GVO

as well as the non-granting of the rights of data subjects according to Art. 12 et seq. DS-GVO,

in particular:

– unauthorized or unlawful processing

– Processing contrary to good faith

– processing that is not transparent for the data subject

– unauthorized disclosure of and access to data

– Accidental loss, destruction or corruption of data

– Denial of data subject rights

– Incompatible use of the data by the person responsible

purposes

– Processing of unforeseen data

– Processing of incorrect data

– Processing beyond the storage period

In the case of damage resulting from the processing itself, this exists

event in this same processing.

to c.) Sources of risk

A relevant part of the sources of risk is the area of responsibility or

processors and the processing carried out by them according to plan

to assign. It is also necessary to consider the extent to which people in the

Area of the person responsible or any processor aware or

unintentionally exceed the scope provided for processing

could (e.g. a sales department that requires the earmarking of customer data

may change, for example to meet a sales target).

Another example is employees who willfully disobey instructions

on the handling of personal data violated or intentionally in

act without authorization in pursuit of their own interests.

There are also risks from unauthorized attackers such as cybercriminals

take into account. Sources of risk may also be government agencies that

gain unauthorized access. Finally, sources of risk

lie with communication partners with whom personal data

authorized to be exchanged, or with manufacturers and service providers who

Information technology, including the software used with it, which is used for

the processing of personal data or in their environment

will provide or wait.

Finally, technical malfunctions and external influences, e.g. B. through

force majeure, to be considered as sources of risk.

2. Estimation of the probability of occurrence and severity of possible

damage

For each possible damage, the probability of occurrence and

estimated severity. These can only be

to grasp cases mathematically.

Nevertheless, the GDPR requires the risk to be assessed on the basis of objective criteria

assess (recital 76). Especially in cases of immaterial damage, such as

e.g. B. damage to reputation, must also - on the basis of objective criteria -

be judged as to how serious the possible negative consequences for

the lifestyle of the persons concerned are to be classified.

One way of measuring a risk is to use a scale

determination of the severity and probability of occurrence of a

possible damage on a scale - with, for example, four levels

gen – to represent.

Both for the differentiation of the probability of occurrence and for

possible damage could be used in each case the following gradations:

– slightly

– manageable

– substantial

- large

The assignment to the levels must be justified.

probability of occurrence

The probability of occurrence of a risk describes the probability

probability of a specific event (which itself may also be damage

can) occurs and with what further probability there is consequential damage

can come.

For example, is the damaging event an unwanted one?

disclosure of a person's sexual orientation, the likelihood

reliability of both this disclosure and the resulting from it

assess further damage.

The probabilities of the various paths leading to such a

Disclosure can add up here. In the example mentioned

include inadequate precautions of those responsible, more careless

Dealings of employees under their direct responsibility with the

information, technical malfunctions or spying by third parties

the paths to consider.

The severity of the potential damage

The severity of possible damage must be determined in each individual case in particular

taking into account the type, scope, circumstances and purposes of the processing

be determined (recital 76). Significant factors are in particular:

– Processing of specially protected data within the meaning of Art. 9 and 10

DS-GVO, in which the DS-GVO expressly requires increased protection

neediness provides;

– Processing of data of groups of people worthy of protection (e.g. children,

employees);

– Processing of non-modifiable and uniquely identifying data

such as B. clear personal identification numbers compared to pseudonymous

ated data;

– Automated processing that involves a systematic and comprehensive

Assessment of personal aspects (e.g. profiling) include and on their

Basis then decisions with significant legal effects for

affected persons are met (cf. Art. 35 Para. 3 lit. a DS-GVO);

- if the damage is not or hardly reversible or the affected person

has only few or limited possibilities, the processing itself

to check or to be checked by a court or to object to this processing

to withdraw, for example, because they have no knowledge of the processing;

– if the processing enables systematic monitoring;

– the number of data subjects, the number of data sets and

the number of features in a dataset; and the geographical one

Coverage achieved with the processed data.

3. Assignment to risk classifications

After the probability of occurrence and the severity of possible damage

were determined, these must correspond to the risk classifications "low risk",

"Risk" and "high risk" are assigned. Like this picture specifically

takes place is not described in more detail in the GDPR - it therefore exists

basically scope for different models.

The overall risk of processing is generally the highest risk

class of individual risks. Should many in this risk class

Individual risks may exist, but it may be necessary in individual cases

assume a higher risk class.

risk matrix

For the assessment of the risk of processing according to the probability of occurrence

probability and the severity of the possible damage can be the following

matrix are used:

306

materials

When estimating the risk using the matrix, cases may arise

in which the occurrence of the damage is relatively probable or the potential

cial damage would weigh particularly heavily and thus borderline areas

between risk areas may be affected. Here are in the fields

entered two colors in the matrix. This makes it clear that in these

borderline cases, a case-by-case analysis is necessary. In case of doubt, this can

come to the conclusion that, despite the result of the generic

assessment based on the matrix of individual cases appears to be so serious that

that there is still a high risk. Conversely, in individual cases

e.g. B. also a minor possible damage that is manageable

probability of occurrence represent a low risk.

