Forty-ninth activity report

to data protection

and

Third activity report

to freedom of information

of

Hessian Commissioner for Data Protection

and freedom of information

professor dr Michael Ronellenfitsch

submitted as of December 31, 2020

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

of the Hessian Data Protection and Freedom of Information Act

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

The Hessian Commissioner for Data Protection and Freedom of Information

49th activity report on data protection / 3rd activity report on freedom of information

Contributions to data protection and freedom of information

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

Prof. Dr. Michael Ronellenfitsch

Gustav-Stresemann-Ring 1, 65189 Wiesbaden

PO Box 31 63, 65021 Wiesbaden

Phone:

Fax:

E-mail:

Internet:

(06 11) 14 08-0

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

poststelle@datenschutz.hessen.de

www.datenschutz.hessen.de

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

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

Table of contents

Table of contents

IX

List of Abbreviations

List of Abbreviations

List of Abbreviations

OJ EU

Section.

Inc

oh

kind

AsylbLG

Official Journal of the European Union

Unit volume

public company

tax code

Article

Asylum Seekers Benefits Act

Federal Labor Court

BigBlueButton

Binding Corporate Rules (binding internal

data protection regulations)

Federal Data Protection Act

Federal Data Protection Act old version

decision

Federal Commissioner for Data Protection and

Freedom of Information

Federal Fiscal Court

Civil Code

Federal Law Gazette

Federal Court of Justice

BAG

BBB

BCR

BDSG

BDSG a. f

acc.

BfDI

BFH

Civil Code

Federal Law Gazette

BGH

BT Drucks., BT-Drs

BTLE

BVerfG

or.

Borders, Travel & Law Enforcement (Subgroup)

Federal Constitutional Court

respectively

approx.

COVID-19

C.S.C

approximately

Coronavirus disease 2019

Coordinated Supervision Committee

That means

German industry standard(s)

German Foundation for Organ Transplantation

i.e. H.

DIN

DSO

GDPR, GDPR General Data Protection Regulation

DSK

Conference of the independent data protection supervisory

federal and state authorities; short: data

protection conference

e. V

EDSA

registered association

European Data Protection Board

XI

The Hessian Commissioner for Data Protection and Freedom of Information

49th activity report on data protection / 3rd activity report on freedom of information

EN

ERVV

recital

Etc.

EU

ECJ

Eurodac SCG

European standard

Ordinance on the technical framework

conditions of electronic legal transactions

and via the special government mailbox

recital

et cetera

European Union

Court of Justice of the European Union

Eurodac Supervision Coordination Group

the following

following (pages) / subsequent

General Data Protection Regulation (= GDPR)

in which case

Law and Ordinance Gazette (Hessen)

Hessian representative for data protection and

Freedom of Information

Hessian Data Protection and Freedom of Information

law

Hessian Municipal Code

Hessian Ministry of Education

Hessian security check law

Hessian security check and closure

property law

usually

International Electrotechnical Commission

internal committee

within the framework of

in terms of

International Organization for Standardization

(International Standardization Organization)

with the meaning of

combined with

German Infection Protection Act

collection agency

Internal Market Information System

information system)

information technology

f.

onwards

GDPR

possibly.

GVBl.

HBDI

HDSIG

HGO

HKM

HSUG

HSÜVG

i. i.e. R

IEC

INA

i. r.d.

i. s.d.

ISO

i. S.v.

i. V. m.

IfSG

ICU

IMI

IT

XII

List of Abbreviations

vehicle

COM

LDA

lit.

LAG

lsbh

LT Drs.

LUSD

MTA

MUA

ND

No.

OFD

above

OwiG

QR code

No./Rn.

Rs.

S

s.

s.a.

SDM

SIS II SCG

so-called.

SSA

StGB

StbergG

TB

etc.

UK

UNITED STATES)

motor vehicle

European Commission

State Office for Data Protection Supervision

Littera

regional labor court

State Sports Association of Hesse

State Parliament printed matter (Hessen)

Teacher and student database

Mail transfer agent

Mail User Agent

name service

number

Head of Finance

above/named/named/named

Administrative Offenses Act

Quick response code

marginal number

case

page or sentence

please refer

see also

Standard Privacy Model

Schengen Information System II Supervision

Coordination Group

so-called/so-called/so-called

State Education Board

criminal code

Tax Advisory Act

activity report

among other things

United Kingdom

United States of America

XIII

The Hessian Commissioner for Data Protection and Freedom of Information

49th activity report on data protection / 3rd activity report on freedom of information

etc.

v.

see.

VIS SCG

VKS

WHO

WIRELESS INTERNET ACCESS

e.g. B.

item

and so forth

from

compare

Visa Information System Supervision Coordination

group

video conferencing system

World Health Organization

organization)

Wireless Local Area Network

for example

digit

XIV

Register of Legislation

Register of Legislation

Register of Legislation

The versions valid at the time of processing are quoted.

law/regulation

site(s)

Asylum seekers-

performance law

Asylum Seekers Benefits Act in the version published

from August 1997 (Federal Law Gazette I p. 2022), last amended by law

from December 21, 2020

oh

BDSG

BDSG a. f

Civil Code

12. BImSchV

CoKoBeV/Corona

contact and

operating

constraint

regulation

CoKoBeV/Corona

contact and

operational

restrictive

regulation

GDPR

Tax code 1.10. 2002 (BGBl. I p. 3866; 2003 I p. 61), last

modified by article 28 of the law of December 21, 2020

(BGBl. I p. 3096)

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

amended by Art. 12 Second Privacy Adaptation and

EU Implementation Act of 20.11.2019 (Federal Law Gazette I p. 1626)

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

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

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

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

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

Hazardous Incident Ordinance in the version published by

March 15, 2017 (Federal Law Gazette I p. 483), which was last amended by Article 107 of the

Ordinance of June 19, 2020 (BGBl. I p. 1328) was changed

Ordinance on the restriction of social contacts and the

Operation of facilities and offers based on the

corona pandemic

(Corona Contact and Operational Restriction Ordinance) from 7.

May 2020, get up. by Article 4 No. 3 of the Ordinance of 26 November

November 2020 (GVBl. p. 826)

Ordinance on the restriction of social contacts and the

Operation of facilities and offers based on the

Corona pandemic in the version effective on August 15, 2020

changes due to Art. 3 of the Seventeenth Ordinance

Adaptation of the regulations to combat the corona virus

from August 11, 2020 (GVBl. p. 538)

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)

XV

The Hessian Commissioner for Data Protection and Freedom of Information

49th activity report on data protection / 3rd activity report on freedom of information

Cooperative Law i. i.e. F. from 16.10.2006 (Federal Law Gazette I p. 2230),

last amended by law from December 22nd, 2020 (Federal Law Gazette I p. 3256)

Money Laundering Act of June 23, 2017 (Federal Law Gazette I p. 1822), most recently

amended by Article 269 of the Ordinance of June 19, 2020 (BGBl.

I p. 1328)

Hessian Data Protection and Freedom of Information Act of

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

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

Commercial Code in the BGBl Part III, structure number 4100-1,

published revised version, last amended by Article 3

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

Hessian school law from August 1st, 2017, last changed by Art. 1

of the law of September 29, 2020 (GVBl. p. 706).

Hessian law on public safety and order dated

January 14, 2005 (GVBl. I 2005 p. 14), last amended by Article 19

Hess. Foreigners Participation Act of 07.05.2020 (GVBl. p. 318)

Hessian Security Check Act of 19.12.2014,

Title revised and amended by law of 11.12.2019

(GVBl. p. 406)

Hessian security check and classified information law

(HSÜVG) of December 19, 2014, amended by law of December 11, 2019

(GVBl. p. 406)

Law on the Prevention and Control of Infectious Diseases

in humans from 20.07.2000

(Federal Law Gazette I p. 1045), last amended by Article 4a of the law of

December 21, 2020 (Federal Law Gazette I p. 3136)

Municipal Fees Act as amended on 24.03.2013

(GVBl.2013, 134) last amended by Art. 1 Law on

New regulations for the collection of road fees from 05/28/2018

(GVBl. p. 247)

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 modified by Article 3 § 31 of the law of February 16th

2001 (BGBl. I p. 266)

Banking Act in the version published by

09.09.1998 (Federal Law Gazette I p. 2776), last amended by Article 4 of the

Law of December 9th, 2020 (Federal Law Gazette I p. 2773)

GenG

GWG

HDSIG

HGB

HSchG

HSOG

HSUG

HSÜVG

IfSG

KAG

KUG

KWG

XVI

OWiG

OWiG

PAuswG

Social Code I

SGB X

StGB

StbergG

StVG

TPG

Register of Legislation

Code of Administrative Offenses as amended

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

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

Code of Administrative Offenses as amended

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

by Article 3 of the law of November 30th, 2020 (Federal Law Gazette I p. 2600)

Personal Identity Card Act of 06/18/2009 (Federal Law Gazette I p. 1346), last

amended by Article 13 of the law of December 3rd, 2020 (Federal Law Gazette I

p. 2744)

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

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

Law of 06/12/2020 (Federal Law Gazette I p. 1248, 1255)

The Tenth Book of the Social Code - Social Administration Procedures

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

01/18/2001 (Federal Law Gazette I p. 130), last amended by law from

03.12.2020 (Federal Law Gazette I p. 2668, 2673)

Criminal Code in the version published by

November 13, 1998 (Federal Law Gazette I p. 3322), last amended by Article 47 of the

Law of December 21, 2020 (Federal Law Gazette I p. 3096) has been changed

Tax Advisory Act in the version of the notice dated

November 4th, 1975 (Federal Law Gazette I p. 2735), last amended by Article 37 of the

Law of December 21, 2020 (Federal Law Gazette I p. 3096)

Road Traffic Act of 05.03.2003, last amended by

Art. 3 of the law of November 26, 2020 (Federal Law Gazette I p. 2575)

Law on Donation, Removal and Transfer of Organs

and fabrics from September 4th, 2007 (Federal Law Gazette I p. 2206, TPG), most recently

changed by Art. 6 Patient Data Protection Act of October 14th, 2020

(BGBl. I p. 2115)

XVIII

core items

core items

core items

1. Number and examination effort of the procedures in European cooperation

work (coherence, cooperation, BCR procedures) with participation

of the HBDI are constantly increasing and intensifying. Last but not least

the Brexit and the so-called Schrems II judgment of the ECJ are massive

data protection effects also apply to data traffic in third countries

expected (Part I No. 2.1 and 2.2).

2. The implementation of the corona protection measures led to many
everyday areas of life to data protection complaints,
Inquiries and advice from data subjects and for data processing
responsible. This concerned z. B. Schools (Part I, Items 5.1, 5.2),
Municipalities (Part I No. 3.1), companies (Part I No. 8.3), hospitals
(Part I No. 8.1), sports clubs (Part I No. 10.1), restaurants (Part I No. 11.6),
Hairdressing companies (Part I No. 11.6), the use of advertising measures (Part
I Section 13.2) and e-mails (Part I Section 14.1).
The increased, corona-related (forced) stay was probably
of many people in their homes is a reason why the single
gave increased again to video surveillance in the neighboring context
increased (Part I No. 9.1).
3. As before, a central focus was the processing of
complaints, inquiries and advice on exercising data subject
rights, such as the right to erasure 17 DS-GVO (Part I No. 3.2; 11.2,
12.2, 12.3) or the right to information 15 DS-GVO (Part I No. 6.3,
12.1,12.2, 12.3) as well as for consent (Part I No. 7.1, 7.2, 7.3, 12.3) and
their revocation (Part I No. 7.1), for access control (Part I No. 11.4)
and on the information requirements according to Art. 14 DS-GVO (Part I No. 12.2).
4. With the amendment of the Hessian Security Check Act,
now Hessian security check and classified information law,
special data protection regulations were created and
Search powers of the HBDI restricted (Part I, Item 4.1).
5. Reporting data breaches and data breaches in accordance with
Art. 33 DS-GVO now form a large part of the reactive activity
my supervisory authority (Part I, Sections 6.1, 8.4, 8.7, 15.1, 15.2, 17.2). So

Corona-related work in the home office led to further incidents

in new constellations, such as B. Unauthorized Data Disclosures

the use of video conferencing systems or private end devices

Home office (Part I No. 15.1).

XIX

The Hessian Commissioner for Data Protection and Freedom of Information

49th activity report on data protection / 3rd activity report on freedom of information

6. The processing of personal data by banks and

Banks are only permitted if a corresponding legal basis

position this provides. These can often also be found in civil law (Part I No.

11.1), sometimes the existence of a legitimate interest on the part of

be a requirement of the credit institution. If the presence of a

justified interest as a prerequisite for admissibility, that is

Blackening of data on documents to be submitted as a rule

permitted (Part I, Item 11.3).

7. The joint cross-border examination of tracking procedures

(use of cookies) on newspaper websites has started and will

ensure legally compliant practice in the long term (Part I, Item 13.1).

8. Priorities in the area of sanctions and fine procedures were

repeated violations of data subject rights and the so-called

employee excesses. There were also corona-related issues (Part I

Clause 6.1, 16.2).

9. The conception of the Hessian Freedom of Information Act would

it correspond if the legislature the access to information also

to the State Office for the Protection of the Constitution and the police

measured would open (Part II.2).

10. Submissions within the competence of the Hessian Information Freedom

orders have increased only slightly (Part II.5, 6).

XX

foreword

foreword

foreword

During the processing of this activity report, the office holder changed

About the Hessian Commissioner for Data Protection and Freedom of Information.

Even if the law binds the incumbent to the continuity of the

performance of office is guaranteed, there is no universal legal succession in this respect.

The formulation of the data protection policy of the Hessian

responsible for data protection and freedom of information is rather an autonomous one

Matter of the person holding the office. The 49th Activity

report concerns a period in which the former Data Protection Officer

was responsible. It follows that this is fundamentally also the factual

Responsible for the 49th activity report. The formal final decision

On the other hand, responsibility for the activity report is incumbent on

the current incumbent. The structure of this corresponds to this

activity report. The former incumbent reports on the period of his

Responsibility. The current incumbent, on the other hand, leads in

the current situation of data protection and the expected development

of data protection law.

Apart from this distinction, the structure of this report follows

the structure of previous reports.

Prof. Dr. Michael Ronellenfitsch

XXI

To revitalize data protection after the pandemic has subsided

To revitalize data protection after decay

the pandemic

Comments of the new HBDI Prof. Dr. Alexander Rossnagel

To revitalize data protection after the pandemic has subsided

Since March 1st, 2021 I have held the office of Hessian Commissioner for

data protection and freedom of information. In this respect, the responsibility lies with

the period that the present 49th activity report of the Hessian

Data Protection Officer and the 3rd Activity Report of the Hessian

mandates for freedom of information covers, with the previous incumbent

Prof. Dr. Michael Ronellenfitsch. Since both reports but during my term of office

be published, I would like for these reports some – rather forward-looking

directed – considerations on the tasks and organizational development

of the Hessian Commissioner for Data Protection and Freedom of Information

hold onto.

The protection of the fundamental rights of persons affected by data processing

has gained importance and attention. Its importance increases

because digitization leads to more intensive processing of personal

gener data leads. Greater attention is paid to data protection because

the European data protection law new obligations of the persons responsible and

extended rights of the persons concerned also with effective action

and possible sanctions of data protection supervision.

Nevertheless, the implementation of data protection is becoming increasingly difficult and

causes new challenges for the Hessian data protection supervisory authority.

The main reasons for this are the following developments:

On the one hand, the risks for the fundamental rights to data protection and

informational self-determination qualitatively and quantitatively. The digital

le capturing of everyday life through the Internet of Things (e.g.

through networked automobiles, smart meters, smart homes and smart offices,

language assistants, health apps) and requires additional ones

Data. Virtual infrastructures (e.g. search systems, social media, cloud

Computing and exchange platforms) enable digital ability to act

ability, but at the same time the formation of intensive personality profiles. New

Methods of evaluating personal data (big data, artificial

Intelligence), allow new insights and conclusions, but

new ways of controlling behavior. The ones with digitization

Using the associated opportunities and avoiding risks requires a

data protection-compliant design of such information technology systems. This

applies both to companies - especially if they are data-driven

pursue business models. But this also applies to the administration – so far

they digitization for the additional collection of data on women citizens

and citizens uses.

On the other hand, digitization causes additional problems for those responsible

duties, entails additional requirements and requires additional ones

Attention. This means that large companies and administrations

rightly so. Small and medium-sized companies can easily do this

overwhelm. The demand for data protection obligations may, however, result

not lead to a reduction in data protection. Rather have to

data protection-compliant solutions are found that also include data protection in

small and medium-sized enterprises and in small communities.

Thirdly, global networking brings with it new challenges,

if it should not lead to a reduction in data protection. Here

the European Court of Justice gives the data protection supervisory authorities new

Tasks. According to its jurisprudence, every responsible person who

personal data in countries outside the European Economic

schaftsraum, ensure that there the protection of fundamental rights

related to the personal data in a comparable way

is guaranteed. This requirement is for transmissions to many states

a problem. For the United States, the Court has expressly stated that

because of the unlimited access possibility of the security authorities and

intelligence services and because of the lack of legal protection for those affected

People from Europe do not have a comparable level of data protection there.

This creates the new challenge of transferring data in

to stop the United States. Indirectly, the Court has set the objective

to reduce the existing dependency on providers from the USA and in

the Union to achieve the greatest possible digital sovereignty:

Those responsible may only use information technology that

enables us to meet data protection requirements. Without

Making companies and authorities incapable of working can only do this

be achieved if functionally equivalent alternatives become available in the internal market

the information technology systems from the USA are offered.

Finally, the corona pandemic has made the implementation of data protection

legal requirements made difficult. She forced and forces to be more social

Distance. And it forced and forces to take digitalization measures (like

Home office, video conferences, electronic file processing and others

electronic forms of communication) in order to still manage the social

life, economic exchange and public administration

to be right. Due to the extremely short response time at first

Lockdown in spring 2020 has many organizations, companies and

Administrations, universities and schools for available and functional ones

XXIV

To revitalize data protection after the pandemic has subsided

digital solutions are used - without paying attention to data protection.

As a result, data protection has been reduced significantly and across the board.

Nevertheless, the supervisory authorities have these solutions due to the

temporarily tolerated due to social emergency. If the Corona

Pandemic is over and normal social conditions are back

prevail, these digital solutions will lose importance,

but not disappear because they have largely proven their suitability

have. But then it will also be necessary to use all the solutions found

put to the test and to the data protection requirements

adjust gene.

The Hessian data protection supervisory authority must meet these challenges

set in the years to come. She hopes for understanding and

even the support of public and private bodies

in Hessen. Because: Private offers and public fulfillment of tasks are

dependent on trust. This can only be achieved through a data protection

fair digitization. Therefore it is necessary in the development of

Information technology projects as early as possible, a data protection-compliant

to strive for and in the case of (corona-related) undesirable developments

seek constructive corrections.

In order to be able to master these challenges, the supervisory
authority in Hesse requires a suitable framework for action. This
is mainly determined by the Europeanization of data protection. The
The European legal framework offers fundamentally helpful foundations and
instruments. In order to be able to use them properly, however, there are organizational
Adjustments in data protection supervision required:
In order to ensure uniform implementation of data protection in the Union,
the General Data Protection Regulation (GDPR) sees a narrow cross-border
increasing cooperation between supervisory authorities in the Member States
before. If a supervisory procedure affects several Member States, they should
supervisory authorities agree on the necessary measures. does not come
If an agreement is reached, the European Data Protection Board will decide
in the controversial supervisory procedure. It consists of the
data protection officers of the Member States. The committee is as well
independent of individual supervisory procedures, determined throughout the Union
increase, such as the abstract provisions of the GDPR in practice
are understand. Who wants to influence how data protection in the Union
future understood and practiced, must actively engage in cooperation
of the supervisory authorities and in the work of the European data protection
bring in committee. For this purpose, the Hessian Commissioner for Data
protection and freedom of information set up a staff unit. This must

However, according to the increasing work requirements,
be built if it is to reach its goal.

A second staff position was also changed in response to the
Implementing conditions of data protection set up. It concerns the
tiziariat. The DS-GVO has the tasks and options for action of the
supervisory authority expanded. Above all, it can be used to enforce
Data protection law in relation to non-public responsible arrangements
for data processing and in the event of a violation of data protection regulations
impose severe sanctions (fines). orders and fines
however, lead to legal disputes. From both instruments
can therefore only be used sensibly if the supervisory authority
is also able to succeed in the subsequent court cases
to perform. The judiciary supports the specialist departments with the decree
of orders and warnings, issues the fine notices itself
and oversees the judicial process. This is why this one is too
to expand the staff unit in such a way that an "equality of arms" with the legal
offices of the companies concerned.
For the exercise of fundamental rights and participation in the demo-
cratic decision-making is next to that in a digital society
Privacy of access to public information of particular
Meaning. This freedom of information has only been in law in Hesse since 2018
intended. Your practical uptake and fulfillment need to be
still developing in Hesse. Access to information is in the law for
intended for the state administration, but for the communities and districts
only if they apply the right to access information for their
public bodies have expressly stipulated by statute. have this
so far only a few municipalities and districts have decided. Here will be in
further discussions on the advantages and disadvantages of a

information claim to be kept. For the Hessian representative

for freedom of information is the further development and enforcement of the

information access to public authorities is an important task.

Finally, I would like to thank my predecessor, Prof. Dr. Michael

Ronellenfitsch, thank you very much for giving me such a

orderly house handed over to me by precautions and advice

made taking office much easier, but above all also for the fact that

he is still preparing the report for the last year of his term of office

accepted and hereby submits it.

Prof. Dr. Alexander Rossnagel

XXVI

I

First part

49. Activity report on data protection

49. Activity report on data protection

The Hessian Commissioner for Data Protection and Freedom of Information

Introduction data protection

1. Introduction Data Protection

Introduction data protection

In the foreword it was pointed out that when the new election of the

data protection officer whose term of office and the period of validity

he of the activity report are asynchronous. The submission time of the report

designates only the subject matter of the report. Relevant to data protection law

Event (violation and response) and report of this event fall without

not together. When you change office, this period of time increases

still. The processes relevant to data protection law, which are listed in the activity report

are to be dealt with, thereby completely losing their news value and
give the activity report a general balance sheet character.
The task of the activity report is not only to identify data protection violations
to reveal and a parliamentary control of the supervisory authorities
enable, but conversely also to point out equipment deficiencies,
which prevent them from effectively fulfilling their tasks (cf. Art. 52 para. 4
GDPR). In my opinion, there is a lack of equipment under the
Aspect of equality of arms with those to be controlled. Since in pri-
in response to our powers of intervention, legal and personnel
has been upgraded, it is essential that the tasks of the staff unit
Legal services by staff at the appropriate hierarchical level
be taken. So should a raising of the head of the legal department
be made. The same applies to the European area.
Here, the importance of European issues must also be
appropriate status of the representative of my
authority at European and international level.
In the European and international area, this can be achieved by
the combination with my deputy, which leads to classification according to B 4
(Annex I HBesG). Consequently, the classification in the
Legal department appropriate (at least B 3).
Incidentally, the activities of my authority were significantly affected by the Corona
affected by the pandemic. Here it was necessary to prevent a fait accompli
be created for the time after the pandemic has subsided. This sat
the functionality of my authority. Functionality has been
also constantly demonstrated when using the home office concept
placed. The preparations for the 50th anniversary of the Hessian

data protection law, which had already come a long way, unfortunately had to

be aborted. As it stands, we need preparations

extend to the 60th anniversary. The proper treatment of

Inputs also considering contact blocking requirements

may have contributed to those affected's limitations

accepted their informational self-determination with understanding.

4

Europe, International

2. Europe, International

Europe, International

2.1

Cooperation with the other European supervisory authorities

according to Chapter VII DS-GVO as well as participation in working committees of the DSK

and the EDPB (see also 47th and 48th activity report, Section 4.2.2 and

Clause 3.2)

With the entry into force of the GDPR, as in the 47th and 48th activities,

ness report, numerous innovations for the cooperation

of the supervisory authorities in Germany and Europe. The GDPR

obliges the European data protection supervisory authorities, in cases

to cooperate closely on cross-border data processing. To the

to cope with the additional communicative and organizational effort

results from the intensification of the cooperation, the HBDI has

In 2019, the European and International Office was set up

as a link between the HBDI and various external bodies

Hessen in Germany, Europe and the world.

All complaints, inquiries and reports received by the HBDI from

Violations of the protection of personal data according to Art. 33 DS-

GMOs are first checked in the specialist departments to determine whether

cross-border processing exists, which the obligation to

work with other European supervisory authorities. a border

According to Art. 4 No. 23 DS-GVO, there is more processing if

the controller or processor in several Member States

is established and processing in several of these establishments

takes place or if there is only a single branch in the EU, but

the processing has a significant impact on data subjects in more

than a Member State has or can have.

Process of cooperation and coherence according to Chapter VII GDPR

Not only since the GDPR came into force have there been complaints at the HBDI

there are also increasing numbers of complaints against Hessian companies and authorities

against companies based in other EU member states. After

with the DS-GVO newly introduced concept of the so-called one-stop shop

cross-border data processing, a supervisory authority (usually

the supervisory authority of the head office of the controller or

Processor, Art. 56 Para. 1 DS-GVO) as the lead supervisory

authority is the only contact person for the person responsible or

according to Art. 56 Para. 6 DS-GVO. That is, a company must

because of one and the same data processing only with one supervisory authority

deal with. However, this does not mean that the responsible authority

supervisory authority alone decides. Rather act alongside the lead

Supervisory authority also all other affected supervisory authorities at the

decision making with. "Concerned" are according to Art. 4 No. 22

DS-GVO all supervisory authorities of the member states, in their sovereign territory

the controller or processor is established, individually

affected persons ("data subjects") reside or with whom

a complaint has been filed. The lead supervisory authority

and the supervisory authorities concerned work in the cooperation process

closely together and try to reach a consensus (Art. 60 para. 1

GDPR). The lead supervisory authority examines the case and submits it

concerned supervisory authorities a draft decision (Art. 60 para. 3

sentence 2 GDPR). Those affected can object to this draft resolution

object to the supervisory authorities (Article 60 (4) GDPR). With insoluble

In the event of disagreement, the matter will be referred to the European

Data Protection Committee (EDSA) in the consistency procedure according to Art. 63 DS-GVO

submitted for a binding decision.

Cooperation, coordination and communication in cross-border

The administrative procedure involved is carried out electronically via the so-called IMI system

(Internal Market Information System)

system). Incoming to the European data protection supervisory authorities

Complaints and reports according to Art. 33 DS-GVO with cross-border

in a first step in a procedure according to Art. 56

DS-GVO to determine the lead and affected supervisory

authorities in the IMI system. The facts for the

other supervisory authorities in English (EDSA paper “GDPR in

IMI – User Guide For Supervisory Authorities”: “All cooperation procedures

should be documented in English.”) summarized and the

Presumably responsible and the presumably affected supervisory

hear to show off. The other supervisory authorities then have the opportunity

to review the case and appoint as lead or within one month

to report the relevant supervisory authority.

If it is determined in the Art. 56 procedure that the European lead

lies with the HBDI, the Office for Europe and International Affairs will transfer it

the complaint received by the IMI system along with other documents

the respective specialist department, which then after a thorough examination

of the facts processed the complaint and contacted the responsible

lic.

In the event that the leadership of another European

supervisory authority, transmits the Office of Europe and International Affairs

the complaint to the relevant authority for processing. For this must

the complaint and all other information necessary for processing

Locations and relevant information are translated into English,

since communication between the various supervisory authorities in

IMI system is in English.

Increased number of cases and increased examination effort

The number of complaints reported through the IMI system, Art. 33-

ments and official investigations increased in the reporting period in comparison

continued to increase compared to the previous year, see also Part I Clause 15.1, 17.1 and 17.2. In the reporting period

a total of 759 were from the European and International Office

Art. 56 procedure registered in the IMI system for a possible impact

or to check leadership. In 198 of these proceedings, the staff unit

Europe and International reported as “affected” to the HBDI, deals

subsequently with the content of the matter and is involved in the decision-

finding with. The HBDI is responsible for processing five further procedures

of the complaint as the lead supervisory authority. In addition

the Office for Europe and International Affairs 42 received at the HBDI

Complaints for further processing as lead management to other European

ische supervisory authorities. In these procedures, the HBDI acts as a

affected supervisory authority in the decision-making process and remains in the

so-called one-stop-shop procedure Contact person for the complainant

or the complainant and will provide information on a regular basis

the status of processing.

In the reporting period, 290 cross-border administrative procedures

room from the European supervisory authorities draft resolutions in accordance with Art. 60

Para. 3 sentence 2 DS-GVO in the IMI system, by the administrative department

Europe and International together with the respective departments in the

with a view to identifying any concerns and filing an appeal

were. In addition, the European and International Office has the other

submitted 22 of its own draft resolutions to the European supervisory authorities.

201 procedures in which the HBDI is involved as the supervisory authority concerned

was able to make a final decision in the reporting

be closed, including eight cases with Hessian leadership.

The number of procedures for mutual administrative assistance under Art. 61 DS-

GMOs continue to increase. During the reporting period, the Europe and

International 271 Requests for administrative assistance from other European supervisors

authorities and 15 of their own requests for administrative assistance to other supervisory authorities.

In the new year, the number of cooperations to be processed by the HBDI

tion procedures continue to rise. Not least because of the exit

Great Britain from the EU, which in some cross-border

Administrative procedure leads to the lead by the British

Data protection supervisory authority switches to the HBDI.

Binding Corporate Rules Approval Process

In addition to the cross-border ones to be processed via the IMI system

Administrative procedures is another focus of the activities of the staff

represent Europe and International in the review and approval of Binding

Corporate Rules (German: binding internal data protection regulations; in short:

BCR), which - also due to the so-called Schrems II judgment of the ECJ (ECJ,

Judgment of July 16, 2020, Case C-311/18) and the ineffectiveness of the EU-US

Privacy Shields – enjoying growing popularity as a transfer tool.

BCR are complex contracts with measures to protect personal

related data that a multinational corporation undertakes to comply with

is obliged to transfer personal data within the group of companies

so-called third countries (i.e. countries outside the European Economic Area)

to transmit, which in and of itself does not provide an adequate level of data protection

offer.

The BCR documents are processed in a Europe-wide cooperation

examined jointly by supervisory authorities of several Member States.

A supervisory authority acts as the lead or so-called BCR Lead

and coordinates the process. One or two more regulators

are supported as so-called co-examiners. In addition, all euro

European supervisory authorities in accordance with Art. 63 DS-GVO

Consistency mechanism to be included and opportunity for testing

and commenting on the BCR received before the EDPB issued an opinion

to this end.

Approval can only be granted if this opinion is positive

by the BCR Lead, which are then for the other supervisory authorities

is binding. All European supervisory authorities will thus become more involved

taken responsibility and duty. The aim of the process innovation

is a stronger standardization of the BCR, but with it a new and

increased examination effort for the supervisory authorities.

Over 100 BCR approval applications are currently pending. for 13

of these BCR procedures, the HBDI is in charge throughout Europe as the so-called BCR lead

8th

Europe, International

responsible. Of these, five BCR approval procedures were suspended as a result of the

Brexits from UK Data Protection Authority as new BCR Lead

accepted. The HBDI is in charge of 27 other BCR procedures

within Germany and took over the co-examination in two procedures.

Participation in committees of the DSK and at the level of the EDSA as well

Information transfer at the HBDI

About their tasks in cross-border administrative procedures and

the European and

international at national and European level various

working committees of the DSK or working groups of the EDPB. This includes the

Representation of Germany at the level of the EDPB in the Inter-

national transfers subgroup. The International Transfers Subgroup deals

deals with international data transfers and all topics and questions

that arise in this area. In addition to participating in regular

The staff unit is involved in subgroup meetings and BCR sessions

Europe and international issues at European level in various drafts

teams and task forces and reports together with colleagues

The LDA Bayern and the BfDI constantly submit to the German supervisory authorities

about the work of the subgroup and developments in the field of

European and international data protection law. The feedbacks

from the German supervisory authorities brings the HBDI as a country representative

then in turn enter into the discussions at European level. That's how it works

it z. B., influence on guidelines and recommendations to be adopted by the EDPB

to take lungs, which are then used for later supervisory activities

of all those involved become authoritative and trend-setting.

In addition, sifts through the information from the International Transfers Subgroup

the European and International Office but also all incoming mail

from the other subgroups of the EDPB (e.g. working papers and results

se, agendas and minutes), which the staff unit partly per

E-mail, but also electronically via Confluence, the collaboration tool of the

EDSA, reach. Monthly go from Europe alone from these subgroups

over 100 e-mails in the inbox of the European and International Office

one, which, after review and examination of the content, is sent to the responsible person

Technical presentations at the HBDI - be it for mere information and knowledge or

possibly further cause - must be forwarded. This

puts the specialist departments of the HBDI in a position to actively and creatively in

to bring in the work at European level and e.g. B. through cooperation

in ad hoc groups or early commenting on papers that are coming up

are in the draft stage, influence the opinion-forming process

to take in the EDPB.

The HBDI is also represented at the national level by the European and

Represent international issues in working committees of the DSK. That is the direction of the

nationwide working group organization and structure at the staff office

Europe and International. The organization and structure working group

supports the work of the DSK in important organizational issues

genes and develops concepts and processes for better integration of the

Work at German and European level. another topic,

which the working group is dealing with intensively are questions that arise from

of European cooperation according to Chapter VII of the GDPR,

including the concrete handling of these procedures in the IMI system. No

The staff unit is responsible for organizing regular working group meetings

Europe and International constantly the developments on national and

to be observed and evaluated at European level in order to help colleagues

and to be able to report to colleagues from the German supervisory authorities. There-

in addition, the European and International Office for the HBDI also takes

participate in the meetings of the Working Group on International Data Traffic. As

Representatives in the International Transfers Subgroup also join the HBDI

assigned a role to this working group that should not be underestimated.

Conclusion and outlook

In addition to the cooperation and coherence procedures according to Chapter VII DS-GVO

bundles a multitude of communicative and organizational tasks

Employee of the Office for Europe and International Affairs. Cooperation

with the other European regulators has entered the second year

largely implemented after the GDPR came into force. The steadily increasing

Number of cross-border administrative procedures and BCR applications

provides for the HBDI and the other German and European data

protection authorities but still a challenge and a

significant additional communication and organizational effort. Not

most recently due to the participation in working committees, drafting teams and tasks

Forces at national and European level, Britain's exit

from the EU and the effects that cannot yet be fully foreseen

effects of the so-called Schrems II judgment of the ECJ on data transfers to third countries

is in the coming years with a further significant increase in the

Consulting and auditing work for the Office of Europe and Inter-

to be expected nationally.

Europe, International

2.2

International Data Transfers - Privacy Shield Repealed, New

Standard data protection clauses in progress

With a landmark decision (C-311/18, Schrems II), the

ECJ for considerable uncertainty in data transfers to third countries

taken care of. To provide guidance and support to data exporters on this

to offer, the HBDI works as a member of the task force of the European
Data Protection Committee (EDPB) intensively on the development across Europe
coordinated recommendations for measures with which the instruments
for transfers of personal data to third countries
compliance with the EU level of protection for personal data
guarantee.
At the same time, the European Commission has drafts for so-called
Standard data protection clauses drafted and submitted to the EDPB for comments
submitted. The HBDI, as the permanent representative of the
Expert working group on international data transfers of the EDPB and
Member of the writing team involved.
A review of the EU-U.S.
Privacy Shields pending (report on the previous checks:
48. TB, Section 3.1, p. 7f; 47. TB, Section 4.2.1, p. 94ff. and 46. TB, Section 4.1, p. 55 ff.).
However, this became obsolete because the ECJ with its decision of
July 16, 2020 the decision of the EU on which the Privacy Shield is based
declared invalid by the European Commission. The consequences of this judgement
are very far-reaching and not only represent data transfers from the EU to the
USA in question: As a result, the ECJ burdens data exporters in the EU,
who wish to transfer personal data outside the EU,
enormous additional testing requirements. Where to date on a privacy
Recipient's Shield certification in the US or so-called
Standard contractual clauses (which are now standard data protection clauses under the GDPR
clauses) has concluded in order to ensure data protection in the
The ECJ is now demanding considerably more to take care of the recipient country.
Essentially, each data exporter must check in the specific case whether

the data recipient(s) in the third country are also able to

agreements made under the standard data protection clauses (or the

Agreements of another instrument for transfers of personal

transferred data to third countries according to Chapter V of the GDPR) actually

to comply with This means that it must be checked whether in a third country

there are laws that could prevent the data recipient from

to comply with individual agreements. Basically all

Legal regulations and practices in the third country in question, which through

the instrument for transfers of personal data to third countries

created level of protection could negatively affect. special focus

kus lays the ECJ on regulations, the public authorities of the third country

Grant access to the transmitted data. If such go beyond measure,

this is necessary and proportionate in a democratic society

is, or there are no enforceable rights for the data subjects

and no effective legal protection against such measures, the

data exporter to consider whether and how to cover these deficiencies in data protection

levels in the recipient country. To this end, the ECJ

called "additional measures" into the field, but without going into detail,

what these may consist of. However, he goes on to say that a transfer

where the data is exposed to such an identified risk that

cannot be brought to a level of protection by additional measures,

which is essentially equivalent to the one within the EU is not

allowed to take place and therefore avoided, suspended or

must be ended.

The ECJ places the burden of carrying out these tests first and foremost on the
data exporters. The EDPB works to support them in this
currently working on extensive recommendations for dealing with international
Data transfers taking into account those of the ECJ in its judgment
established requirements along with additional measures that
Supplement transfer tools from Chapter V DS-GVO to ensure compliance with the
to ensure levels of protection for personal data. These are
at https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/EDPB%20
Recommendations%2001_2020%20Supplementary%20Measures%20EN.pdf
find. Another paper that deals more closely with the requirements for state
access for monitoring purposes can be found here: https://daten-
schutz.hessen.de/sites/datenschutz.hessen.de/files/EDPB%20Recommendations%20
02_2020%20Essential%20Guarantees%20Surveillance%20Measures%20EN.pdf.
However, both papers are currently still in a public
hearing. The call for comments was in significant
scope followed. There are a total of 207 opinions on the first paper
received. They comprise about 1500 pages and are now closed
sift through and discuss in order to decide whether and to what extent the paper
should then be revised. All data involved are always
involve safety supervisory authorities, i.e. all 27 European and
including all German supervisory authorities. Their constant information
and involvement in European discussion and voting processes
belong in the field of international data transfers as well
Tasks such as the actual technical work in the European committees.

Europe, International

The European Commission (COM) also missed the verdict

revised the standard data protection clauses and submitted them to the EDPB

the procedure for the adoption of a new decision by the COM on the

acceptance: https://ec.europa.eu/info/law/better-regulation/have-your-say/

initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-

Clauses for the transfer of personal data to third countries.

In the development of the EDPB's opinion on these standard data

protection clauses, the HBDI is a member of the team of authors of the expert

group is also intensively involved at the European level. The ones from the EDPB

The adopted statement on this can be found at https://edpb.europa.

eu/our-work-tools/consistency-findings/edpbedps-joint-opinions_en.

The judgment and its implications will give the HBDI a whole

busy for a while. All existing guidelines and

other papers that are related to this at German and European level

Topic exist to revise. The verdict got some attention

excited, so that requests for advice and

complaints to be dealt with. Finally, the KOM already

announced that also all pre-existing adequacy decisions

(there are currently twelve, which can be found here: https://datenschutz.hessen.de/

data protection/international/appropriateness resolutions%C3%BCsse) to the

the standards set by the ECJ in its judgement. Also

EDPB statements are prepared for these checks

Need to become. After all, the submission of a draft stands for a

UK adequacy decision imminent.

The experts will also provide a comprehensive statement on this

of the EDPB to be drawn up.

13

General administration, municipalities

3. General administration, municipalities

General administration, municipalities

3.1

Data storage of swimming pool visitors

The storage of the name and address of visitors to municipal

Swimming pools is not legally permitted because the legislator for it

no legal basis was deliberately created due to the lack of a requirement

has.

When the outdoor pools reopened in Hesse at the beginning of summer,

I was asked by various Hessian municipalities whether they

collect the name and address of visitors to the swimming pools upon entry

and whether they would have to keep that data for a month, as is the case with the

restaurant operators is required.

In addition, I received a number of inquiries from citizens with which complaints

led to the fact that when making an appointment online for a swimming pool

visit not only name and address, but also date of birth and

telephone number were requested.

The questions seemed to be the same, but were legally closed

differentiate.

I had to inform the requesting municipalities that it was necessary for the survey

of the name and address of the swimming pool visitors and storage

of this data for a period of one month for the purpose of contact tracing

there is no legal basis; because unlike for restaurant operators and

Organizers of festivals contained the Corona contact and operating restrictions

There is no regulation under the ordinance for visits to swimming pools.

On the occasion of the inquiries from the municipalities, I had both with the

Hessian Ministry for Economic Affairs, Energy, Transport and Housing

contact with the Hessian Ministry for Social Affairs and Integration

included to discuss the issue. From the Ministry of Social Affairs

I was then informed that the legislator was aware of this

have waived the regulation for the collection of personal data,

because when visiting the swimming pool, you comply with hygiene regulations

feared no increased risk of infection, so that a requirement of

Contact tracing does not exist.

When booking appointments online, with the number of visitors in advance

should be controlled by swimming pools, I have the information

be of name and address for access control is considered permissible.

However, the storage of the data after the swimming pool

visit to be regarded as inadmissible. The collection of the date of birth is for

access control is not required and should therefore be omitted.

I have reported this to the pool operators.

3.2

Right to be forgotten – erasure of the names of

elected officials from meeting minutes under appeal

to the GDPR

Former municipal representatives are not entitled to have theirs deleted

Names from session logs. However, they must have a publication

of the minutes of the meeting with the mentioning of names on the internet.

A small inquiry was made in the Hessian state parliament as to whether former

According to Art. 17 DS-GVO, municipal representatives have a right to

that their names were taken from the minutes of meetings of the municipal

be deleted. The Hessian Ministry of the Interior and Sport has its

Answer coordinated with me.