With the procedure described up to this point, the

risk of data processing, taking into account the circumstances

of processing.

307

47th activity report on data protection

V. Risk Control

By way of the data protection impact assessment or – if likely

there is no high risk - in a simplified procedure, the next

th step to appropriately contain the risks

determine.

Basically, the risk of processing by means of remedial measures

to contain Often this will correspond with the prior art

technical and organizational measures (TOMs) can be achieved,

which are suitable to protect the rights and freedoms of the natural persons concerned

adequately ensure by reducing the probability of occurrence

and/or mitigate the severity of the potential damage. In addition

include measures to contain adverse events (e.g.

Attacks by cybercriminals) like classic security measures

from information security, but with a view to protecting the

are to be assessed by the persons concerned and not by the person responsible.

VI. residual risk

The risk remaining after these measures have been implemented is

referred to as risk. If this residual risk is classified as high, then there is

the obligation for prior consultation in accordance with Art. 36 GDPR.

The person responsible must check carefully (and according to Art. 5 Para. 2 DS-GVO

documented as proof of compliance with the requirements of the GDPR

have), whether he has all possible according to the principle of proportionality

taken measures to mitigate the risk before commencing

processing begins.

After the remedial measures have been implemented, they must be tested for effectiveness

tested and continuously monitored. Possibly shows

when implementing the measures that there are other risks that

are also to be treated.

Conclusion

The objective determination and assessment of the risk of processing

personal data in the above Sense is required to determine how

the rights and freedoms of natural persons are effectively protected.

Short Paper No. 19

Informing and obliging employees to comply

the data protection requirements according to the data protection

basic regulation

This short paper by the independent federal data protection authorities

and the countries (data protection conference - DSK) serves as a first orientation

especially for the non-public area, as in the opinion of the

DSK the General Data Protection Regulation (GDPR) in practice

should be applied. This view is subject to a

future – possibly different – interpretation of the European

Data Protection Board.

What does the General Data Protection Regulation (GDPR) regulate?

According to Article 29 GDPR, employees of a person responsible (a company, a club, an association, a self-employed person, a authority and so on) or a processor's personal data Data exclusively on the instructions of the person responsible or arbeiters process, unless a statutory provision dictates one processing of this data.

In addition, Article 32 Paragraph 4 DS-GVO regulates that the person responsible or processor must take steps to ensure that persons subordinate to him (in particular his employees) who Have access to personal data, only on the instructions of the controller or processor (unless a statutory regulation prescribes the processing of this data). For the In the case of order processing, Article 28 paragraph 3 sentence 2 letter be b DS-GVO that the processor must ensure that the persons authorized to process the personal data have committed to confidentiality (insofar as they do not are subject to statutory confidentiality obligations; The latter applies, for example for private medical, tax consultant or legal clearing houses).

Even if, according to the wording of the GDPR, only the employees of one are to be "obligated" by the processor, the content of this "obligatory de information" (hereinafter: obligation) also those responsible and their employees. How responsible this legal obligation implement (and, if necessary, prove to the supervisory authority), is not bindingly regulated. It is recommended that this be in the form of a written or to implement an electronic declaration of commitment. A pattern for one

such obligation can be found in the Annex.

What should be committed?

The obligation of employees to maintain data secrecy

and to comply with data protection requirements is an important one

part of the measures required for a responsible

cher (see Article 5 paragraph 2 and Article 24 paragraph 1 GDPR) or a

Processor (see Article 28 Paragraph 3 Clause 2 Letter b GDPR)

ensure and prove compliance with the principles of the GDPR

may (“accountability”). These principles of the GDPR, laid down in

Article 5 paragraph 1 DS-GVO essentially includes the following obligations:

Personal data must

a) in a lawful and fair manner and in a way that is fair to the data subject

be processed in a comprehensible manner ("lawfulness, processing

good faith, transparency”);

b) collected for specified, explicit and legitimate purposes and

may not be used in a manner incompatible with these purposes

be further processed ("earmarking");

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

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

d) accurate and, where necessary, up to date; it

all reasonable measures must be taken to ensure that personal

data that are inaccurate in relation to the purposes of their processing,

promptly deleted or corrected ("accuracy");

e) stored in a form that allows the identification of those concerned

persons only for as long as is necessary for the purposes for which they

work is required (“Storage Limitation”);

f) processed in a manner that provides adequate security

of personal data, including protection against

unauthorized or unlawful processing and against unintentional

loss, accidental destruction or accidental damage

through appropriate technical and organizational measures ("Integrity

and confidentiality").