This was preceded by a report in a Frankfurt newspaper that

in Friedberg a former city councilor with reference to the GDPR

had demanded that his name be removed from all minutes of the

City council meetings will be removed. The city is this desire

followed and has the name of both from all electronic documents

deleted, as well as blacked out in all meeting documents in paper form,

which meant a not inconsiderable effort. The Small Inquiry

the state government aimed to find out whether this request already

was asked more often and whether the state government sees a need for regulation here.

Regardless of the involvement in answering these little ones

A former city councilor also made inquiries to the HBDI

contacted another municipality, which also requested the deletion of his data

from old protocols with reference to the GDPR.

When evaluating the question of whether a right to erasure of personal

related information in the minutes of the meeting is between the

Minutes of meetings, located in the archives of municipal councils

are located and the publication of minutes of meetings on the Internet

differentiate.

As the HMDIS already did in its answer to the small inquiry (LT-Drs.

20/3107), there is an obligation to record the meetings

the municipal council from the Hessian Municipal Code (HGO). After

According to § 61 para. 1 sentence 2 HGO, the minutes must also expressly include the names

of those present at the meeting. As long as the logs are kept

must also be the names of the attendees at the meeting

retained as part of the records. After the storage

The logs are subject to the archiving regulations

kept. If permanent archiving is provided here,

the names of the session participants are also permanently archived. A extinguishing

There is no ruling from Art. 17 (3) lit. d GDPR. The archiving lies

in the public interest.

On the other hand, the minutes of the meeting can be published on the Internet

naming the meeting participants present no legal basis,

since the HGO does not provide for such publication. That's why one

Such publication only with an expressly declared consent

legally permissible in accordance with Article 6 (1) (a) of the GDPR. Should an Internet

publication without such consent, then the

Affected persons also have a right to erasure in accordance with Article 17 (1) (d).

GDPR to.

3.3

Special government mailbox

The establishment of only one special authority mailbox per municipality

is not acceptable under data protection law.

According to § 6 paragraph 1 of the regulation on the technical framework

of electronic legal transactions and via the special public authority mailbox

(ERVV) can be the authorities and legal entities of the public

right (PO box owner) for the transmission of electronic documents

a secure transmission channel, a special electronic authority

use the mailbox used to communicate with the courts.

The city of Frankfurt drew my attention to the fact that the

Hessian Center for Data Processing (HZD) per municipality only

want to set up such an official mailbox. The city has this from data-

from a protective law point of view and the establishment of a central

PO box at the main office for all other offices (social welfare office, youth welfare office,

health department etc.) referred to as a step backwards under data protection law,

since previously the offices could be addressed individually. Especially where special

sensitive data would be processed would be through the "central post office" at

special authority mailbox, a body gain knowledge of data that

had not previously been accessible to her.

I agree with this view and voiced my concerns

presented to the HZD. This argued that the restriction

to only one special electronic authority mailbox per authority

result directly from § 6 ERVV, since the authorities and "a"

P.O. Box will be spoken. Each authority only exists once and that

The concept of authority is to be interpreted in the context of the procedural rules, i. H.,

the term is to be attributed to the authority as a whole. In addition, it was stated

that with the establishment of several special authority mailboxes at one

Municipality the risk of incorrect addressing increases.

The HZD's interpretation of the concept of authority is data-

not legally tenable. I already have in my activity reports

stated in the past that from the point of view of data protection from

functional authority concept is to be assumed. I have this against him

Presented to the Hessian Ministry for Digital Strategy and Development

and in particular highlighted the following:

- Even with the interpretation of the authorities by the HZD

concept, the foreigners authority does not become the health authority or

the opposite. Both are responsible for their own data protection

Bodies (albeit under the umbrella of the city administration) that are completely

different legal bases work and accordingly

the requirements of Art. 5 Para. 1, 24, 25 and 32 GDPR

have that their data is not available without an appropriate legal basis

be transmitted to the respective office. However, this would be just for one

the case. All data went through the main office.

However, a city government is not exactly an informational entity.

Incidentally, I have made the Ministry aware that

the notice from the Federal Ministry of Justice that there is only one per authority

there could be a special official mailbox, by no means nationwide

will be followed, since both federal authorities and local authorities in

other federal states have long since had several special official mailboxes

were set up according to § 6 ERVV.

In any case, the federal government has regulatory competence for the municipalities

not to.

The Minister of State for Digital Strategy and Development had me between-

timely informed that in the federal states by an increasing

Discussion a change to the previous one, by the Federal Ministry of Justice

formulated position. For example, in justified

Exceptional cases and after the definition of uniform criteria, a deviation

from the "single mailbox strategy" should be considered.

Meanwhile, the Ministry informed me that, in principle, the institution

a special public authority mailbox per office is considered uncritical

and correspond to the so-called "functional authority concept". Which he-

setting the criteria for awarding several special electronic

Authority mailboxes for a municipality and the practical implementation

this award is currently being worked out.

3.4

Commissioning of external service providers within the scope of Section 6a (3) KAG

The commissioning of external service providers within the scope of § 6a KAG is subject

the general data protection regulations.

In the summer of 2020, several citizens came forward and complained about

a letter from their local government to introduce a recurring

running road contribution. In this cover letter, the citizens were

and citizens are asked to provide information about their properties and their concrete

to do construction. For this purpose, an attached questionnaire should be filled out

and to a private service provider commissioned by the municipality

be sent. The complainants had reservations about this

course of action and asked whether this course of action was legally permissible

and whether they are obliged to a commissioned service provider

disclose their personal information. In the example to me

sent seven-page cover letter no explanation was found

Procedure when commissioning the external service provider and also

no relevant data protection notice.

A basic option for commissioning external service providers

exists within the framework of the provision of Section 6a (3) of the Act on Com-

municipal taxes (KAG).

§ 6a KAG

(1) The fixing and levying of several taxes on the same taxpayer

concern can be summarized in one decision.

(2) A decision on taxes for a specific period of time may determine that

it also applies to future periods as long as the calculation bases and

do not change the tax amount. Tax assessment notices with permanent effect are official

to cancel or change if the obligation to pay taxes no longer applies or if the amount changes

of taxes changes.

(3) The municipalities and districts can in their fee and contribution statutes

determine that the determination of calculation bases, the calculation of taxes,

the preparation and dispatch of tax assessment notices and the receipt of the

to be paid by a third party commissioned to do so.

The third party may only be commissioned if the proper execution and examination

is guaranteed according to the regulations applicable to the municipalities and districts. The

Municipalities and rural districts can decide to carry out the tasks mentioned in sentence 1

also use the data processing systems of third parties.

The requirements result directly from the provision,

which the parties involved have to fulfil. On the part of the commissioner

Service provider must comply with the applicable regulations of the municipalities

and rural districts must be guaranteed and the commissioning municipality must

have formulated their fee and contribution statutes accordingly.

In addition to the requirements that result directly from the provision of

§ 6a KAG, require the corresponding data transmissions

between the municipality and the commissioned service provider to comply with data

protection regulations, insofar as personal data are processed there

be served. This does not necessarily have to be the case in the relevant

Facts should, however, personal data to the commissioned

service providers are transmitted. Therefore, here is an agreement to

Contract data processing is required by law in accordance with Article 28 of the GDPR. So far

the legal regulations are complied with, such a procedure is

Connection with the introduction of a recurring street contribution

basically legally permissible.

The further question was whether the citizens in a

such connection be obligated by the local government

can, the personal data directly to the commissioner

to transmit to service providers. This is not the case. Such a procedure

Rather, it requires the consent of those affected, since it is a legal obligation

for transmission only to the public body that legally

authorized to collect data. An immediate transmission to

a commissioned service provider can therefore only be offered as a supplement, not

but be required.

police, judiciary

4. Police, Justice

police, judiciary

4.1

Amendment of the Hessian Security Check Act

(HSÜG) – now: security clearance and

Classified Information Act (HSÜVG)

The Hessian Security Check Act (HSÜG) is in 2019

been amended (by law of December 11, 2019, GVBl. p. 406) and

is now called the Hessian security check and classified information

law (HSÜVG). As part of the public hearing in the Interior Committee

of the Hessian state parliament, I have a statement on the draft law

me submitted (committee proposal INA 20/10, p. 13 ff., on the draft law

to change the Hessian Security Check Act, LT-Drs.

20/1090) in which I raised various privacy concerns

have. However, these points of criticism were not taken up by the legislature.

In addition to the already discussed during the deliberations on the previous version of the

security review act expressed concerns about obtaining a

Schufa self-disclosure (now in § 10 para. 1a sentence 1 HSÜVG), which still

are always relevant, I have in this legislative process

with regard to the security check u. a. Criticism of the expansion of

Insight into websites and the publicly visible part of social networks

to persons involved (§ 10 Para. 1a Clause 3, § 11 Para. 2 in conjunction with Para. 1

Sentence 1 No. 17 HSÜVG). In particular, there is a lack of a resilient one

Justification for the extension to this group of people (in § 3 para. 3 sentence

1 HSÜVG, the persons involved are defined in more detail). In addition, neither

from the regulation formulated as an optional provision nor from the justification

to § 10 para. 1a sentence 3 HSÜVG reliable criteria can be seen, when from

which insight should be disregarded. In the explanatory memorandum to the bill

(LT-Drs. 20/1090, p. 14) it is only stated that the design

as an optional requirement to take account of individual needs and

Capacities in the inspection staff should serve.

21

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

§ 3 HSÜVG

(...)

(3) The security check according to §§ 8 and 9 (Ü2 and 3) should include:

1. the adult spouse of the person concerned or

2. the adult life partner of the person concerned

person and

3. the adult with whom the person concerned is in a long-term relationship

marriage-like or same-sex community (cohabitation).

(...)

§ 10 HSÜVG

(...)

(1a) The participating authority can also provide a data overview of the Schufa Holding

AG according to Art. 15 Para. 1 of the Regulation (EU) 2016/679 of the European Parliament

and of the Council of 27 April 2016 on the protection of individuals with regard to processing

personal data, free movement of data and cancellation of the policy

95/46/EG (General Data Protection Regulation) (OJ EU No. L 119 p. 1, No. L 314 p. 72, 2018

No. L 127 p. 2) from the data subject if there are indications of a possible

financial vulnerability exist. For persons within the meaning of Section 5 Paragraph 1 Clause 1 No. 3

to request this data overview in any case. The participating authority can

in addition to the data subject to the necessary extent of access to generally accessible information

own websites and the publicly visible part of social networks; at

Security checks according to §§ 8 and 9 (Ü 2 and 3) can also be granted this insight

of the person involved. […]

(...)

§ 11 HSÜVG

(1) The data subject shall state in the security declaration:

(...)

No. 17 Address of a generally accessible own Internet page, user name or

ID for public memberships and participation in social networks,

(...)

(2) If persons are included in accordance with Section 3 Paragraph 3 Clause 1, those in Paragraph 1 are also included

Sentence 1 nos. 5 to 7, 11, 14 to 17 and 20 mentioned data with the exception of the number of

specify children.

(...)

Furthermore, I have my doubts about the new regulation § 32a

HSÜVG presented, which the application of the Hessian data protection

and Freedom of Information Act (HDSIG) and the powers of the Hessian

representative for data protection and freedom of information

as well as special data protection regulations in the area of security

creates checks.

police, judiciary

§ 32a HSÜVG

(1) For the application of the provisions of the Hessian Data Protection and Information

freedom law, the following applies:

1. Section 1 (8), Section 14 (1) and (3) to (5) and Section 19 do not apply,

2. Sections 37, 41, 46 (1) to (4) and Sections 47, 48, 49 (1) and (2), 57, 59 and 78

apply accordingly.

(2) Any person can contact the Hessian representative or the Hessian representative

for data protection and freedom of information if you believe that the processing

processing of their personal data under this law by public or not

public bodies to have had their rights violated.

(3) The Hessian Commissioner for Data Protection and Freedom of Information monitors

in the case of public and non-public bodies, compliance with the applicable regulations

ten about data protection in fulfilling the tasks of this law. of control

by the Hessian Commissioner or the Hessian Commissioner for Data Protection and

Freedom of information is also subject to non-personal data in files on the

Security clearance when the data subject controls those related to them

Data in individual cases to the Hessian representative for data protection and

Freedom of information contradicts.

(4) Public and non-public bodies are obliged to inform the Hessian Commissioner

or the Hessian Commissioner for Data Protection and Information Security at the

to assist in the fulfillment of his or her duties. Her or him is particular

1. Information on his or her questions and inspection of all documents, in particular

in the stored data and in the data processing programs,

which are related to the control according to paragraph 2,

access to all offices at all times.

2.

This does not apply if the competent supreme state authority determines in individual cases that

the information or insight would endanger the security of the federal government or a state.

In particular, it is not understandable why the investigative powers

of the Hessian Commissioner for Data Protection and Freedom of Information in about

Paragraph 3 sentence 2 (right of objection of the person concerned) and in Paragraph 4 sentence 3

(Exclusion of investigative powers in individual cases by the competent authority

supreme state authority) restricted in this way as well as the powers of remedial action

limited to the complaint and warning according to § 14 Para. 2 HDSIG

be, para. 1 No. 1. When the investigative powers are restricted

It is essentially about the adoption of regulations from the

Section 24 (2) and (4) BDSG old version (see BT-Drs. 18/11325, p. 126). This

Regulations were also at the time of validity of the BDSG a. F. not without

Criticism (e.g. Dammann in Simitis, Federal Data Protection Act, 8th edition 2014,

§ 24 para. 25 ff., 39 ff. with evidence) and are present with regard to

the exclusion of investigative powers in individual cases in paragraph 4 sentence 3

has also been tightened (in § 24 Para. 4 BDSG old version the exclusion applied

e.g. not for the general obligation to provide support in paragraph 4 sentence 1).

As a result, there is no viable justification as to why such

Restrictions and restrictions on the powers of the Hessian representative for

Data protection and freedom of information are necessary here. Especially in this one

sensitive and important area of security clearances should be one

independent supervisory authority as one with effective powers

equipped data protection control authority can act.

4.2

Data protection checks in the police sector

In addition to the regular check of the anti-terrorist database (ATD), 2020

for the first time data protection checks by my authority at the Hessian

police to fulfill my new legal inspection obligations.

In the course of the amendment of the Hessian law on public

Security and order (HSOG) in 2018 are also new data protection

legal inspection obligations for my authority have been added. These new ones

Obligations for data protection control result specifically from § 29a HSOG and

apply to preventive police measures according to the catalog in § 28 para.

2 HSOG. To meet the legal requirements regarding the new inspection requirements

To meet the requirements, the responsible technical department was given an additional one

site equipped.

§ 28 HSOG

(...)

(2) Depending on the implementation of the specific measure, the

1. Measures according to § 15 paragraphs 2 and 6, in which processes outside of apartments

were recorded, the target person and the persons significantly affected,

2. Measures pursuant to Section 15 (4) the person against whom the measure was directed,

other monitored persons and the persons who use the monitored apartment

held or lived at the time the measure was carried out,

3. Measures pursuant to Article 15, Paragraph 6, in which events within apartments are recorded

were, and according to § 16 the target person, the persons significantly affected and the

Persons whose not generally accessible apartment was entered,

police, judiciary

4. Measures according to § 15a paragraph 1, 2 sentence 1, paragraph 2a sentence 1 and 2 as well as paragraph 3 the

shared the monitored and affected telecommunications, the user or the

user as well as the target person,

5. Measures according to § 15b those involved in the monitored telecommunications and

the information identifying the information technology system and the data on it

made not only fleeting changes,

6. Measures according to § 15c the target person, the persons affected and the information

to identify the information technology system and the changes made to it

not just fleeting changes,

7. Measures according to § 17 the target person and the persons whose personal

data has been reported

8. Measures pursuant to Section 26 contained in the transmission request pursuant to Section 26 (2).

Characteristics and the data subjects against whom further after evaluation of the data

measures have been taken.

(...)

§ 29a HSOG

The Hessian data protection officer leads without prejudice to her or his others

Tasks and checks At least random checks every two years

with regard to data processing in the case of measures to be logged in accordance with Section 28 (2).

and of transmissions according to § 23.

Upon request, the files on the events were presented to me for review

which I had previously used for random checks on two police chiefs.

services had been selected. The focus of each exam

were in addition to the substantive legal requirements of the measures

in each case also the authority to issue orders, the timely

termination of the measures and the handling of the legally regulated ones

Notification obligation according to § 29 paragraphs 5 to 7 HSOG.

§ 29 HSOG

(1) The data subjects receive information, notification or information regarding

the data processed about you in accordance with §§ 50 to 52 of the Hessian law

Data Protection and Freedom of Information Act, insofar as data processing is part of the

§ 40 of the Hessian Data Protection and Freedom of Information Act

takes place, and otherwise in accordance with §§ 31 to 33 of the Hessian Data Protection and

Freedom of Information Act and Articles 13 to 15 of Regulation (EU) No. 2016/679,

unless otherwise stipulated in paragraphs 2 to 7.

(...)

25

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

(5) If personal data were obtained through measures pursuant to Section 28 (2), the

the persons concerned designated there after the measure has been completed

to notify. Inquiries to establish the identity or address of a

person to be notified are only to be made if this is taken into account

the intensity of the intervention of the measure against this person, the effort for the

Determination of their identity and the resulting for these or other persons

impairments is required.

(6) A notification according to paragraph 5 is to be deferred as long as it

1. the purpose of the measure,

2. a criminal investigation following the triggering facts

treatment,

3. the existence of the state,

4. Body, life or liberty of a person or

5. Items of significant value whose preservation is necessary in the public interest

is, would endanger. If a V person or VE person is deployed

the notification only as soon as this is possible without jeopardizing the possibility of

further use of the V-Person or VE-Person is possible. The decision

the management of the authority or a

employees commissioned by them or an employee commissioned by them.

If the notification is deferred for one of the above reasons,

to document this. About the postponement of notification is the or

the Hessian data protection officer no later than six months after completion of the

measure and then at six-monthly intervals.

(7) There will be no notification according to paragraph 5 if this is in the overriding interest

of an affected person. In addition, the notification of a

and 5 designated person against whom the measure was not directed, refrain

if it is only marginally affected by the measure and it can be assumed that it will

not interested in notification. The decision to refrain from a

The management of the authorities or an employee commissioned by them shall be notified

or an employee commissioned by them.

(...)

As part of the audit, I checked the scope of the notifications

determined that the notifications after the completion of the measures

took i. s.d. § 28 para. 2 HSOG partly not to a sufficient extent

took place and did not always meet the requirements in terms of content. Also for

Notifications according to § 29 Para. 5 HSOG, § 29 Para. 1 HSOG applies, which is based on

the regulations on the rights of data subjects, such as the present one in particular

relevant provision of Section 51 HDSIG. Here I caused

that new patterns are developed, which will then be used in the future as part of the

notification of the persons concerned should be used.

26

police, judiciary

In addition, I have recognized that the documentation of the examination-relevant

Improve content in the files for data protection purposes

is. I have pointed this out to the relevant departments.

However, the evaluation of the test is not yet fully completed.

senior

In addition, I checked the anti-terrorist database again in 2020.

The exams covered selected police headquarters and that

State Office for the Protection of the Constitution in Hesse. subject of this year

The data records newly created in 2019 were tested. The control

did not reveal any faulty data processing or other abnormalities.

It was positive to note that the files were kept by the police and the

State Office for the Protection of the Constitution in Hesse, in accordance with our

beats from past exams and the files for the

data protection audit purposes are now better structured.

27

schools, colleges

5. Schools, colleges

schools, colleges

5.1

Documentation on exemption from wearing the mouth and nose mask

protection in school

Schools are faced with a variety of challenges as a result of the corona pandemic. That concerns

also dealing with schoolchildren who are through a medical

Certificate of the obligation to wear mouth and nose protection

have been freed. Represented with regard to the documentation of the exemption

I consider that a note in the student file about the submission

of the certificate is sufficient. I also don't think it's naming a diagnosis

necessary. The Hessian Ministry of Education has joined this

and inform the schools about it.

From the area of the State Education Authority (SSA) for the district and

the city of Kassel I received the first complaints from parents about

that schools issue medical certificates stating that they are exempt from wearing the mouthpiece

Copied nose protection at school and filed it in the student file

or also demanded the mention of a diagnosis in the medical certificate. appointed

the affected schools refer to instructions from the local SSA.

Courts keep diagnosis in the certificate and localization in the student file

for lawful

The SSA for the district had the instructions for the schools

and the city of Kassel on the basis of a decision by the administrative

richts (VG) Würzburg (Az.: W 8 E.10.1301 from 16.09.2020).

The administrative judges also considered it obligatory to provide a copy

to include the medical certificate as proof in the student file

also the naming of a diagnosis in the certificate. shared this legal opinion

a number of other administrative courts in other federal states. In addition

there were two decisions by higher administrative courts (OVG Münster from

September 24th, 2020, Az.: 13 B 1368/20 and VGH Munich of October 26th, 2020, Az.: 20

CE 20.2185) with identical content.

My legal opinion is supported by the Hessian Ministry of Education

divided

I myself and partly also other data protection supervisory authorities

however, contrary to previous case law, the following is different:

The legal basis for the obligation to wear a mouth and nose mask

Protection results from the Infection Protection Act and the respective

current state ordinance to combat the corona virus. In it will

expressed that the exemption by those affected is credible

is to do. This is done by submitting a certificate. In contrast

to the previously known court decisions, I consider the nominal

diagnosis is neither mandatory nor necessary. principal

and teachers are usually wealthy due to lack of medical

knowledge to not evaluate the diagnoses. This is too

not necessary, because this is not part of a school's task.

In addition, the principle of data economy i. S.v. Article 5 paragraph 1 letter c

to take into account. In addition, it is health data and therefore

to data of a special category within the meaning of Art. 9 Para. 1 DS-GVO.

That their processing in this specific case by an existing

public interest (§ 9 Abs. 2 lit. c DS-GVO) could be justified,

I can't understand that.

I also consider it disproportionate to provide a copy of the medical certificate

to locate tests in the student file. Of course the school has to

be given the opportunity to send the original of the certificate in an appropriate

to be able to see a form. If in a specific individual case on the part of

School if there are doubts about the authenticity of a medical certificate,

the further procedure must be coordinated with the state school authority. The

The certificate is submitted with details of the issuing doctor or

doctor documented. The HKM has a template for this in a letter dated

September 21, 2020 made available to schools as well as a general one

Instructions for dealing with medical certificates.

The quick coordination with the HKM has led to the fact that in Hesse

did not come to any administrative court decision that I know of

had to, which was based on the topic of mouth and nose protection. The

Schools have obviously adhered to the guidelines, so that we

few weeks after the first complaints no further cases to me

were brought up.

5.2

Use of video conferencing systems in schools

The use of video conferencing systems in schools raises data protection

common questions. In the spring of last year, as part of the

the first lock-downs for educational use were largely tolerated

pronounced almost all systems that I determined in August 2020

conditions until July 31, 2021. Until this one

The Hessian Ministry of Education is to launch a state-wide offer at this time

implemented for his schools.

School closures require quick action

Until the start of the first lockdown in March 2020, the use of

Video conferencing systems (VKS) for schools are not an issue, since they were in one at the time

specified framework, the lessons took place in classroom form. Only with the

government orders, because of the pandemic u. a. the schools too

close, considerations had to be made, the contact of the school
to maintain with the students in an appropriate manner,
to at least u. a. to submit tasks. In a hurry was now
searched for suitable VKS, with considerations regarding the data
protection were not a priority in many cases.
The Hessian Ministry of Culture (HKM) approached me and asked for
In view of the urgency of the matter and because of the lack of
Knowledge of many school administrations around data processing at the
Use of VKS for a pragmatic release of the products. The
Ensuring the school education and upbringing paired with
a completely unknown situation surrounding the pandemic development
then made me decide to use digital tools
to temporarily lower the level of data protection (see also the homepage of the HBDI, article
from March 23, 2020 – https://datenschutz.hessen.de/datenschutz/hochschulen-
schools-and-archives/information-on-digital-learning-and-the-digital). To-
I had a temporary toleration of almost all VKS
Pedagogical systems based on art. 6
Paragraph 1 lit. d and e pronounced. I deliberately refrained from doing so
stringent requirements through the unpredictable situation for the schools
complex data protection regulations are becoming even more difficult
permit. At the same time, I was aware that the mission in particular
US products could be conflicted because of their
Data protection compliance no statements could be made. That is
there were indeed critical voices from teachers and parents.

Overall, I see myself in my assessment and the resulting

derived guidelines for action confirmed.

Toleration is extended with conditions

The data protection-compliant, nationwide offer I demanded for

the schools, which the HKM has made available and on the

Open source software BigBlueButton based, could until the beginning of

new school year cannot be realized. Therefore, the ministry resigned

approached me again and asked for the extension of the toleration phase.

I have complied with this request and the toleration until July 31, 2021

extended. However, I have attached conditions to the extension

(For details, see the HBDI website – https://datenschutz.hessen.

de/datenschutz/hochschulen-schulen-und-archive/hbdi-duldet-%C3%BCtransition-

show-the-use-of).

The HKM is now required, as part of a Europe-wide tender

a VKS based on the open source application BigBlueButton (BBB)

to be established, which should be docked to the Hessian school portal.

It can therefore be assumed that the schools in Hesse will

year 2021/22 will have a data protection compliant VKS. Think

Support in the implementation of data protection requirements

I have promised.

A digitization standard has been needed for a long time

I have repeatedly pointed this out to the HKM in the past

made that a legal basis for the use of digital tools

is urgently required by the school. Unfortunately, you have my information until-

not been implemented for a long time and the Hessian school law is not about a digital

lization standard added. School must, however, within the framework of its pedagogical

leeway to be able to, on the basis of a

resolution of the school or teacher conference according to their own needs

oriented path to digitization. Are the legal ones

and organizational prerequisites are in place for this, is the collection

the consent of students or parents who have previously

is mandatory, then no longer required. However, the school must

Ensure data security and the participation of all those affected.

5.3

Official e-mail addresses for teachers

One of the demands I have made for years to improve data

protection in schools is the Hessian Ministry of Education (HKM)

complied with in the reporting year. The introduction of official e-mail addresses

for the Hessian teachers significantly improves their work situation

and makes their data processing more secure.

A business e-mail account with the name of the person concerned

is established in almost all areas of public administration.

Since then, teachers have been an exception. Maybe this was

due to the special work situation of the teachers, who have no

job in the traditional sense and essential activities,

such as B. the preparation of lessons or correction of exams, in the domestic

common area. In any case, the official e-mail account was over

for many years and despite my repeated interventions for the HKM

no problem. Therefore, it was partly the school authorities that gave the employees

provided school-related e-mail accounts or the schools

set up e-mail addresses for the teachers themselves via a provider. In

not a few cases, however, the private e-mail account was also used: The

Mixing of private and business e-mails was unavoidable

and contained potential data protection risks.

The technical implementation process is demanding

Such a project, namely setting up almost 70,000 e-mail addresses

ten, is technically and organizationally enormously complex. Although from mine

Not required on the side, the HKM commissioned the state service provider

Hessian Center for Data Processing (HZD) with the implementation of the

project. Additionally required human resources were

nisterium provided.

In a brief summary can be the procedure for creating

of a business e-mail account as follows:

If a teacher is newly hired, they state their personal

data with you. With the delivery of the employment contract, the hiring

process initiated in personnel administration, in which a responsible

Employees the stored information partly manually as a master data record

in the HR database of the State of Hesse (SAP HR). The

The master data record forms the basis for the digital identity of the employee

and has a unique identity feature with the personnel number

(Unique Identifier), which will be used to identify the new teacher in the future without any doubt

can be identified.

After that, the data integration system creates a new user account for the
teacher in the user administration (school active directory), which u. a.
serves as the basis for later authentication of the teacher as soon as
it logs into its mailbox via the URL.
In the mailbox environment, the data integration system sets a disabled
RAD account (Resource Active Directory account) and a linked mailbox
which is linked to a specific account in the user management.
This ensures that the teacher is correct when logging in
authenticated against their account and connected to their email inbox
becomes. As soon as the information in the user administration and in the post
professional environment have been implemented, the new e-mail address, which is one
central naming convention follows, with the user account through the data
integration system synchronized. Then the new teacher
communicated the data of their mailbox including the initial password.
The description only applies to the case constellation "New appointment of a teaching
power". Similar complex steps must be taken for teachers who are already employed
be carried out, but also in the event of a name change or
retirement from service. With the help of two-factor authentication
the teacher can activate their mailbox. For this
However, the private end devices must be used as well as for
the use of the mailbox.
Acceptable use policy defines rights and obligations
A usage guideline drawn up by the Ministry specifies the
maintenance of official e-mail accounts. First of all, it is stated that
the use by the teachers in the official context is obligatory.
Regular retrieval and thus acknowledgment is also more detailed

emails set. The use of the teacher's private end devices is fundamental

additionally permitted under certain technical conditions. untouched

however, the general data protection problem remains

the so-called Bring Your Own Device (BYOD), i.e. the use of private

End devices for the official area. The digital

pact and the plan to equip teachers with official end devices,

also eliminate this data protection deficit.

34

schools, colleges

The storage and transmission of personal data via the

official e-mail address is only in compliance with the applicable for schools

permitted by data protection regulations. It is only allowed within the framework

of the official task, as far as it is for the respective

pursued official purpose is required. Particularly sensitive personal

Related data according to Art. 9 DS-GVO may not be used as content or attachment

be sent in an e-mail, provided they are not encrypted.

This applies to information about health and disability, including data

regarding special educational support, origin, religion, political

or ideological beliefs, sexual orientation, trade union

affiliation. The same applies to personnel file data and others

Personal data subject to a high level of protection.

Are used for the use of the official e-mail address under No. 8

uses private end devices under the conditions specified in this guideline,

may then, according to Section 83 (1) and (7) HSchG and Section 1 (5) and Section 3

of the regulation on the processing of personal data in school

only the personal data specified in Appendix 1 Section A 6

processed by students and their parents. Data

with a normal protection requirement can therefore with the official

E-mail address to be communicated.

The guideline also states that an evaluation of the

fallen log data for reasons of data and system security,

of system technology (e.g. for troubleshooting and tracking) and for

Abuse control is done. The evaluations are event-related

instead of. The query and evaluation of the data is carried out using the Hessian language

Ministry of Education, for example, if there is a suspicion that a

There is access for unauthorized third parties ("hacking"). The evaluation can

specific case of suspicion also by order of the department head

take place. The staff representatives and the official data protection officers

are to be involved in this case. In addition, an evaluation

possible at any time with the consent of the person concerned. The reason for

the evaluation and its result must be documented in a comprehensible manner.

Additions that I had thought necessary were made by the Ministry

included in the directive. By February 2021, the process for

Introduction of the official e-mail address for teachers to be completed.

transportation

6. Transportation

transportation

6.1

Data protection incident at the service provider of transport associations

Customer data from the so-called blocked lists of the transport associations

retrievable on the Internet – data leak closed, required technical

organizational measures taken and affected persons informed.

During the reporting period, I was notified of a personal protection violation

data according to Art. 33 DS-GVO from several transport associations

reported. Other data protection supervisory authorities have also been

of the transnational transport associations. background

of the reports was an unintentional publication of personal

pulled data on the Internet in relation to so-called blacklists. With these

blacklists belonging to the mobile ticketing system are the

Passenger data in connection with the blocking of user accounts.

The blocking of a user account can, for example, be the result of an unsuccessful

dunning process in the event of non-payment of purchased tickets. The blocking of

User accounts prevent the purchase of tickets and new registrations

with the same data.

The customer data was due to a configuration error of a service

ters (processor) for several years over the Internet under one

Web address that is not publicly known can be called up without access protection. The

However, the web address could not be found with common search engines.

The service provider discovered the error himself and those responsible

Transport associations informed accordingly. In direct response to the

Identification of the incident was the possibility of access via the Internet

disabled and the direct violation of the protection of personal

data thus turned off.

Whether the data leak was actually exploited by unauthorized access,

could not be clarified for the entire time of exposure, but could

cannot be excluded either. The one made by the service provider

However, analysis of the available log data has no indication of access

arise from third parties. Also, no other indications of an abusive

use of the personal data can be identified.

As a reaction to the report, my employees have further technical

cal tests carried out. The knowledge gained in this way was

those responsible together with the questions that have arisen

notified and they were invited to comment.

As a result, there was an extensive exchange of information between

the person responsible and the processor on the one hand and

n employees on the other side. Here were about the actual

Questions that go beyond the infringement with regard to the underlying

ing IT infrastructure, the associated IT systems and the means of these

implemented IT services discussed. In addition, the associated

development, operation and maintenance processes in the considerations

included.

In the course of clarifying the facts, it turned out that a project for

comprehensive revision and improvement of the processes even before the

Personal data breach identification initiated

had been. In this respect, the identification of the violations of protection

personal data is not the cause, but the consequence of the initiated

project. An improvement in the periodic review process,

Assessment and evaluation of the technical and organizational measures

measures to ensure the security of processing pursuant to Art. 32

Paragraph 1 lit. d GDPR was also the focus of the project. This project

had not yet been completed during the period of my exams. The planned one

The further course of the project was presented to me in the form of a roadmap and

Explained within the framework of an appointment with all those involved.

In addition to resolving personal data protection violations

data I was able to convince myself that the

bünden and their processors have taken the path far beyond that

concrete addressing of violations of the protection of personal data

data goes out. The measures taken seem appropriate to me

to ensure the security of processing within the meaning of Art. 32 DS-GVO

to be improved comprehensively. I intend to give myself

Time from the successful implementation of the other planned measures

to convince.

Overall, I was able to determine that the notification pursuant to Art. 33 DS-

GMO underlying breaches of protection have been remedied and

that a repetition of these violations is not to be expected.

Those affected by personal data breaches

After the risk assessment had been carried out and after

Utilization of my advice by the transport associations according to Art. 34

DS-GVO notified if they could be identified. Additionally

the transport associations published a corresponding press release.

transportation

6.2

License plate recognition in publicly accessible parking garages

The use of license plate recognition systems in parking garages can

compliance with certain requirements may be permissible.

In 2020, I received complaints from citizens that increasingly

Parking in the public car parks automated number plate recognition

solution is introduced instead of the paper parking ticket. This approach

violate data protection, because parking with a parking ticket is a data protection

gentler alternative. As a further argument for inadmissibility

automated license plate recognition, the case law of the

Federal Constitutional Court (BVerfG decision of December 18, 2018 - 1 BvR 142/15

(License plate checks 2)) for automated license plate checks

reported by the police.

During automated license plate recognition, video cameras are switched on

installed at the entrance and exit of the car park. These cameras will

operated with software that automatically recognizes the license plate number

and saves it along with the entry and exit times. The driver

or the driver and passengers are not captured by the camera. In the

Exit becomes the recorded number plate after paying the parking fee

recognized and the exit barrier opened.

Between the person parking and the operator of the car park is through

factual behavior (parking) concluded a parking contract. The parking time

determines the parking fee to be paid. The automated number plate recognition

This is primarily used by the car park operators to record the parking time

and used to prevent parking time fraud.

This should also speed up the entry and exit processes.

Processing of personal data – a license plate is

according to § 45 S. 2 StVG a personal date - is according to Art. 6 Para. 1

S. 1 lit. b DS-GVO permissible if they are used to fulfill a contract with the

concerned is required.

When using the automated identifiers, the complainants

character recognition systems on the point that the necessity

due to an alternative method of parking time recording using a

paper parking ticket would be negated.

Which data processing is required to fulfill the contract,

is primarily determined by the content of the contract and the purpose of the contract

certainly. The parking time as a basis for calculating the parking fees

must be unequivocally recorded. But also the specific detection method

must be required within the meaning of this provision. The person responsible may

no milder, but equally suitable and reasonable detection method

method are available. In this context, a trade-off must be made

between the right to informational self-determination of the parker

and the interest of the car park operator, a contemporary, efficient and

to offer a competitive product. Also the technological one

Progress and the latest state of the art must be included in this consideration

refer, which does not mean that what is technically possible is operational

is. In any case, proportionality must be maintained.

The interest of the car park operator in optimizing the operational process,

better fraud prevention, less administrative effort and customer-friendly

easier billing in the event of loss of the parking ticket outweigh this

Interest of the parkers in the non-recording of their license plates

View, however, only if the recorded number plate after completion

the parking process is irretrievably deleted.

The inadmissibility of license plate recognition does not follow from the

jurisprudence of the Federal Constitutional Court.

There was a large number of road users without a specific

there was a suspicion of this, using the automated license plate

trolls are compared with the wanted list in general and regardless of the cause.

In the specific case, however, the license plate recognition takes place on an event-related basis

connection with the fulfillment of the placement contract and only applies to

parking ends.

In all the cases I have, I have one to create transparency

prompt notification of the license plate recognition taking place.

This is determined depending on the actual circumstances. At the latest at the

Entry into the underground car park must be via the automated license plate

be informed. A note only at the ticket machine fulfills this

requirement not. I recommend, due to the difficulty in recognizing the

Information signs while driving and the limited capacity

due to the focus on traffic additionally on the internet site

to place a corresponding notice in the parking garage.

A possibility of turning as an indispensable prerequisite for use

technology, on the other hand, is not required of me.

Subject to the irretrievable deletion of the recorded identification

sign and taking other, in particular by Art. 32 DS-GVO

required measures, the use of automated license plate

be designed in compliance with data protection regulations.

40

transportation

6.3

Access to data only on the basis of legal

retention periods are maintained

The exclusion of the right to information in relation to such personal

Genetic data that is subject to a retention obligation is not absolute.

Rather, it is subject to the proviso that the provision of information

would require disproportionate effort in the specific case and a

Processing for other purposes through appropriate technical and organizational

satirical measures are excluded.

As part of the provision of information in accordance with Art. 15 DS-GVO, the reporting

period before that responsible person personal data, due to

were held up by § 257 HGB, not included in the information letter

had taken. This was justified by the fact that in this regard according to

§ 34 para. 1 BDSG is exempt from the obligation to provide information.

Furthermore, an energy supplier shared within the framework of the provision of information

according to Art. 15 DS-GVO, all persons requesting information that it

could be that further personal data due to legal

Storage regulations are stored and their provision of information

is refused due to the disproportionate effort.

§ 34 BDSG releases those responsible from their obligation to provide information

Art. 15 GDPR. The regulation age relevant for this activity contribution

native of paragraph 1 number 2 a gives the data processing body the

Possibility to refuse the provision of information regarding the data that

are only stored because they are due to legal or statutory

moderate storage regulations may not be deleted. alone

However, the fact of storage due to a retention obligation

not automatically to restrict the provision of information. The grant

The information can only be refused if you have an unreasonable

would require a lot of effort, both technically and organizationally

Measures have been taken that require processing for other purposes

exclude. Precisely these requirements regulated in the second clause

are often not taken into account in practice, since it is mistakenly assumed that

that these only apply to the regulatory alternative of paragraph 1 number 2 b.

The consideration of the following aspects in connection with the information

refusal according to § 34 BDSG I was asked:

– A statutory or statutory retention requirement

obliges the person responsible to store personal data.

The most common legal storage regulations are § 257 HGB

and § 147 paragraph 3 AO.

In parallel, Art. 17 Para. 3 lit. b GDPR (and Section 35 Para. 3 BDSG

for contractual and statutory retention requirements) in the event

the existence of a storage regulation is an exception to the law

for the deletion of the data subject.

- The storage of personal data takes place only on the

Basis of this retention policy.

This excludes the application of this exception,

if the storage of the data also serves another purpose or

the retention period has already expired.

– The person responsible represents a disproportionate effort for the

issuance of the information.

In doing so, the effort involved in providing specific information must

tion interest of the person entitled to information in a disproportionate manner

predominate. This consideration is fundamentally carried out by the person responsible

made with every request for information. In similar cases

it can be done once and then only has to be documented once

become.

In favor of the data subject are when determining the effort

also to take into account the existing technical possibilities,

blocked and archived data of the person concerned during the

future grant available (BT-Drs. 18/11325 p. 104).

The data protection supervisory authority can determine the existence of the disproportionate

fully checked with moderate effort.

– There must be technical and organizational measures which

prevent processing for any other purpose.

It is determined which measures are to be taken in detail

according to the type of data stored and the circumstances of the storage

security. Examples of action is the leadership of separate

databases (productive database and locked storage

information) and limited access rights.

– The factual and legal reasons for the refusal to provide information

must be documented in a comprehensible manner and

may be made available to the data protection supervisory authority.

– The person responsible must provide the data subject with the relevant reasons

for the refusal to provide information, unless through the notification

the purpose pursued with the refusal to provide information would be endangered.

The bodies responsible for providing information were asked to

requirements and adapt their practice.

The energy supplier in the above Fall was asked to change his practice

and only to those requesting information towards the information request

42

refusal to assert whose data is actually due to the storage

compliance obligations are held up and where disproportionate

Effort could be demonstrably determined. Also he was on his

obligation to justify pointed out.

transportation

43

Employee data protection, social affairs

7. Employee data protection, social affairs

Employee data protection, social affairs

7.1

Biometric recording of working hours using fingerprints

Those responsible who oblige their employees to participate in systems

who record the time by means of fingerprints in order to

to prevent use and tampering are against the regulations

of the DS-GVO and must therefore be subject to orders within the meaning of Art. 58 Para. 2

DS-GVO and expect sanctions according to Art. 83 Para. 5 DS-GVO.

During the reporting period, I received several inquiries and complaints

ranges dealing with the lawfulness of the processing of biometric data

deal in employment. So turned at the beginning

of the year two employees of a small medium-sized company

independently to my authority and reported on the use

of a working time recording system using fingerprints in their company

employer. The complainants asked me whether the use of a

such a system is permissible under data protection law without their consent.

I took the complainants' inquiries as an opportunity to

to listen to those responsible and to use the biometric work

time recording system in his company. In my

hearing letter I informed the person responsible about my fundamental

additional concerns about the use of biometric time tracking

systems. I asked him to give me the purpose and legal basis for

communicate the data processing procedure.

When I was heard, the person responsible said that he was in favor of the

Decided to introduce the system after it was at the earlier im

Deployed time recording system repeatedly to abuse and

manipulation by individual employees. To remedy here

to create - which is not least in the interest of law-abiding employees

required - a tamper-proof system had been introduced.