The core element of the measure is that the employees on compliance

be bound by operational instructions. The shape of the respective

sung is of secondary importance. In addition to individual instructions

of superiors, in particular company agreements and general

service instructions. In addition, process descriptions (e.g

from quality management), schedules and documentation

(e.g. register of processing activities) and manuals

instructional character.

310

materials

Who needs to be committed?

The group of persons to be obliged (the DS-GVO speaks in this respect

of “subject natural persons”) is due to the importance of these

regulation to be interpreted broadly. In particular, in addition to the regular

core of workers also trainees, interns, legal trainees, temporary workers

and involve volunteers.

So much for the secrecy of employees in the public sector

is expressly regulated by law or collective bargaining agreement, such a

obligation does not occur.

When does the commitment have to be made?

The commitment must be made upon commencement of the activity. she should

should therefore be made on the first working day if possible (at the latest).

How must an obligation be made?

Responsible for the obligation is the company management, the owner of a

company or one of its representatives. Even if, as stated above,

the GDPR does not prescribe a specific form of obligation, it should

a special form can be used for reasons of proof, whereby the

Commitment may be in writing or in an electronic format.

The obligation also includes instruction about the resulting

duties. The employees are - if possible based on typical cases -

to inform you about what you can do in terms of data protection with your

have to consider daily work. With the obligation according to the GDPR

other non-disclosure agreements can also be combined,

for example on trade, telecommunications or tax secrecy. Out of

Reasons for proof within the framework of the accountability according to the DS-GVO

it is important to adequately document the commitment.

Is the one-off data protection obligation enough?

For the ongoing sensitization of employees to questions of data protection

it is advisable to do this at regular time intervals as part of training courses

or in written notices, for example in the company newspaper

to remind employees that they have been committed and which ones

importance of this obligation. If a job change in

company or authority, with a change of responsibilities

is connected, this should always be taken as an opportunity to

Obligation to review and adjust if necessary.

Attachment/example of a written commitment1:

Commitment to confidentiality and compliance

data protection requirements according to the data protection

Basic Regulation (GDPR)

Mrs Mr _____

undertakes not to process personal data without authorization

ten. Personal data may therefore only be processed

if there is consent or a legal regulation

Processing permitted or required. The principles of the GDPR for

the processing of personal data must be safeguarded; They are in

Article 5 paragraph 1 DS-GVO and contain essentially

the following obligations2:

Personal data must

a) in a lawful and fair manner and in a manner that is safe for the person concerned

be processed in a comprehensible manner ("lawfulness,

Fair processing, transparency");

b) collected for specified, explicit and legitimate purposes and

may not be in a manner incompatible with these purposes

further processed ("purpose limitation");

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

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

d) accurate and, where necessary, up to date;

all reasonable measures must be taken to ensure that personal

related data, with regard to the purposes of their processing

are inaccurate, be deleted or corrected immediately ("directory

activity");

e) stored in a form that allows the identification of the

fenen persons only for as long as is necessary for the purposes for

which they are processed is necessary ("storage limitation");

f) processed in a manner that provides adequate security

of personal data, including protection

from unauthorized or unlawful processing and from unauthorized

accidental loss, accidental destruction or accidental damage

312

materials

Damage caused by suitable technical and organizational measures

(“Integrity and Confidentiality”).

Personal data may therefore only be processed according to the instructions of the responsible

be processed verbatim. In addition to individual instructions from superiors

apply as instructions: process descriptions, flow charts, operational

agreements, general service instructions and operational documents

mentations and manuals3.

Violations of this obligation may result in a fine and/or exemption

be punished with imprisonment. A violation can also be a violation

of contractual obligations or special confidentiality obligations

represent. (Civil law) claims for damages can also arise

resulting from culpable breaches of this obligation. Her

arise from the employment or service contract or separate ones

Confidentiality obligations resulting from agreements are enforced by these

statement unaffected.

The obligation continues to apply after the end of the activity.

I confirm this commitment. Have a copy of the commitment

i received

_____

Place, date Signature of Signature of

Obliged Responsible

1 To the extent that the confidentiality of employees in the public sector is required by law or

is expressly regulated in a collective agreement, such an obligation does not have to take place.

2 The content of the obligation must be adjusted in individual cases. So can certain tasks

and activities require additional information, for example on employee or social

data protection, on telecommunications secrecy and so on.

3 The list must be adjusted in individual cases. In this way, further documents can

actor or enumerated types are not important for individual responsible persons.

313

314

materials

5. Resolution of the 36th Conference of

Freedom of Information Officer in Germany

from 16.10.2018

5.1

Social participation needs consistent publication of

administrative regulations!

An open and transparent administrative culture is a prerequisite for

for citizens and the state to meet on an equal footing.