Due to the stated purpose, the person responsible represented the

Opinion that as the legal basis Art. 9 Para. 2 lit. b DS-GVO for

turn because the use of the biometric time recording system

required to exercise rights under labor law.

During the examination process it became apparent that the use of the biometric

rule time recording system in the described embodiment against the

GDPR violated. I have therefore informed the person responsible that I

intend to use my powers under Art. 58 Para. 2 DS-GVO

close. Specifically, I considered the person responsible

to instruct the processing method biometric timekeeping

by means of fingerprints by obtaining effective declarations of consent

to bring the employees' genes into line with the GDPR, cf. Art. 58

Paragraph 2 lit. d GDPR, or to impose a ban, cf. Article 58 Paragraph 2 lit. f

GDPR. In addition, I have informed the person responsible that

due to the identified violations of the provisions of the GDPR

Sanctions according to Article 58 Paragraph 2 lit. i i. In conjunction with Article 83 Paragraph 4 Letter a, Paragraph 5 Letter a

GDPR must be checked.

The person responsible then informed me that he

drive biometric time recording set and through an RFID

replaced the time recording system.

My decision was based on the following questions and considerations:

I. What are biometric data within the meaning of Art. 4 clause

14 GDPR and these are special

personal data within the meaning of Art. 9 DS-GVO?

The European legislator has introduced the concept of biometric data in

Art. 4 No. 14 GDPR defined. Biometric data are included hereafter

personal data obtained through special technical processes

the physical, physiological or behavioral characteristics of a person

natural person who uniquely identifies that natural person

Enable or confirm person, such as facial images or dactylosco-

physical data (procedure for evaluating fingerprints). Typical

are personal characteristics within the meaning of Art. 4 No. 14 DS-GVO

like fingerprint, iris, retina, face, hand geometry or even that

palm vein pattern.

Art. 9 Para. 1 DS-GVO contains a general ban on processing for

special categories of personal data. This includes after

The wording of the regulation also includes the biometric data described above

to uniquely identify a natural person.

II. Biometric recording of working hours using fingerprints –

How does this work?

With the term fingerprint, the imprint of the so-called papillary ridges

described on the end phalanx of a finger. These papillary ridges can be

differentiated by various features: basic pattern, rough features

male, finer features such as forking and line endings (so-called minutiae)

and pore structure.

Due to the different characteristics as well as their individual

distribution is based on the uniqueness of each person’s fingerprint

went.

If the fingerprint is to be used - for example for recording working hours -

This usually means that using a fingerprint reader initially

fingerprint analysis is performed. Here the minutiae

filtered out. Using special algorithms, the minutiae are converted into a

mathematical form (feature vector 1). The feature vector 1

is then saved, e.g. B. in a database or on a

chip card. There is no specific fingerprint from feature vector 1

more reconstructable. If the fingerprint is then read in again

imprint, the system calculates a feature vector based on the minutiae

2 and a comparison value (threshold value) between feature vectors 1 and 2.

Exceeds the calculated comparative value of the two feature vectors

a certain degree of coverage, the person is recognized and the recording

planning of working hours started or ended using a fingerprint.

The position paper contains detailed information on this topic

on the biometric analysis of the conference of independent data protection

Commissioned by the federal and state governments from April 3rd, 2019, which is about the

DSK website at https://www.datenschutzkonferenz-online.de/media/

oh/20190405_oh_positionspapier_biometrie.pdf.

III. Why does the biometric recording of working hours using

fingerprint in the underlying case against the

Provisions of the GDPR?

1. The reservation of permission and the prohibition principle of the GDPR, see Article 5

Paragraph 1 i. In conjunction with Art. 6 (1) GDPR and Art. 9 (1) GDPR

Art. 5 Para. 1 lit. a to f DS-GVO describes the principles for the processing

processing of personal data. According to Art. 5 Para. 1 lit. a DS-GVO

personal data lawfully, fairly and fairly

and processed in a manner that is comprehensible to the data subject

(“lawfulness, fair processing, transparency”).

The regulation of Art. 5 Para. 1 lit. a DS-GVO determines that the

Processing of personal data only if there is a legal

permit is permissible (so-called reservation of permit). The rule

of Article 6 (1) lit. a - f) GDPR contains the permissions that

can justify the processing of personal data.

For the processing of special categories of personal data, where-

down also biometric data within the meaning of Art. 4 No. 14 DS-GVO fall,

the legal requirements are even stricter: Art. 9 para. 1 sentence 1 DS-
GVO prohibits the processing of special categories of personal data
data (prohibition principle). A final list of exceptions
of the ban on processing contains Art. 9 Para. 2 DS-GVO.

Based on the case described, it follows that - if for the
biometric time recording system using fingerprints at the responsible
Literally no exception of Art. 9 Para. 2 DS-GVO applies - the
use of the system is prohibited, see Article 9 (1) GDPR.

2. Why are the prerequisites for an exception in the sense
of Art. 9 Para. 2 DS-GVO i. in conjunction with Section 26 (3) sentence 1 BDSG?

As already mentioned at the beginning, the person responsible within the framework of
Hearing procedure submitted that he was in favor of the introduction of the system
tems decided after it was used by the one previously in use
Time attendance system repeatedly subjected to abuse and manipulation
individual workers came. To remedy this - what
not least in the interest of law-abiding employees -,
a tamper-proof system had been introduced.

Due to the stated purpose, the person responsible represented the
Opinion that as the legal basis Art. 9 Para. 2 lit. b DS-GVO for
turn. The provision contains an exception to the prohibition of
Processing of special categories of personal data, e.g. for the
If the processing is necessary for the person responsible to
can exercise the rights to which he is entitled under labor law. through the in
The addition contained in the provision "insofar as this is required by Union law or the

law of the member states (...) is permissible" makes the European law
lender clearly that Art. 9 (2) (b) GDPR is a Union law or
member state regulation required. The rule is in itself
therefore no legal basis for the processing of special categories
personal data allowed.
For the area of employee data protection, such a rule contains
However, § 26 Para. 3 Sentence 1 BDSG applies. According to the wording of the provision, the
Processing of special categories of personal data within the meaning
of Art. 9 Para. 1 GDPR for employment purposes
Among other things, permissible if they are used to exercise rights under the
labor law is required and there is no reason to believe that
the legitimate interest of the data subject in the exclusion of
Processing predominates (cf. also BT-Drs. 18/11325, 102).
48
Employee data protection, social affairs
On the one hand, the concept of necessity is central here: According to the will
of the German legislator are part of the necessity test
the affected fundamental rights positions and conflicting interests
to weigh up the production of practical concordance and to reach a balance
bringing together the interests of the controller and those of the processing
affected persons as far as possible (BT-Drs. 18/11325,
101). This requires an examination based on the scale of the proportional
principle of responsibility, which in turn presupposes that on the part of the responsible
lichen a legitimate purpose is pursued, the processing procedure for the
Realization of this purpose is suitable and it is the mildest of all
means that are equally effectively available (cf. BAG, decision

from April 9th, 2019 – 1 ABR 51/17, 39 = NZA 2019, 1055 (1059)).

In addition to the proportionality test in the context of necessity

there must be no reason to assume that the interests worthy of protection

the employees concerned protect the interests of the person responsible

predominate (BT-Drs. 18/11325, 102).

Only if the above conditions are met can the

Processing of employee fingerprint data for the purpose of

Working time recording on the legal basis of § 26 paragraph 3 sentence 1 BDSG

be supported. Whether a biometric recording of working hours at all

can meet the requirements of Section 26 (3) sentence 1 BDSG is questionable.

As far as the biometric recording of working hours by means of fingerprints

Fulfill the purpose of preventing the manipulation of timekeeping data

should, the requirements of § 26 paragraph 3 sentence 1 BDSG are already in a

Overall view with § 26 paragraph 1 sentence 2 BDSG not fulfilled.

Although the recording of working hours may imply the exercise of rights arising from

serve employment rights, cf. § 26 paragraph 3 sentence 1 BDSG i. V. m. § 611 a paragraph 1 sentence 1

and 2 BGB. As far as the employer the biometric recording of working hours

by means of fingerprints, but precisely for the purpose of preventing

Introduces nipulation of time tracking data, it encourages adoption of the

employer revealed that the employees of his company committed criminal offenses

commit, namely the offense of working time fraud according to § 263

Comply with the Criminal Code (also LAG Berlin-Brandenburg, judgment of 4.6.2020 - 10

Sa 2130/19, 71). For the processing of personal data for

Section 26 (1) sentence provides for coverage of criminal offenses in the employment relationship

2 BDSG a special legal regulation. The regulation allows

Processing of personal data of employees for detection

of criminal offenses only if strict conditions are met, for example if

documenting factual indications of the suspicion of a criminal offense in

Establish employment and processing for detection

of the criminal offense, cf. Section 26 (1) sentence 2 BDSG.

If § 26 paragraph 1 sentence 2 BDSG but for the processing of personal

data etc. requires that "factual evidence to be documented"

justify the suspicion of a criminal offence, why should the processing

of the more vulnerable special categories of personal data

data to be subject to lower requirements (cf. insofar as the applicable

the statements of the LAG Berlin-Brandenburg, judgment of 4.6.2020 - 10

Sa 2130/19, 72)? Such an understanding would both of the legal

systematic as well as the sense and purpose of the provision.

In addition, it should be noted that an encroachment on fundamental rights of a high

Intensity can already be disproportionate as such if the intervention

occasion does not have sufficient weight (BVerfG, judgment of 27.02.2008

– 1 BvR 370/07, 244). As far as the intervention to ward off certain dangers

serves, it is decisive for the weight of the reason for the intervention

rank and the type of endangerment of the objects to be protected (as before). The one with the

biometric time registration by means of fingerprints

the personality right is already due to the assessments of Art. 9 Para. 1

GDPR of high intensity, so that the employer's interest in

a "tamper-proof" working time recording using fingerprints

on the other hand, must resign (also LAG Berlin-Brandenburg, judgment

from June 4th, 2020 – 10 Sa 2130/19, 72).

3. Could introduce a biometric time and attendance system

Basis of effective consent of the employees according to § 26 paragraph 3 sentence 2

BDSG data protection compliant possible?

Section 26 (3) sentence 2 BDSG enables the person responsible to process the data

special categories of personal data – including biometric data

Data - on the basis of an express reference to this data -

the consent of the employees. It cannot therefore be ruled out that

Employers a biometric time recording system based on effective

Introduce declarations of consent for employees in compliance with data protection

and can use.

The requirements for an effective declaration of consent should be

However, those responsible should not be underestimated: In addition to § 26 para. 3 sentence

2 BDSG, the requirements of § 26 Para. 2 BDSG must be observed.

In addition, the person responsible for compliance with the principles

responsible for the processing of personal data and must

be able to demonstrate compliance with them (accountability), cf. Art. 5 para.

2 GDPR. With a view to the consent process, those responsible should

cess and the design of the declaration of consent, e.g. B. the following

Ask questions:

– Is the consent at all suitable for the planned data processing?

This presupposes that the consent at any time (with effect for the future)

revoke and the data processing process - depending on the declaration of intent

of the employees concerned – can be designed “differently”.

(alternative behavior). Especially for the biometric recording of working hours

Therefore, an alternative way of recording time should be provided

(e.g. using a chip card or token).

– Can an informed declaration of intent be assumed?

This presupposes that the employee is made to understand

the purpose of the processing of his personal data

and how the process works. Looking at accountability

of the person responsible, it is advisable to provide the information in text form in a

to provide clear and simple language. According to § 26 paragraph 3

Clause 1 BDSG, it must also be ensured that the consent

of the employees concerned explicitly to the processing of biometric

shear data.

– Have the affected employees been informed of their right of withdrawal?

The information about the right of withdrawal is according to § 26 paragraph 2 sentence 3

BDSG in text form.

– Is employee consent given on a voluntary basis?

§ 26 paragraph 2 sentences 1 and 2 BDSG measure the question of the voluntariness of

Consent is of particular importance in the employment context. This wears

account of the fact that between employer and employee

superior/subordinate relationship exists. The consent comes for processing

Therefore, the processing of employee data is not regularly considered (cf. also

Short Paper No. 14 Employee Data Protection of the DSK). Especially if

it is about the question of the voluntariness of the consent to the processing

whose categories of personal data are concerned is according to the will of the

legislator to apply a strict standard (cf. also BT-Drs. 18/11325,

102). Those responsible should therefore ask themselves whether the problem

the superior/subordinate relationship between employer and employee

affects the participant with regard to the planned data processing situation,

under what actual circumstances/circumstances the consent

is obtained from those affected (possibility of pressure

situations) and whether the consent was given in an inadmissible way to further

Conditions is "coupled". As case constellations, if they exist

§ 26 states that it can be assumed that the consent was voluntary

Paragraph 2 sentence 3 BDSG the existence of a legal or economic

Advantage of the employee and the pursuit of similar interests

by employers and employees.

– Are the formal requirements for the consent in the employment

relationship observed?

According to Section 26 (2) sentence 3 BDSG, consent must be given in writing or electronically

to take place technically, unless another is due to the special circumstances

shape is appropriate.

– Can the person responsible prove that the data subject

sam has consented to the processing of your personal data?

Those responsible should be aware of this, especially against the background of the

in Art. 5 Para. 2 DS-GVO standardized accountability.

7.2

Examination of costs for health services for asylum seekers

The public sector has a legitimate interest in correct

Invoicing by providers of healthcare services (especially

special clinics, doctors) for asylum seekers. The asylum seekers

are obliged to provide the necessary medical confidentiality

Consent to the data processing necessary for the billing verification

to grant work.

The Hessian Ministry for Social Affairs and Integration submitted to me

a matter relating to the right to benefits for asylum seekers and asked

for advice on data protection law. Specifically, it was about the fact that after

Asylum Seekers Benefits Act (§§ 4 and 6 AsylbLG) Asylum seekers entitlement

have necessary medical care.

In the initial reception facilities in Hesse, their own medical

Ambulances that guarantee basic medical care. For one above

diagnostics and therapy that go beyond this, the asylum seekers are

external specialists / clinics. These external medical services

Service providers then address the cost-based billing

the regional council of Giessen. The RP Gießen is then correct

to check the billing. This process takes place without the participation of

health insurance companies.

Medical care for those with health insurance

(Social Security Code V)

Statutory health insurance companies are obliged to check the proper

according billing on the part of the service provider an expert

Obtain an opinion from the Medical Service (MDK). have crane

kenkassen or the MDK for an expert opinion or examination

required data of the insured person from the service providers

requested, the service providers are legally obliged to do so

to transmit data to the MDK. As far as in individual cases an expert

Opinion regarding the necessity and duration of inpatient treatment

treatment is required, the medical staff of the MDK is authorized to

me from hospitals and prevention or rehabilitation facilities

to enter. The procedure is in the Social Security Code V - Statutory Health Insurance

insurance - regulated in more detail (§ 275 Para. 1, § 276 Para. 2 and 4 SGB V).

Difference between Social Security Code V (health insurance)

and asylum seeker benefit law

This test procedure, which is standardized in Book V of the Social Insurance Code, is

However, this is not provided for in the performance law. The possibility of at least one

random hospital bill check or a plausibility check

bility control of the treatment bills is developing, it was reported

me the Ministry, according to the RP Giessen for reasons of medical

confidentiality difficult. The RP Gießen has the problem closer

described that billing hospitals rely on

Doctor's letters or documentation because of medical confidentiality

not allowed to publish. According to the ministry, this creates a

Discrepancy between the payment obligation of the public sector on the one hand and

not possible correct invoice verification on the other hand.

Against this background, it is necessary, according to the ministry, that the MDK

in the area of asylum seekers, a comprehensive right of examination with a view to the

costs claimed by service providers are granted.

Data protection regulatory assessment and advice

In the field of statutory health insurance, SGB V, there are sufficient

Statutory audit authorizations for the health insurance companies and the MDK

and a corresponding duty of service providers to provide information.

This is not the case with benefits under the Asylum Seekers Benefits Act

to benefits according to the Social Security Code V. In this respect, the regulations

stipulations of this code that relate to auditing, not in

applied to the asylum seeker area. Comparable regulations

Audit rights or information obligations between cost bearers and service providers

However, the asylum seeker benefits law does not know the providers.

In some federal states, however, the benefits according to § 4 AsylbLG

taken over by statutory health insurance ("Bremer Modell"). the

legislator has this concept in the extensive regulation § 264 SGB V

generally regulated. As part of this solution, the health insurance

sen or the MDK with regard to the invoice verification accordingly

§§ 275 f. SGB V.

However, Hesse has so far not been able to provide the services via the

processed by health insurance companies, so that with regard to the test and information

regulations cannot be referred to the Social Security Code V.

In this respect, the DS-GVO and especially the medical confidentiality are one

Authorization to test the payer and information from the service provider

bring against.

No breach of medical confidentiality in the case of

consent

The medical confidentiality is in the case of a cost review, however

not violated if the consent of the person to whose personal

sun-related data it works. Because in this case the data processing

according to the European General Data Protection Regulation, Art. 6

Paragraph 1 a) GDPR.

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following

conditions are met:

a) The data subject has given their consent to the processing of data relating to them

personal data for one or more specific purposes.

Employee data protection, social affairs

Since in the present context it is of course also about sensitive data of the asylum

applicant, namely in particular ethnicity and health data

Asylum seekers, Art. 9 DS-GVO must also be observed, which

concerned data of a sensitive nature. But this provision also opens in

In the event of consent, the path to lawful data processing, Art. 9

Para. 1, Para. 2 a) GDPR.

Art. 9 GDPR

(1) The processing of personal data revealing racial and ethnic

origin (...) emerge, as well as the processing (...) of health data of a

natural person is prohibited.

(2) Paragraph 1 does not apply in the following cases:

a) The data subject has consent to the processing of said personal data

expressly consented to data for one or more specified purposes, unless

because, according to Union law or the law of the Member States, the ban can be

Paragraph 1 cannot be revoked by the consent of the data subject.

(...)

The at the end of the quoted standard text of Art. 9 Para. 2 a) DS-GVO addressed

Although the exclusion of consent as a legal basis is dependent on the

German data protection supervisory authorities discussed, but by the legislature

in any case not been noticed, so that even with sensitive data

consent as justification for data processing

stands. Of course, the GDPR is still going through in the public sector in particular

national law of the member states supplemented and completed (Art. 6 para. 2

and 3 DS-GVO), which is also included in the data protection assessment

to the GDPR and must be observed.

With a view to the Hessian Ministry for Social Affairs and Integration

Subject of invoicing submitted to me by the providers

of health services on the one hand and the need for verification

of the public payer on the other hand and the problem of medical

The law on benefits for asylum seekers now contains a confidentiality obligation

decisive provision, § 9 para. 3 AsylbLG, because this regulation viz

the obligations of the beneficiaries to cooperate in the social sector

and also the obligation of the beneficiary to issue the

necessary approvals (consent) for the performance of tasks

refers to the public service administration and accordingly for

declared applicable, namely § 9 para. 3 AsylbLG.

55

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

§ 9 AsylbLG

(...)

(3) §§ 60 to 67 of the first book of the Social Security Code on the participation of the

Beneficiaries are to be applied accordingly.

The background to the provision is precisely that the asylum seeker

Performance law is not legal to social law in terms of the legal system

has been assigned (cf. § 68 SGB I), but it is nonetheless required that

duties of cooperation standardized for the beneficiaries in social law

also to be imposed on the recipients of asylum seeker benefits. The

specifically means those who provide medical/medical services

claim to have agreed to that

the accuracy/adequacy of the information provided for these services by the clinics,

Doctors, etc. submitted invoices from the public administration as

Service providers and cost bearers can also be effectively controlled. Of-

Half arranges the social law that in particular because of the medical

Confidentiality necessary consents with a view to the required

Performing public administration tasks (here auditing)

are to be issued by the service recipient, § 60 Para. 1 No. 1 SGB X.

§ 60 SGB I

(1) Anyone who applies for or receives social benefits has

1. to state all facts that are relevant to the performance and, at the request of the

responsible service provider of the provision of the necessary information by third parties

agree.

(...)

The corresponding application of this provision in the area of asylum seekers

therefore means above all that the responsible asylum seeker benefits

authority from the affected asylum seekers the consent regarding

the required information from the service providers (clinic, doctors)

can demand.

I have the requesting Ministry for Social Affairs and Integration on this

Legal situation pointed out.

56

Employee data protection, social affairs

7.3

It stays the same: No comprehensive picture recordings in the day care center without

Compliance with data protection requirements

The production of photo (and video) recordings in day-care centers or

Kindergartens remain a sensitive ongoing topic under data protection law. The

Responsible bodies have been even more since the GDPR came into force

in the obligation to take comprehensive technical and organizational measures

and ensure the necessary transparency towards parents/custodial

obligated to ensure - for all related processes

(from production to further use) and further handling

these recordings.

I received a complaint from an affected parent about a child

the day-care center or the (independent) provider of this day-care center in which or

where one of the applicant's children will be admitted

should. The organization also operates other day-care centers

in other places.

The object of the complaint was data protection addressing

say, in the (um-

catchy) contract for child care. This contract contained B

In one place there is also a passage on “Creating and distributing photo and

Film records". The data protection regulations throughout the contract

did not seem to be tenable for the complainant and against the applicable

violating data protection law. The possibility of individual passages and

The institution did not intend to object to their regulations. A supervisor

The possibility of this only became possible through the full signing of the contract

parents/guardians opened.

So the person involved involved me, asking for my review and intervention.

Introduction

The topic of photo and film recordings in day-care centers or children's

Gardens has been an ongoing topic in the field of social affairs and

regularly/annually the subject of complaints, requests for advice,

test applications etc.

The sensitivity of this topic is obvious, because the special

Children's need for protection is immediately obvious and obvious

and last but not least z. B. in the constitutionally laid down

(so-called) guard task of the state down.

The laws and regulations that have been in force for years or even decades

gifts of the state related to the protection of children and

Since the DS-GVO came into force, young people have been protected by data protection law

Perspective once again expressly and additionally sharpened by

the DS-GVO the special need for protection of children and young people

expressly mentioned in several places (see only e.g. Art. 6 Para. 1

lit. f, Art. 8 or Erw.Gr. 38 GDPR).

In this respect, it is and will remain an important topic for me,

accompanied by complaints and inquiries attentively and critically and,

if necessary, also emphatically towards responsible bodies

for solutions acceptable to data protection authorities.

Facts and legal assessment

In addition to his complaint, the complainant also handed me the

complete support contract of the institution, which he criticized. After

whose critical review I had to vague and

non-transparent regulations under a regulation on data protection

stating On the other hand, the statements made there and

Regulations on the "creation and distribution of photos and films"

in the eye, e.g. B. in particular the following passage:

"By signing this contract, the legal guardians agree

the distribution or public display of recordings on which

your child or yourself can also be seen for the following purposes - also after

Termination of the supervisory relationship – with the proviso that

no legitimate interests of the child and family are affected

become.

– Using photos, slides created by the staff for

Printed products (e.g. facility concept, letters to parents, annual reports,

chronicles, photo gallery in the protected parent area).

– Presentation of photos, films, slides that the staff or a

created on behalf of another person, at parents' evenings, in local

tical committees and other circles of an interested public.

– Publish photos and film recordings that the staff or

a member of the press created, in press reports about the facility."

Without going into too much detail, large parts of the regulations for

Data protection and the handling of photo and film recordings to or completely

indefinite ("general statements"), so that e.g. B. effective consent

the parents/guardians could not be granted at all, because

they do not recognize the extent of data processing by the carrier and

could estimate. They simply weren't able to see

to know exactly what they should give their consent to.

Also the “unrestricted” possibility of use mentioned in the contract

of personal data for internal purposes or even among themselves

between the various subsidiaries (day care centers)

had to be addressed as unacceptable.

Finally and not least, this also applied to the passage quoted above,

which must be considered unacceptable under data protection law.

I therefore have the operator of the day-care center(s) with my concerns

confronted. In a short-term first reaction to my related

Letter from the legal counsel of the person responsible then -

quite fortunately – one of my concerns and clear indications

grateful, constructive processing of the contract as a whole

and the topic "Creating and distributing photos and films"

emerge as a focus.

The pronounced willingness to cooperate, especially in the form of opposing and

Recording my criticisms with immediate adjustment and implementation in

the contract there quickly turned out to be positively remarkable

reliable in terms of content.

In this way – a brief list of examples follows – one of the required

data requirements of the GDPR (cf. Art. 12 and 13 GDPR)

protection information reformulated and integrated. Furthermore, a - because
of the coupling ban according to Art. 7 Para. 4 DS-GVO - from the contract on the
Support services independent declaration of consent for manufacturing
and use of photographs (still and moving) of people
designed to meet the requirements of Article 6 Paragraph 1 Clause 1 Letter a, Article 7 GDPR
and § 22 KUG is sufficient. Among other things, also certain situations
in which recordings are considered or made at all,
selected and precisely defined.
Also - also in connection with the photo and video recordings
– the IT security concept was again critically examined, revised and new
implemented.
The result was mutual and consistently constructive
Cooperation between the carrier and me within a short time both
the contract as well as the technical and organizational measures
revised in accordance with data protection regulations and quickly put into practice,

so that I do not use my powers under Art. 58 DS-GVO
had to do.
Conclusion
Contract regulations or declarations of consent in day-care centers
or kindergartens are from a data protection supervisory authority perspective
often problematic or even - in some cases - unacceptable because
they do not meet the data protection requirements. Because it is for this
for various reasons there is and cannot be a uniform pattern,

this topic will continue to concern me. However, this can

also give pleasure once in a while when I meet an approachable, cooperative

rational and reliable counterpart, my

Demands are understandable and they are grateful and reliable

as implemented immediately.

8. Healthcare

healthcare

8.1

Temperature measurements as an admission requirement for visitors and patients in hospitals

Due to the corona pandemic, I had myself with me during the reporting period

special data protection issues in the health sector

too busy. This was also the case with the following

ten operation: A hospital intended, with patients and visitors

to measure fever before entering the hospital to prevent early Covid-19

identify suspicious cases.

The request dealt with the admissibility under data protection law

of fever measurements as an admission requirement for visitors and patients

of hospitals during the COVID-19 pandemic. The fever

In the case of prone admissions, this was done manually, in all other cases

automated using a thermal imaging camera installed in the entrance area

of the hospital. The video recording and temperature measurement was

indicated with information boards. The results of the automated

th measurement were on a monitor at the Infopoint in a separate

Area displayed to which only authorized persons had access. The

System reported affected people with a body temperature of

above 39°C had been detected.

Measures taken

The following measures were taken in dialogue with me: The automated

The measurement data and video recordings collected were only carried out on the

main memory of the computer. Storage on a hard disk

did not happen. As a result, the data was only available for a short time

are inaccessible and are irretrievably deleted when the computer is shut down

become. In addition, there was no connection to the computer that

collected data automatically with the clinic network (stand-alone system).

The data could also only be called up technically if the pre-

set temperature value of 39°C was exceeded. From the technical

Page could thus significantly reduce the risk of access by unauthorized persons

be reduced. Legally, only a limited number of employees received

access to the premises and access to the

collected data. The persons concerned were kept secret

and committed to secrecy. Affected people with elevated values

were specifically and discreetly addressed by nursing staff and in

ready premises.

Legal Assessment

1. Scope of application of the GDPR and legal basis

In my opinion, the manual fever measurement of visitors falls

or patients generally not within the scope of the DS-

GMO, provided that the measurement results are not stored in the device and

cannot be subsequently stored in a file system. It deals

This is a non-automated processing of personal data

Data. The scope of the GDPR is therefore not open (Art. 2

Para. 1 GDPR). Manual fever measurement is to be judged differently

among employees. Here is the scope of the

DS-GVO also opened if no automated data processing takes place

(see, inter alia, Section 26 (7) BDSG). On the admissibility of fever measurements

Employees will not be discussed further at this point.

The automated fever measurement of visitors, for example through thermal imaging

cameras, or a transcription of non-automatically collected

Results, on the other hand, fall within the scope of the GDPR. Both

through the thermal imaging camera or manually recorded data

about health data, d. H. special categories of personal data

within the meaning of Art. 4 No. 1, 9 Para. 1 DS-GVO. In the concrete present

case comes as the legal basis of special category processing

personal data (here: health data) Art. 6 (1) lit. e, f,

9 Paragraph 1, 2 lit. i GDPR in connection with Section 20 Paragraph 1 No. 3 HDSIG or

§ 22 Paragraph 1 No. 1 lit. c BDSG into consideration.

The requirements of Section 20 Paragraph 1 No. 3 HDSIG and the

§ 22 Paragraph 1 No. 1 lit. c BDSG. So must the interests of the person responsible

the interests of the data subject outweigh the processing. The

Processing must be proportionate to that pursued

purpose and uphold the essence of the right to data protection.

Given the unpredictability of the pandemic development in 2020

was, in my view, an appropriate ratio of the one provided here

Data collection on the risk to patients, visitors and caregivers

at least not to be denied by an infection. However

always had to keep an eye on the proportionality of the data collection

and again and again with regard to the development of the pandemic

be re-evaluated.

62

healthcare

Furthermore, Section 20 (2) HDSIG and Section 22 (2) BDSG standardize the obligation

of the person responsible, in the case of the application of a legal basis

Para. 1 specific measures to safeguard the interests of those affected

person to provide. The regulations each depend on the implementation

technical and organizational measures taken in relation to the

concrete processing guarantee a higher level of data protection. In this

Context also applies to the parameters of type, scope, circumstances and purposes

of processing as well as the factors of probability of occurrence and severity

referenced. Logging (No. 2), sensitivity

the data processing participants (No. 3), but also access

restrictions (No. 4). The person responsible has therefore under

Considering the circumstances of the individual case appropriate and appropriate

to take appropriate measures. So must u. be ensured,

that no unauthorized third party has knowledge of the data

obtained and the data destroyed in accordance with data protection regulations.

2. Resolution of the data protection conference of September 10, 2020

In 2020, the need for

The necessity of taking fever and its expediency are discussed. Part

It has been argued that elevated body temperature is not necessarily considered
should be considered symptomatic of a SARS-CoV-2 infection. Also would have
many infected people have no symptoms and therefore no elevated temperature.
Rather, milder measures such as compliance with the
Hygiene and distance regulations and the event-related survey
of the persons concerned available. Due to the arguments mentioned
mente is also the admissibility of fever measurement, for example
Employees and customers of industrial companies, through the conference
the independent data protection supervisory authorities of the federal and state governments
rejected (see also Annex I 2.3, decision of the Conference of Independent
Federal and state data protection supervisory authorities for the use of
Thermal imaging cameras or electronic temperature recording as part of the
Corona pandemic from September 10th, 2020, available on the DSK homepage).
However, the aforementioned decision of the data protection conference applies expressly
not for the field of health care, including nursing.
Unlike, for example, in industrial companies, in the area of
Healthcare provided by hospitals in a balancing of interests
the health protection of doctors, nursing staff and patients from a
Infection with the COVID-19 virus is becoming more important. Health
of the groups of people mentioned is in particular in a hospital
a particularly sensitive commodity. A high quality and safe

Patient care is part of the public interest and straight
of particular importance in the case of the pandemic. Securing

reaching hospital staff is essential here, so that further-reaching

corresponding processing of sensitive health data is required and

can be appropriate.

Conclusion

Under the condition of particularly strict technical security requirements

and comprehensive information for data subjects like you

described above, during the Corona Pandemic I

for example, the automated fever measurement in systemically relevant health

be declared permissible in individual cases in order to ensure adequate

health care for citizens and corresponding protection

of the nursing staff to ensure

8.2

Use of an e-mail distribution list to search for patient files

Employees have suitable technical and organizational

take toric measures to prevent unauthorized persons from accessing

deny personal data. This applies in particular to

health data. In the present case, a large internal e-mail

shared to search for patient records that could not be found.

In a Hessian clinic, personal data of patients

repeatedly and unfiltered via a large internal e-mail distribution list

sent to over 600 recipients. In most cases where patient

data were affected, it was a matter of clarifying the whereabouts of a

patient record. For this purpose, the following patient data was sent via the distributor

sent:

- First and Last Name,
- Birth date,

– Length of stay in the hospital as well

– the patient case number of the data subject.

This violation of data protection regulations, in particular Art. 5

Para. 1 lit. f GDPR, the Hessian Commissioner for Data Protection

and freedom of information reported by submission.

64

healthcare

Measures taken

An already existing internal instruction on data protection was

Instructions by the Hessian Commissioner for Data Protection and Information

mation freedom revised in several places. Among other things

stipulated that the sending of personal data via the

E-mail distribution list is not permitted. As an immediate measure was before completion

of the new data protection regulations to prevent further violations

Circular mail sent to all employees.

In addition, service instructions on how to proceed in the case of

clear whereabouts of patient files issued, so that now the following

Procedure is defined:

1. Patient files, the whereabouts of which are unclear, are first

employee individually via the hospital archive

requested.

2. If the file cannot be found there, the employees

and employees of the archive and speak to those last involved

Head physician secretariats.

3. If the patient file cannot be found here either, the

Search can be expanded moderately, but only beyond the individual

Contacting the responsible employees.

The use of an e-mail distribution list is not permitted.

In cases of doubt, the data protection officer of the clinic is in good time

to contact.

In addition, the use of the large internal e-mail distribution list

restricted. Topics that are of general interest can only be

made available to the respective addressees via the management

become. This ensures that no personal data and certainly no

sensitive health data are sent to unauthorized persons.

Conclusion

When using internal e-mail distribution lists in public or private

Companies should exercise caution when sending personal data. After

Article 5(1)(c) GDPR, the responsible bodies must ensure

that personal data, such as names of patients, birth

date or length of stay in a hospital, confidential

treated and protected from unauthorized access. Also applies

for the processing of personal data, including the

Distribution of patient data via an e-mail distribution list counts, the principle

the data minimization of Art. 5 Para. 1 lit. c DS-GVO. As a consequence,

that, for example, the disclosure of personal data is only permissible

if this is necessary and appropriate to achieve the purpose. The

present case shows that a tiered model with the stepwise

Extension of addressees of personal data is sufficient. It is

on the other hand, it is not necessary for a large group of people to attend from the outset

access to the data.

8.3

Data protection in connection with the obligation to wear a mask

retail trade

Over the past year I have received a large number of inquiries related to

the implementation of the obligation to cover mouth and nose that has been in force since May 2020

in shops. The following post provides information on how I use the citizens

advised in this area.

When it comes to the obligation to wear a mouth and nose cover (mask

obligation) is a protective measure in accordance with Section 28 a Paragraph 1 No. 2

Infection Protection Act (IfSG), which regulates the spread of the corona virus

Disease-2019 (COVID-19) is to be prevented.

According to § 1 a of the Ordinance on the Restriction of Social Contacts

and the operation of facilities and offers due to the co-

rona pandemic (Corona Contact and Operational Restriction Ordinance,

CoKoBeV for short) of November 26, 2020, there is an obligation in many areas

wear a mouth and nose cover.

The exceptions to this obligation can be found in Section 1a (3) CoKoBeV. There-

according to are persons who due to a health impairment

or disability cannot wear a mouth and nose cover

Obligation to wear a mouth and nose cover exempted.

Further information on how this is to be specifically proven can be obtained from the

order unfortunately not be removed. In practice, this leads to a

great uncertainty as to how to deal with it.

§ 1 a CoKoBeV of November 26, 2020

(...)

(3) The obligation pursuant to paragraph 1 sentences 1 and 2 does not apply to

1. Children under 6 years of age,

2. Persons who, due to a health impairment or disability

cannot wear a mouth and nose cover,

66

healthcare

3. Personnel of institutions and companies according to paragraph 1 sentence 1, insofar as no

tact to other people or other and at least equivalent

Protective measures, in particular separating devices, are taken,

4. Lecturers at universities, vocational academies, music academies and extracurricular

educational institutions and those involved in examinations if a hygiene concept

that at least the distances to be maintained and the regular air

exchange ensures

5. Participants in the state compulsory subject examination and in the second state law examination

test,

6. Teachers and learners during practical lessons with wind instruments, as well as

7. Customers in companies and facilities according to paragraph 1 sentence 1 number 4, to the extent

and as long as the use of the service is only without mouth and nose

can be done.

Legal Assessment

When informing whether someone has health problems or a

has a disability and therefore cannot wear a mouth and nose cover,

it is undoubtedly health data according to Art. 4 No. 15 DS-

GMOs for which processing according to Art. 9 DS-GVO is only possible in very limited

limited cases.

However, it must also be checked whether the GDPR is actually in place when examining the

Exemption from the mask requirement applies. Art. 2 Para. 1 GDPR

determines the material scope of the GDPR. After that applies

the regulation for the processing of data stored in a file system

are or should be stored.

If there is no data processing when checking the mask requirement, i.e

If the information is not recorded or stored, the test fails

the mask requirement by shopkeepers does not fall within the scope of the

data protection law.

Even if one takes the view that the purely visual inspection of the mask

exemption falls under the GDPR, such data collection could

the shopkeeper according to Art. 9 Para. 2 i) DS-GVO i. in conjunction with Section 22 (1) No. 1 c)

BDSG be justified. For storage of this information see

I here however no necessity.

Conclusion and Outlook

In connection with transactions, there were neither in the Co-

rona regulation still in the case law precise references, such as a

Mask exemption can be proven or what content such a

must have certificate. However, shop owners can exercise domiciliary rights

claim and customers without a mask who are exempt from the mask

not be able to credibly demonstrate the obligation to pay, refer to the business. When

this exemption is actually made credible is not defined - and

is ultimately at the discretion of the respective counterpart.

From a data protection point of view, data collection from the data subject is based on

limit the amount required. If the mask exemption by the

Affected persons proven to the shopkeeper with a certificate,

an inspection is sufficient. For making a copy there

however, there is no sufficient legal basis.

8.4

Access to data by former employees in the hospital

If employees leave a hospital, attention must be paid to this

that they also have access to the hospital's data

is withdrawn.

Last year, a Hessian hospital reported to me as part of a

Report according to Art. 33 DS-GVO the following facts:

A former employee who has already left the service of the hospital

was seen gaining access to a

procured station base and work there on a hospital PC

performed.

At the time the incident was reported, it could not be ruled out

denying that former employees have access to personal data

third had taken.

In good time within the reporting period of 72 hours, the

hospital sent me a corresponding message.

Legal Assessment

According to Art. 5 Para. 1 lit. f i. In conjunction with Art. 32 GDPR, the data in the crane

kenhaus be processed in a manner that provides reasonable security

of personal data, including protection against

unauthorized or unlawful processing and against unintentional

loss, accidental destruction or accidental damage.

The hospital must therefore ensure that it is not possible for unauthorized persons

is to gain access to patient data. That includes access

and access to the computers is secured accordingly. This can

either through technical measures, such as a password

healthcare

protection of the PCs, or through organizational measures,

such as access restrictions.

After termination of the employment relationship, it may therefore

Former employees will no longer be able to access hospital data

to access.

Measures taken

After the incident, the hospital deleted all user accounts of the former

disabled staff and the staff of the station and the gate

informed that the person is a retired person

employee acts.

As a result, the IT department carried out an evaluation

to understand whether and if so, which data by the former

employees were viewed.

It turned out that the employee who had already left the

area of the station base was seen by staff, to none

had access to personal data.

Using the log files of the Windows sessions and the logging data

in the hospital information system it was possible to understand that the

last registrations of this employee before his departure date

and there was no access to patient data. Information from the

According to Art. 34 DS-GVO was therefore not necessary.

Furthermore, the employees were once again informed that

who are not known to you and who are in areas that

are reserved exclusively for employees, immediately to the supervisor

and/or to be reported to the data protection officer.

Conclusion

If employees leave a company, the person responsible may

Don't forget to deactivate the employees' accounts and, if necessary,

to change passwords.

The case also shows how important and sensible it is that a corresponding

Appropriate logging of access is carried out. In this way, in individual cases

be verified whether unauthorized access to personal

data took place.

8.5

The principle of anonymity in transplantation law

The principle of anonymity applies in German transplantation law

between organ donors or their relatives and organ recipients.

It can also be done with the express consent of the data subjects

this principle cannot be broken. Correspondence is permitted

between relatives of the organ donors and organ recipients through

anonymous letters.

A relative of a deceased organ donor complained in his

Submission about the withholding of a letter by the German Foundation

Organ Transplantation (DSO). The DSO is the nationwide coordination

site for postmortem organ donation. She received a letter back in 2016

of an organ recipient, which was addressed to the submitter.

The DSO was initiating corresponding letters at the time due to the unclear

Legal position no further. Only after a corresponding change in the law

of the Transplantation Act, the letters were anonymized and sent to the

recipient sent. The submitter also received with some delay

the letter from the organ recipient. He questioned in his submission under

other things, the withholding of the letter and the legal assessment

the DSO that, despite the corresponding consent, the cancellation of the

Anonymity is not allowed here.

Legal Assessment

In the German transplant system, the principle of anonymity applies between

cal organ donors or their relatives and organ recipients. In the

Transplantation Act (Act on Donation, Removal and Transfer

of organs and tissues from September 4, 2007, Federal Law Gazette I p. 2206, TPG)

§ 14 para. 2 sentence 3 regulates a strict earmarking requirement:

“The personal data collected under this law

may not be processed for purposes other than those specified in this law

become."

Even the consent of the persons concerned can prevent the use of the

do not legitimize clock data by the DSO for purposes of correspondence.

According to § 14 paragraph 2 sentence 1 TPG, the employees of the DSO may in principle

no personal data of organ donors, relatives of

healthcare

reveal to goose donors or organ recipients. A breach of this

Strict prohibition of disclosure is punishable (§ 19 Abs. 3 Nr. 3 TPG).

Therefore, the withholding of the letters by the DSO was data protection law

not to complain about. Due to the anonymity requirement and the strict

Purpose limitation was a legally secure use of the contact data itself

not possible for anonymous communication.