The conference of freedom of information officers in Germany demands

the social service providers, administrative regulations independent of the application,

to publish in a timely and user-friendly manner, insofar as they do not do so

are already required by law.1

Social participation of all people in our society follows from the im

principle of the welfare state enshrined in the Basic Law. expression of this principle

a social security system based on social security benefits

Social codes guarantee a basic standard of social security

should. Only informed citizens can make the decisions that concern them

Understand benefits agency decisions, file claims

do, but also fulfill obligations.

All social service providers use administrative regulations to

a uniform processing and decision-making practice for your authority

ensure. Administrative regulations are internal directives that regulate

how laws are to be interpreted and applied. Admittedly, administrative

regulations directly only the administration itself; those on their basis

However, the decisions made have an external effect. administrative regulations

are therefore to be announced so that "the person concerned (...) is aware of the content of the

rights and obligations established for him by them”2.

For example, the Federal Employment Agency and the

German pension insurance, which publish current instructions. Many

other social service providers, on the other hand, provide the information at best

out upon request.

1 Legal obligations currently exist in: Hamburg, Bremen, Rhineland-Palatinate,

Schleswig-Holstein (from January 1st, 2020).

2 Judgment of the Federal Administrative Court of November 25, 2004, Az. 5 CN 1.03.

subject index

subject index

FIRST PART: REPORT ON DATA PROTECTION

subject index

factual terms

address data

accreditations

– DAkkS

– test criteria

– certification bodies

insight into files

administrative assistance

Employer

workers

processor

Information

credit bureaus

right to information

request for information

Provision of information

right of providing information

Information systems, police

auto repair shops

correction

reporting obligation

professional secrecy

Employee (data)

Text number of

activity report

3.2.2

4.10.4

4.10.4

4.10.4

4.10.4

3.4.1, 3.4.3, 4.1.1, 5.3

3.1.2

4.1.5, 4.9.1

3.2.1

3.5.3, 4.1.3, 4.4.2, 4.5.2,

4.10.1, 4.10.2, 4.11.2

2.6, 4.7.2, 4.9.2

4.8.1, 4.8.2

3.3.1, 4.1.1, 4.5.2

3.1.2

4.1.2, 4.3.4

2.6, 3.1.3, 4.1.1, 4.1.2, 4.5.2,

4.3.4

4.5.3

4.1.1

data storage

Data Protection Officer

- Contact details

- Report

Data Protection Impact Assessment

– CNIL methodology

– risk assessment

data breach

– obligation to notify

– fine

– Obligation to report

– Prognosis decision

data transfer

– credit bureaus

– gas supplier

– Chambers of Commerce and Industry

– network operator

– Religious communities

318

3.5.1

3.5.1

5.2

4.8.2

3.5.3

4.4.3

4.10.1

Online application

online search

Online imprint

Online Reporting Procedure

Online portal

Online TKÜ

Online Access Act

organizational control

4.4.1

4.7.4

1.3.1, 2.2

4.3.2

4.10.2

4.7.3

4.10.4

4.3.2, 4.4.2

2.1

2.4

4.2.2

3.5.2

2.5, 2.6

4.7.3

4.1.3

4.3.2

2.5

3.5.3, 4.3.1

4.10.1

panoramic shots

Parliamentary Control Commission

4.3.6

2.6

321

The Hessian Commissioner for Data Protection and Freedom of Information

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

patient record

patient data

patient information

personnel file

personnel information system

Privacy by design

Privacy Shield

log files

log data

inspection requirements

Source TKÜ

3.4.3, 5.3

3.4.2

4.1.4

4.1.2

4.1.2

4.3.1

4.2.1, 4.4.1

3.4.2

3.3.2

4.8.2

3.5.3

3.1.2

Standard Privacy Model

– storage

- Building blocks

– Data protection management

– documentation

– Guarantee objectives

– Delete and Destroy

– logging

– separation

phone calls

Transparency (principle)

transmission

– electronic documents

– telemetry data

– Whois queries

accident data storage

union law

Responsible

processing activity(s)

processing operations

consumption data

virtualization

web application

promotional purposes

Whatsapp

credit bureaus

certifications

access rights

Access Permission

cooperation, european

Summary, structured

Reliability Check(s)

change of purpose

earmarking

324

2.6, 2.7

4.9.1

4.1.7

4.3.3

4.4.2

4.10.1

4.3.1

4.3.6

2.3, 2.5, 3.1.4, 4.1.2

2.5

4.1.6

2.5, 3.1.4

PART TWO: FREEDOM OF INFORMATION REPORT

subject index

Text number of

Freedom of Information Report

factual terms

trade and business secrets

Hessian Freedom of Information Act 2

Informational self-determination

information requests

– municipalities

– Ministries

information access

Constitutional requirements

administrative action

census verdict

1.3, 1.3.2, 1.3.3

3.1

3.2

3.2

2.3

1.1

1.1

1.3.3

325