Only with the introduction of the new § 12a TPG on April 1st, 2019 did it become clear

legal basis for the mediation of letters between organ recipients

catchers and relatives of organ donors (§ 12a Para. 1 S. 1

No. 4 and 5 TPG). According to Section 12a (7) TPG, anonymity must be maintained between

Organ recipients and relatives of organ donors continue to be secured

become. Even at the express request of both parties, the DSO

even after the new legal situation no contact details for a personal

Meet or disclose a direct contact.

Legal background

The German legislator considers the anonymity between organ recipients

catchers and organ donors as an important principle of transplant

station. Ensuring anonymity and strict earmarking

education requirement should not only the right to informational self-determination

of those affected, but also the trust of the population in the

proper organ recipient selection and the organ and tissue

protect the people and institutions involved in the donation (Spickhoff/Scholz/

Middel, 3rd edition 2018, TPG § 14 para. 1). The impression of a not objective

selection of organ recipients based on certain reasons should be prevented

also to increase the acceptance of organ donation.

The anonymity between organ donors and their relatives and

Organ recipients are provided for in many European legal systems.

The World Health Organization (WHO) also explains in its guidelines

for transplantation of human cells, tissues and organs that the

The anonymity of organ donors and organ recipients must always be protected

(WHO, Guiding Principles on Human Cell, Tissue and Organ Transplantation,

Guiding Principle 11). This is generally justified with the protection

from potential abuse or financial pressure.

Conclusion

There was no data protection misconduct on the part of the DSO. In the

In transplantation law, the principle of anonymity takes precedence over

consent of those concerned. The free decision-making authority

of organ recipients and relatives of organ donors is thereby

limited and communication difficult. This condition can

create a lack of understanding for those affected, but there is only one remedy

make appropriate changes in the law.

8.6

Data protection-compliant control and documentation of the

measles protection

From a data protection point of view, the control of measles protection

basically only by presenting the vaccination certificate or the medical

Appearances take place. The making of copies of these documents is

not permitted, since a corresponding internal memorandum on documents

training purposes is sufficient. Due to the principle of data saving

The name of the respective doctor as well as concrete diagnoses should be mentioned

will only be stored if there are good reasons to do so.

1. Background

Through the Measles Protection Act (Federal Law Gazette I 2020 p. 148), community

facilities – such as schools, day-care centers and accommodation for asylum seekers

– and medical facilities (collectively “facilities”)

as of March 1st, 2020, the measles protection of their employees or the

control the people they care for.

Proof of vaccination protection can be provided according to Section 20 (9)

law (IfSG) by presenting the vaccination certificate or by a doctor

Certificate of vaccination protection or measles immunity can be provided. At

a medical contraindication that speaks against vaccination

instead, a corresponding medical certificate must be submitted.

For the data protection compliant design of the institutions according to § 20

Para. 9 IfSG mandatory control and the corresponding documentation

my authority received numerous inquiries from various stakeholders

and institutions. Therefore, I put my assessments on this topic in

published in a website post. The post is at the link https://

datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/

data protection-compliant-control-and to find.

2. Legal Assessment

Vaccination cards and medical certificates contain according to Art. 9 Para. 1

DS-GVO specially protected health data. The processing of these

Health data by the institutions is according to Art. 6 Para. 1 lit. c i. V. m.

healthcare

Art. 9 (2) lit. i GDPR i. In conjunction with Section 20 (9) IfSG and Section 20 (1) No. 3

HDSIG or § 22 Paragraph 1 No. 1 lit. c BDSG permissible.

The institutions are legally obliged according to § 20 Abs. 9 IfSG,

to process the relevant health data. Section 20 (9) sentence 4 IfSG

even contains an express obligation to transmit personal

related data to the health department if the facility does not have a

supporting evidence is presented. Protection from health

Dangers related to the spread of highly contagious

Incidentally, the infectious disease measles represents a legitimate public interest

resse within the meaning of these standards.

In the employee context, § 23a IfSG also applies, according to which the employer

under certain conditions, the vaccination and serostatus of employees

allowed to process.

3. Control and documentation in practice

As part of the control of the vaccination status should based on the principle

of data minimization (Art. 5 Para. 1 lit. c DS-GVO) only such personal

related data are processed for the fulfillment of obligations

are required by the IfSG.

The production of copies of the vaccination card or the medical certificate

adjustments is not usually required and is therefore not permitted. It should

rather a corresponding file note or documentation sheet

be used. Also the storage of the name of the doctor,

who carried out the vaccinations, or the specific diagnosis is only at

valid reasons justified.

If a technical medical examination of the documents is indicated, how

in particular when examining medical certificates by the competent authority

Health department can also temporarily provide the original certificate

and the processing of additional data must be permissible under data protection law.

According to Section 20 Paragraph 9 Sentence 1 IfSG, the management of the respective institution is responsible

for testing measles immunity and is responsible for it. She

However, this control can also be delegated to employees of the facility. The

School management can For example, this task can also be assigned to the class teacher.

4. School counseling example

Numerous submissions to control measles protection referred to

Schools as responsible institutions. have in this context

For example, parents asked me how the documentation was created by the

School may take place and what information may be stored.

In the school sector, in my opinion, the storage of information

tion on measles protection in the electronic Hessian teacher and

Student database LUSD permitted and, if necessary, the filing of this

Information in the student's written record is preferable. to the measles

protection status of students can only five in the LUSD

permanently defined attributes are saved. More personal

Data is not saved. Through a corresponding role and

authorization concept ensures that only the respective school

tion and specially selected persons have access to this information

can take. An additional storage in the student file is then

generally not required according to the principle of data economy.

Should this nevertheless take place, the information on protection against

unauthorized access, for example in a sealed envelope

or kept separately in a specially marked folder.

5. Conclusion

Due to the Measles Protection Act, the legislature has different

Facilities control obligations in connection with the measles infection

prevention imposed. Some institutions previously had no

comparable procedures and processes in dealing with the vaccination status or

Health data of their employees or persons cared for. The contribution

on my website should therefore also serve to inform the person responsible in

As part of the implementation and evaluation of the controls for data protection

to provide legal assistance.

8.7

Patient records and staff records in abandoned clinic

The legal entities of clinics must ensure that when moving or

End of the clinic operation all documents with personal

Data will be removed from the clinic rooms. The transport of special

Sensitive health data should only be handled by appropriately specialized

transport or moving companies.

In recent years, media reports about vacant hospital

hospitals and clinics that are published on the internet as so-called “lost places”

become public. These abandoned medical facilities are called

Excursion sites for special experiences or unusual photo motifs

advertised or used as a place for celebrations. Sometimes the visitors bump into it

also on patient files left behind or even an entire file archive.

case description

Also in a Hessian clinic, which ceased operations in 2015, im
Summer 2019 isolated documents from the clinic operation found. Through
the former clinic operating company found out about an article on www.bild.de
of that. They informed me of this by means of a notification pursuant to Art. 33
GDPR. To prevent the further disclosure and dissemination of sensitive personal
prevent personal data was a visit to the abandoned clinic
indicated by my employees. After the current owner
was tacticed and gave his consent, my employees set to work
a picture of the situation on site.
They found that the building was covered with a construction fence from the outside
was fenced and the windows on the ground floor as well as the main entrance
were mostly installed from the inside. Some of the windows on the first floor
however, were struck. In the clinic building, among other things, they
rem employee rosters and phone lists, floppy disks, a patient's prescription,
File cover with patient information and a complete discharge letter
secure. Later also X-rays without reference to persons as well as
more diskettes and employee photos found.
According to information provided by former employees of the clinic, all
were organized with personal data before the clinic was closed,
properly packed and transported. The patients-
documents of the clinic, which included about 1100 boxes, were professionally
stored by a service provider. The former clinic operating company
I was able to do this through corresponding invoices and order documents
prove. She also commissioned the sale of the property

a security service to guard the building.

I therefore assume that these are isolated documents and

documents that were probably overlooked when moving out of the building

became.

Legal Assessment

Patient records must be kept due even after a clinic closes

Statutory (e.g. § 630f Para. 3 BGB) and professional retention

obligations to be kept safe. According to Art. 5

Paragraph 1 lit. f) GDPR, in particular through suitable technical and organizational

Satorial measures, adequate security of personal

ensure data. What measures have been taken to protect the data

must be depends, among other things, on the risk of unauthorized

Access, the type of processing and the importance of the data for the

rights and interests of the data subject. When assessing the

appropriate levels of protection are, in particular, the risks posed by unauthorized persons

Disclosure of or unauthorized access to personal information

into account (Article 32 (1) and (2) GDPR).

Patient records are defined by Art. 9 Para. 1 GDPR

specially protected health data within the meaning of Art. 4 No. 15 DS-GVO.

When moving or clearing a clinic, the operating company

therefore to ensure that all patient records are secure

be transported and stored. A professional execution of this

Work that takes into account the sensitivity of patient records

ensured by a correspondingly specialized transport company

become. The transport company is expressly on the special

protect patient data. After the transport

the operating company itself should take care of the patient documents

convince that no documents with personal data are returned

were left.

The abandoned clinic area was not sufficient against unauthorized persons

Third-party access protected. The building was no longer secured

Responsibility of the clinic operating company, but none would have - also

not individual documents with patient information are left behind

that may. A special obligation of the transport company or

a corresponding specialist knowledge was not presented to me. A careful one

final inspection of the clinic rooms also did not take place.

Violations of Art. 5 lit. f GDPR can, according to Art. 83 Para. 5 a GDPR

be punished with an increased fine. Because of the timely

Notification according to Art. 33 Para. 1 DS-GVO was the facts for the health

house operator company here but not relevant to fines. The non-data

The clinic was evacuated in accordance with protection even before the GDPR came into force

instead of. In addition, the clinic operating company was very cooperative and has

my employees were very well supported in processing the process.

Conclusion

For future moves or clearing of archives with patient records

or entire hospital departments, I recommend moving from

select a company specializing in sensitive patient data and for this

To ensure that these are then kept in a suitable manner.

healthcare

In addition, the insurance of the moving company should also be obtained

be that all data related to patients or employees from the

be removed and a final check carried out

be led. By reporting the last few years are deserted

Clinics nationwide in the public eye. The unauthorized

acknowledgment of patient documents left behind, the

responsible in case of closure or relocation of a clinic in any case

exclude in order not to risk regulatory action.

77

video surveillance

9. Video Surveillance

video surveillance

9.1

Video surveillance in hotels and restaurants

Video surveillance of dining and lounge areas in a restaurant

is generally not permitted under data protection law. The same applies to café and

Gastronomy areas in bakeries, petrol stations, etc. also for hotels, since

assign the behavior in these areas to the leisure area of the guests

where personal rights are to be particularly protected.

In the year under review, the number of complaints and requests for advice

field of video surveillance compared to previous years

increased (see I 17.2). This could be the case with video surveillance in the neighboring

economic context to be due, among other things, to the fact that

more people were working from home due to the corona pandemic

or were at home more often due to short-time work or other reasons and

so more aware of one or the other camera in the immediate vicinity

were or felt disturbed by it.

With regard to video surveillance, this activity report provides an example

a case from the hotel and catering industry is presented. Already

In the last report I dealt with this problem

the set. Since there were inquiries and complaints about this during the reporting period

topic are consistently high, the problem is taken up again

and deepened. In addition, reference is made to the newly revised "orientation aid video

Monitoring by non-public bodies" (as of July 17, 2020,

Link: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_vü_dsk.

pdf) as well as the guidelines 3/2019 on the processing of personal data

ten by video equipment version 2.0, adopted by the European

Data Protection Board on January 29, 2020 (Link: https://edpb.europa.eu/

our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-da-

ta-through-video_de), made aware.

A family who was a guest at a hotel complained about the video

surveillance in the breakfast room. That was because of the complaint

Video surveillance system of the entire hotel checked.

The hotel was asked for information according to Article 31 DS-GVO i. V. m. § 40 paragraph 4

BDSG requested. The hotel provided this information comprehensively and in a timely manner

after.

A total of 16 cameras and one dummy camera were installed. At all

Cameras were so-called. Dome cameras, their swivel and

Zoom function is not technically activated and cannot be controlled externally

was. (A dome camera is an electronic camera

ra covered by a hemispherical, clear plastic cover

is surrounded.)

The justification given for the cameras being installed was that

this to protect the domiciliary rights, to prevent and clarify

Criminal offenses, vandalism, cheating and rental fraud, theft,

raids and to ensure the safety of guests and employees

and their property were installed.

The storage period was 72 hours. Sound recordings were not made.

Only in-house technicians had access to collected and recorded data

Data. The recorder was protected by double access control -

locked cabinet in locked server room - guaranteed.

The dummy camera was installed in the restaurant.

After examining the documents it was found that against the installed

Cameras in areas of the underground car park and delivery no data

protection concerns existed. A total of four cameras

criticized. These were two cameras in the reception/hotel lobby area as well

a working camera in the restaurant, and the dummy camera in the

Restaurant.

Art. 6 was used to justify the non-compliant operation

Para. 1 lit. f. General Data Protection Regulation (GDPR) and the orientation

tion aid for video surveillance by non-public bodies.

A video surveillance of dining and lounge areas in a restaurant

is generally not permitted under data protection law. The same applies to cafés and

Gastronomy areas in hotels. In seating areas, the outdoor gastronomy

the counter and at a bar, guests typically stay longer

Time up, they eat, drink and talk. Jurisprudence rules

this behavior to the leisure area of the guests (cf. AG Hamburg, judgment

from April 22, 2008 – 4 C 134/08). Personal rights are particularly important here

protection. Video surveillance disrupts unimpeded communication

tion and the unobserved stay of the visitors and intervenes intensively

their rights. In the dining and lounge areas there is during

the opening times also do not pose a high risk to the property of the hotelier.

In addition to the guests, there are staff on the upper floors at these times

guarded areas, which the police immediately in the event of such incidents

can communicate. Areas to linger, relax and

Invite to communicate (this also includes the foyer of the hotel), may

therefore not regularly monitored with cameras.

Is used for monitoring in entrance and exit areas, corridors and stairwells

protect against burglary and if an alarm system is not suitable,

to effectively protect against this, cameras are allowed at this point outside the

opening hours.

Storage and vaults are in a restaurant/hotel for guests

usually not freely accessible. You can be monitored when in

no permanent jobs have been set up in these areas and none

milder means of achieving the purpose are available, for example

allow access only to authorized persons. The detection area

of the camera is to be limited to the essentials. Allowed in kitchens

Cameras are not used.

The cash desk itself can be video-monitored during opening hours,

if assaults or thefts were committed by third parties and these without

Video surveillance cannot be clarified or proven. To-

there must be no other, milder measures to secure the checkout

give. It should be checked whether the checkout is in a protected area within

relocated in the restaurant or the checkout system with technical measures

(code card, password, etc.) can be secured against access. personal

Employees' personal rights must also be respected in this area,

which is why camera recording should be limited to the checkout terminal.

After a request to adjust the video surveillance, the full

constant removal of the cameras in question, including the dummy cameras,

proven.

9.2

Video surveillance of an expensive monument on a

central urban square

The clearly limited video surveillance of an expensive monument

a public place, taking into account and implementing further

further structural and organizational measures by the data protection supervisory authority

be accepted if other possibilities are obvious and comprehensible

cannot be considered.

As part of a consultation request from a Hessian city, I was

confronted with the question of whether in the context of property protection on a

nem central square of the city a monument erected there with a view to

whose high procurement and maintenance costs are video-monitored

can. Further supplementary structural security measures around the

Monuments had also already been specifically envisaged.

The work of art created by an artist cost around 140,000 euros

and was released shortly after its unveiling and public presentation

after less than a week due to paint smears (graffiti).

damaged. This was because of the used for the artwork

Materials require equally complex, long-term and cost-intensive

repair work triggered.

Legal Assessment

In the case presented here, special consideration had to be given to

that on the one hand a central and heavily visited and frequented place

of the city was addressed and on the other hand also a large ecclesiastical

Facility joined this place or directly to it and

bordered "fluent".

The examination of the admissibility of the construction of the video surveillance planned here

6 Para. 1 e GDPR i. V. m.

§ 4 HDSIG.

According to § 4 para. 1 HDSIG, the observation of publicly accessible rooms

with optical-electronic devices (video surveillance) only permitted,

as far as they 1. fulfill the tasks of public authorities, or 2.

Agreement of domiciliary rights is required and there are no indications that

legitimate interests of those affected prevail. The storage or

Use of data collected under paragraph 1 is permitted if they

Achievement of the intended purpose is necessary and no indications

exist that the legitimate interests of the data subject prevail (§ 4

Para. 3 p. 1 HDSIG).

The city had me in addition to the planned installation of a video camera

another precautionary measure. First of all, the thinking

sometimes structurally bordered and framed. By building one

A fence or a wall should provide direct contact with the

monument are excluded. As a result, the area should and can

of video surveillance on these fenced in areas that are no longer freely accessible

area to be restricted.

In principle, a visit to a public

public square of a city by private individuals, a walk or

also linger here regularly within the individual personal

recreational activities of these people. As part of their free time

can do this in principle and perhaps particularly when located here

video surveillance

adjacent and in the immediate vicinity of a large church institution

is, assume that they are unobserved in this place and

move freely without video surveillance and recording

he follows.

At what time, on what day, in what condition, with what

appearance and how long a person stays there, how they like it

uses the area, how she behaves there and whether she is alone or accompanied

is, all of this would be complemented by a video

recording documented.

The city did not have exactly this in mind, but after the completion of the

structural changes to be made first (enclosure of the thought

times) only this no longer freely accessible and in this

Meaning then no longer public areas for the sole protection of objects

be monitored.

As a result of the weighing of interests to be carried out here in accordance with § 4 HDSIG

I was in this special case constellation and under appreciation and

consideration of the planning information, in this special individual case

to accept the installation of a video protection system. I have however

clearly indicated the requirement that all of the city

suggestions made to me must be complied with, namely the

Construction of the system solely for object protection, the focusing of the video

camera solely on the then no longer accessible, enclosed

area of the work of art and, as a result, no recording of

People/passers-by at/on the square.

Conclusion

The requesting city has my legal assessment and rating

welcomed. In addition, she has the planned procedure and my position

also with the artist on the one hand and the church on the other

discussed and coordinated so that a trans-

parental and consensual solution could be found.

9.3

Unauthorized video surveillance of a local history museum

The comprehensive video surveillance of a small-town home

museums during its opening hours, even if some

minor thefts have occurred because of the disproportionality of a

not justify such action. The interest of visitors

and visitors in an undisturbed, i. H. unobserved stay in

Within the scope of their personal leisure activities, the interest of the

Town.

I received a request for advice from a small town in Hesse on the possibility

ality, the municipal local history museum covering all of them

Equip premises with a video surveillance system. background

of this wish was the recording of some thefts (card stands,

diorama) or occasional vandalism on exhibits.

The building was designed as a three-storey building with a total area of

described over 500 m2. The local museum is on five to six days

a month and am honored by a local museum association

officially supervised - even during opening hours. In addition, they would

The premises are also regularly used for lectures and as a polling station.

There are plans to set up a video surveillance system in all

position rooms, in which around the clock video recording with a

storage period of seven days should take place. Only for lectures and

Elections are planned in the respective premises for these occasions

to cover the respective video cameras. About a still to be specified

Access concept to the stored records you have first

Thought about.

Legal Assessment

As I have regularly emphasized in my activity reports for many years

and has to make it clear again and again, video surveillance is fundamentally

in addition, a significant encroachment on the personality rights of these

concerned and can therefore be a violation of personal rights.

The risk of influencing the behavior of those affected and their

Control is immanent in a video surveillance system.

The examination of the admissibility of setting up such a video surveillance

The monitoring facility was available with a view to the responsible operator

– either the museum association or the city – to be checked twice. For the

Museum Association as the responsible person, the examination is basically on the scale

of Art. 6 Para. 1 lit. f GDPR, for the small town in Hesse

Art. 6 (1) lit. e GDPR i. V. m. § 4 HDSIG possible legal basis.

According to Art. 6 Para. 1 lit. f GDPR, data processing is only lawful if

if the processing is to protect the legitimate interests of the responsible

literal or a third party is required, unless the interests or

Fundamental rights and freedoms of the data subject requiring protection

84

video surveillance

require personal data, especially if

the data subject is a child.

In particular, when personal data is used in situations

works in which a data subject reasonably cannot

has to expect further processing, the interests and

Fundamental rights of the person concerned the interest of the person responsible

predominate (recital 47 to the GDPR).

According to § 4 para. 1 HDSIG, the observation of publicly accessible rooms

with optical-electronic devices (video surveillance) only permitted,

as far as they 1. for the fulfillment of tasks of public authorities, 2. for the perception

of the domiciliary rights is required and there are no indications that

legitimate interests of those affected prevail. The storage or

Use of data collected under paragraph 1 is permitted if they

Achievement of the intended purpose is necessary and no indications

exist that the legitimate interests of the data subject prevail (§ 4

Para. 3 p. 1 HDSIG).

The city had as an occasion for the establishment of a video surveillance system

In addition to the backgrounds already mentioned above,

that the premises are difficult to see and usually

only by (voluntary) supervision in the entrance area during the

opening hours would be monitored.

A visit to a small-town local history museum is regularly held in the

as part of individual personal leisure activities. As part of

these leisure activities can present people reasonably

and basically assume that this is in a small town

Museum takes place unobserved, especially without video surveillance

and recording.

At what time, on what day, in what condition, with what

appearance and how long a person stays there, how they like it

uses the area, how she behaves there and whether she is alone or accompanied

is, all this will be straight and in particular through a video recording

documented. But how long people during opening hours

actually reside on the premises and in front of the different

objects and exhibits, they must freely decide

can. In addition, there is also the vast majority of

Visitors no reason for the need for a

Continuous surveillance using video cameras.

As a result of the weighing of interests to be carried out here, both

Art. 6 Para. 1 lit. f GDPR as well as according to § 4 HDSIG prevail during

85

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

the regular opening hours of the museum the (legitimate) interests

of the museum visitors on an undisturbed, free

Museum visit where they don't have to be filmed, those

Interests of the city, to secure the inventory or for protection

against vandalism other possibilities are available which are not in

interfere with the fundamental rights of visitors. So come

for this e.g. B. lockable showcases (with safety glass), the fixed technical

Fixing individual objects on walls/in the floor or attachment

of protective covers in front of issued documents as a milder

took into consideration.

The possibility of video surveillance only exists outside

the opening hours of the municipal museum.

Conclusion

I have given the requesting town my legal assessment and

assessment set out. For the installation of a video

surveillance system in the local history museum is in place during opening hours

no way. This result was accepted by the city; in any case

I have no other information.

86

societies

10. Clubs

societies

10.1

Precautionary collection of health data by the

Sports club in the context of the corona pandemic

For the collection of health data by sports clubs as part of the

training or competition operations, there is no specific legal

basis. Instead, Art. 6 (1) lit. a, f GDPR applies. At the same time

the sports clubs always adhere to the principle of proportionality and necessity

ability to orient. I got the clubs over at an early stage

informed my legal opinion and instructions for action on my

website published.

After the first lock-down, I received inquiries from the club country

society, but also complaints from parents whose children have questions about the current

Health status should answer in order to participate in training operations in the club

to be able to participate. It dealt with questions such as B. "You have

Runny nose or cough?", "Do you have a fever?" or "Were you on holiday in

a risk area?". With these snapshots, clubs tried

not to allow possible sources of infection to arise in training operations or to

to be released from imminent liability.

There is no legal basis for data collection

As part of my investigations, I took part with the State Sports Association of Hesse

(lsbh) contact. This referred to a publication of the German

Olympic Sports Confederation, which made recommendations in a "guard rail paper".

had worked out for compliance with distance rules, but that made no statement

for the collection of health questions. Also the ordinance on

The state government's contact restrictions did not contain any regulations on this,

but referred to the top associations of the sport.

Health questions are special category data questions

within the meaning of Art. 9 Para. 1 DS-GVO, the processing of which is initially fundamental

is strictly prohibited and only because of the exemption under Art. 9

Para. 2 DS-GVO may be permissible. Here one could argue that

within the meaning of Art. 9 (2) lit. i GDPR “the processing for the purposes of

preventive health care is required”. I was capable of this position

not to join, as I have serious doubts about the usefulness of the data

processing and in this respect already on the necessity of collecting the

had data. Even the Robert Koch Institute had one of its many

Statements on Covid 19 state that the collection of such

data is not relevant from a medical point of view. That's why I have one

Data collection on the health of club members contradicted. Something

the other applies to the collection of contact data (name, availability) in the

framework of the training operation. Here it had to be taken into account that e.g. B. in

Case of SARS-CoV-2 infection in a person participating in sports training

participated, a follow-up of the infection by the health authorities

be made possible or potentially endangered about a possible

infection with the disease should be informed.

A guide is published on my website

The guidelines on my homepage (https://datenschutz.hessen.de) answered

the related questions of the clubs:

1. There is currently no legal obligation for training operations

to keep "corona lists". In this respect, it basically remains with the association

whether he wants to create such lists or not.

2. However, if the club decides to limit training participation personally

to document the

Data collection (creation and storage list) or consent

of those affected. Then the purpose of collection, such as B. the possibility

follow-up in case of SARS-CoV-2 infection, scope of

Collection and duration of storage, to explain.

A legal basis results from Art. 6 Para. 1 lit. f GDPR. In

In this case, consent can be obtained (Art. 6 Para. 1 lit. a

DS-GVO) can be waived.

3. The association must strictly align itself with the principles of

efficiency and proportionality in the scope of the to be collected and

data to be saved. This means that only those for the survey and

The data necessary for the storage purpose may be queried. These are:

- Name and first name

– day of training

– Place of training

– Contact details (e.g. phone number or email address)

Under no circumstances should health data be recorded, e.g. B. in the

Form that you can children and adolescents according to symptoms of illness

questioned and documented. The same applies to the adults.

4. The handling of the data, regardless of whether it is analogue or digital

to be carried out carefully and strictly earmarked. The lists are ahead

to protect against access by unauthorized third parties.

societies

5. The storage (storage period) should last for a period of one month

not exceed. Digital data must be deleted in accordance with data protection regulations.

The same applies to the disposal or destruction of paper-based

Data.

6. Every association is requested to inform its members or the parents of at least

to inform the annual members about its procedure.

As a result, the clubs mainly have these instructions from the HBDI

gratefully received and implemented in everyday training.

This enabled both the protection against infection, with the traceability of

Chains of infection by the health department, as well as data protection

be taken into account.

10.2

Disclosure of the list of members of an income tax assistance association

to the chief financial officer

In the year under review, an income tax assistance association approached me with the question

whether the request of the Oberfinanzdirektion (OFD) for the release of a joint

member list corresponds to the data protection regulations.

The OFD asked the association to publish its list of members. In this

contain the name and address of all members who belong to the

were invited to the assembly of the association. Based on the list wanted the

OFD control whether the members of the association duly to its

general assembly were invited. The club had significant data

intellectual property concerns about handing over the required list to the OFD. The

Those responsible on the part of the association saw the OFD desired

How to breach the GDPR. The transmission of

desired data to the OFD is not covered by any legal basis.

Although the members had given the association a “consent to the

Processing of special categories of personal data” submitted,

but this does not provide for such a transmission either.

The OFD as supervisory authority

As it turned out in the course of my further research, the

Data request as part of OFD's supervisory activities.

According to Section 27 (1) of the Tax Advisory Act (StBerG), this is responsible for supervision

about those income tax assistance associations that are based in the district of the supervisory

have authority. The supervisory authority is responsible for comprehensive supervision

obliged and authorized. Accordingly, supervision encompasses the entire

che activity, the statutory management of the association as well as

the monitoring of compliance with all for the income tax assistance association

applicable regulations (§§ 13 ff. StBerG). The GDPR is also one

Submission of the list of members not opposed. As far as fulfilling the

regulatory tasks of the OFD according to the Tax Advisory Act

according to the OFD, personal data should be required

collected and also processed and used for the purposes of future procedures

become.

In the specific case, the request by the OFD pursued the purpose

to understand whether all members of the income tax assistance association regularly

invited to the general meetings. By the possibility

to participate in the general meetings, the members are

able to exercise their rights in the association. To check whether the acc.

§ 29 Abs. 1 StBerG actually required assembly by the association

was carried out, the OFD took action. The legal basis for this results

derived from Section 93 Paragraph 1 Clause 1 of the Fiscal Code (AO) i. in conjunction with § 164a StBerG.

After that, it is part of the task of the tax authorities, for testing

of the facts at the board of directors of the wage tax assistance association

the names and addresses of the members of the wage tax assistance association

emerge to request.

Request for publication of the list is in the present case

permitted under data protection law

As a result, the request for a list of members of the wage tax

hilfevereins by the OFD under data protection law, as this is based on

based on a legal standard. Incidentally, § 27 StBerG

regulated that the competent state financial authority is responsible for the supervision of

the income tax assistance associations. The Federal Fiscal Court sums up the range

This supervision far: “The supervision extends to the fact that the clubs

fulfill the obligations imposed on them by the StBerG in §§ 21 to 26

and that they observe all other relevant regulations" (BFH,

Judgment of March 23, 1999 – VII R 19/98). Among the "other relevant

Regulations” should also be the rules of civil association law

Code of Laws and the statutes of the association on general meetings

count lungs.

90

societies

proportionality and necessity

Nevertheless, the measure of the financial authority must be based on the principle of

Align proportionality. In particular, the respective concrete in

The measure in question may be necessary in individual cases. The Principles

of proportionality and necessity seemed to me in the present

Facts to be taken into account by the tax authority.

91

Economy, banks, self-employed

11. Economy, banks, self-employed

Economy, banks, self-employed

11.1

Transmission of personal data as part of a

Sale of receivables by a bank to a collection agency

The transmission of claim data to a debt collection company

by a bank in its capacity as seller of a claim

Art. 6 (1) lit. c GDPR i. V. m. § 402 BGB permissible. A consent to

the data transmission by the data subjects is not necessary in this case.

In the reporting year, my office received more and more submissions regarding the

Question of the admissibility of data transmissions in the case of debt sales

received.

In all cases, a bank's own attempts at collection were unsuccessful

remained, creditor of a claim not settled by the customer.

Therefore, the banks decided in some brought to my attention

Cases, the respective claims on third parties on the recovery of

Receivables are specialized to sell. Since the receivables data

represent son-related data within the meaning of the DS-GVO and these to third parties,

here the respective buyer of the receivables, it was necessary to check whether

this data transfer was lawful.

Data protection is a transfer of personal data

lawful if it can be based on a legal norm.

Art. 6 Para. 1 DS-GVO defines the requirements that must be met

to ensure that the transfer of personal data is lawful.

Art. 6 Para. 1 GDPR

1. 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;

b) the processing is necessary for the performance of a contract to which the party concerned

fene person is, or necessary to carry out pre-contractual measures, the

be made at the request of the data subject;

c) the processing is necessary for compliance with a legal obligation imposed by the

Controller is subject to;

d) the processing is necessary to protect the vital interests of the data subject

or to protect another natural person;

f)

e) the processing is necessary for the performance of a task carried out in the public domain

interest or in the exercise of official authority, which the person responsible

was transferred;

the processing is to protect the legitimate interests of the person responsible

or a third party, unless the interests or fundamental rights and

Fundamental freedoms of the data subject, the protection of personal data

require, especially when it comes to the data subject

is about a child.

Point (f) of the first subparagraph shall not apply to public authorities in the performance of their duties

processing carried out.

The cases presented to me for examination concerned the sale of

open claims and the associated transmission of personal

personal data of the respective debtors to the buyer of the receivables.

In principle, the Bank is entitled, as part of a business

cal decision to determine that it will not collect claims itself,

but sold them to a third party. The sale of receivables itself represents

a legal purchase according to § 453 BGB. From this contractual constellation

the buyer of the receivables has a right to the transfer of the

Claim according to §§ 398 ff. BGB and for transmission of the claim data

by the seller in accordance with § 402 BGB, so that he can meet the claim

can assert against the debtor.

§ 402 BGB

The previous creditor is obliged to provide the new creditor with the information necessary to assert the

to provide the information required for the claim and to provide him with the information serving as proof of the claim

Deliver documents in his possession.

According to § 402 BGB, the previous creditor (receivable seller,

here the bank) obliged to pay the new creditor (receivables buyer,

here the debt collection company) the corresponding claim data and

to submit the necessary documents.

Since this is a legal obligation, the data

transmission based on the provisions of Article 6 (1) (c) GDPR i. in conjunction with Section 402

BGB are supported. Consequently, there is also consent to the transmission

not necessary on the part of the person concerned.

94

Economy, banks, self-employed

11.2

Use of credit union member information

by a member of the cooperative

Members of the cooperative may use the information sent to them by the bank

Process data of other cooperative members for a specific purpose. A

The bank cannot claim for early deletion

be made.

During the reporting period, a cooperative bank approached me and

for support in enforcing a request for deletion against

asked about a cooperative member. The member had at the time

the Volksbank to release the data of the cooperative members

(names and addresses) asked for these about his opinion regarding

of a possible merger of the bank with another institution

can. The bank then has the data to the member accordingly

provided. Several months after receiving the data, the member

However, these have not yet been used, so that the bank now demanded

to delete this data.

However, the member did not comply with the request, which is why the bank

contacted my authority.

As a preliminary point, it should be noted that the transmission of the

Data both on the regulations from § 31 Genossenschaftsgesetz (GenG)

as well as the Bank's Articles of Association.

§ 31 GenG

(1) The list of members can be created by any member or by a third party who has a legitimate

legitimate interest, can be viewed at the cooperative. transcripts out

of the list of members are up to the member with regard to the entries concerning him

request to grant.

(2) The third party may only store and use the transmitted data for the purpose

the fulfillment of which they are communicated to him; storage and use for others

purposes is only permissible if the data should have been transmitted for this purpose. Is

the recipient is a non-public body, the cooperative must inform him of this;

in this case, storage and use for other purposes requires consent

the cooperative.

The data transmission by the bank to the cooperative member was

therefore according to Art. 5 Para. 1 lit. a i. In conjunction with Art. 6 (1) lit. b, c GDPR lawful.

There was a membership relationship between the bank and the member

which grants the member certain statutory rights, including the

view the list of members. In addition, there was also a clear legal

regulation in the GenG.

The recipient stated that he wanted to use the data to inform the other

members of the senate in writing by what it deems necessary

to persuade the amendment of the articles of incorporation.

Since the other members after more than four months after receiving the

Data were not contacted, the bank requested the deletion of the matter in question

standing data from the member. This was on the part of the recipient with the

reason that it had not been possible for him to date

be to send the letters. So the bank gave him a copy

made available to the list of members, but not in a common way

Format transmitted so that the data of the approximately 21,000 members manually

were to be formatted for sending.

In terms of data protection law, there was therefore a right to erasure against the

don't limb According to Art. 5 Para. 2 DS-GVO, personal data must be

used for specified, explicit and legitimate purposes. It was

In the present case, it is not apparent that the recipient received the data in question

would be processed for a different purpose than originally intended by the member

specified. The Bank's request was therefore rejected in the present case

because the data processing was lawful.

11.3

Redactions on documents obtained from a credit institution

were requested

If a bank requests documents from a customer, they can

Blackenings are only made in individual cases. On copies of to

ID papers presented for identification may be blacked out in principle

not be made.

I keep getting complaints that blackening on companies

documents requested by banks and then make a copy of them

were handed over will not be accepted. First of all,

distinguish between copies of ID cards created to verify identity

or requested, and other documents.

According to §§ 10 paragraph 1 number 1, 11 paragraph 1 sentence 1 money laundering

schegesetz (GWG) obliged to contractual partners, authorized representatives and

identify beneficial owners. Contractual partner is fundamental

every customer of a bank. Beneficial owners are persons

who actually exercise control over assets. To the

Identification are first name and surname, place of birth, date of birth,

Determine and record citizenship and residential address

to. The identification of persons takes place according to § 12 paragraph 1 sentence 1 number 1

GWG usually by presenting a valid official ID

Photograph or similar documents.

Banks are authorized to document the identification and

obliged to make and record a copy of the submitted documents

maintain. This obligation results from Section 8 (3) sentence 2 GWG. The

Processing of the collected data is due to legal obligation

permissible according to Art. 6 (1) (c) GDPR.

Since the identification obligation applies only to those specified in the law

Characteristics extended and in particular not typical in an identity card

included personal characteristics such as eye color or height, was

de previously partially assumed that data on copies, their collection

is not required may be redacted. on these discussions

the legislator reacted with the clarification in the GWG and regulated that

“complete” copies of identity documents may be made and

must. This clarification has led to uniform possibility

was rejected for redacting on copies of ID card copies. Although is

due to further changes in the GWG, the word "complete" is omitted again.

However, this does not result in the possibility of blackening again

to do. The legislature did not want such a change

carry out.

In addition, the copy of a document must always be unadulterated.

If the copy contained blackening, it would be a so far

act at least a modified copy of the original document.

Blackening of identity documents presented for identification and

are copied to document the identification are therefore fundamentally

not permitted.

Other documents requested by credit institutions are individual

to look at. A legal obligation to make copies

of these documents does not exist in principle. Therefore, processing

of the data collected is often only due to a legitimate interest

credit institute according to Art. 6 Para. 1 lit. f GDPR. here is

to check individually whether a credit institution has a legitimate interest in the

Production or transfer of unredacted copies, that of the

Interests and freedom rights of data subjects are not outweighed.

A legitimate interest can arise from a credit check

of the risk taken with a loan. Used by one

If a bank grants a loan, it is fundamentally entitled to

to check risks arising from the repayment of the loan.

For this purpose, a credit institution is usually allowed to provide documents on income and

request the financial situation. Such documents can often only

be assessed in context. Blackening on these documents

cannot always be recognized as harmless if the content of the

blackened field or the content of the blackening is unknown. Under-

locations are also seldom so strongly standardized that already from the location of the

Blackening on the base whose harmlessness would be recognizable. This

This is especially true for payslips, where many components are used to

Checking the plausibility of the entire document is required.

It is therefore often the result of a consideration that a credit institution has an interest

resse to provide unredacted copies to ensure authenticity

and to be able to check the authenticity of the copied document. In individual cases

however, in appeal proceedings, the inadmissibility of the requirement

from unredacted copies.

This was the case, for example, with the provision of copies of rental agreements

genes whose income served as proof of income without the affected

Property should serve as security for a loan granted. In this

In this case, it was also necessary to take into account that this was third-party data

acted by the contractual relationship between the customer and the

Bank were not affected. An interest of the credit institution in the

The content of the rental agreement was to be acknowledged, but this included

not the interest in knowing the name of individual tenants. Whose

Rights to the omission of data processing therefore outweigh that

Interest of the bank in knowing this data. To that extent was

therefore the person concerned is entitled to blacken the name.

However, if the rights from a concluded rental agreement as security

security for a loan granted is also a different assessment

possible. This applies in particular if the rights to payment of the

rent to be assigned to a bank as security.

In another case, a credit card company wanted unusual ones

Payment transactions with the issued credit card by viewing the

check the unredacted account statements of their customer's current account.

The credit card company feared an increased risk because the payment

development processes are typical for the preparation of a fraud. In this

In this case, however, the credit card company had other and obvious

their options for risk limitation or avoidance.

Also to check whether there is a situation that points to money laundering or

one of their predicate offenses indicates or is indicative of terrorist financing

98

Economy, banks, self-employed

Contains abnormalities or unusual features was the requirement of the

unredacted account statements are not permitted. § 25 h Banking Act

(KWG) does not justify such an inspection. Financial

undertake an immediate exchange of information on individual

Transactions according to Section 47 (5) GWG. A bypass of there

regulated requirements for an exchange of information by

Requesting bank statements from data subjects is not permitted.

Two other cases concerned the redacting of health data. In

Account statements for an account held at another bank,

specified by a credit institution for the credit check when lending

were requested, such health data were due to the settlement

included in medical bills. Since this information is neither for the credit

were relevant to the award, nor a legal basis for their processing

was recognizable, this data was allowed to be blacked out on the account statements

become. Also in a pension notice that is due to the granting

a disability pension had been granted, the information was allowed

be blacked out on the reason for the granting of pensions. Here they are too

Health data not required to assess creditworthiness.

In addition, the general ban on health data applies to health data

Processing in accordance with Art. 9 Para. 1 DS-GVO, unless an exceptional

according to Art. 9 Para. 2 DS-GVO. In both cases there was one

Exception not recognizable.

11.4

Data collection on the factory premises of a company

Reading data from the ID card using an optical

reading device for access control is only permitted with consent

signed If data subjects do not give their consent, the data can

be collected manually.

At the entrance to a company's factory premises, a

establishes and documents which persons do this, when and for what purpose

Enter the factory premises and then leave again. become

personal data of visitors and suppliers processed.

As part of the registration process, there are two entrances to the factory premises

optical scanners used, in which the identity cards or others

ID documents of the visitors are inserted. Capture these scanners

Personal data of visitors (last name, first name, ID number

mer and validity of the document as well as the signature with which the

visitor or supplier confirms that the safety briefing has been carried out).

This serves to avoid manual transmission errors and

Shortening of registration times. Then the security

sonal the type of ID (e.g. ID card), the company for which the

visitor is active, the recipient of the visit, the date and time of the

Start of visit and end of visit added manually. The such

The data collected will be stored for a period of twelve months.

The legal basis for data collection is questionable. The company concerned

6 (1) lit. c GDPR i. V. m. § 4 No. 1 lit. c

and No. 4 Hazardous Incident Ordinance - 12th BImSchV (Federal Law Gazette I 2017 p. 483).

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

(...)

c) the processing is necessary for compliance with a legal obligation imposed by the

Controller is subject to;

(...)

§ 4 Hazardous Incident Ordinance - 12th BImSchV

The operator has to fulfill the obligation resulting from § 3 paragraph 1 in particular

1. Take measures to prevent fires and explosions

a)

b) Not from one facility to another in a way that would affect safety

be avoided within the operational area,

Plants of the operating area can affect and

c) not from the outside in a way that would affect the safety of the area of operation

can affect him

1a. take measures to prevent releases of hazardous substances into air, water or

ground are avoided,

2. the operating area with sufficient warning, alarm and safety devices

to equip

3. the facilities of the operating area with reliable measuring devices and control or

Equip control devices that, insofar as this is required for safety reasons, respectively

are multiple, diverse and independent of each other,

4. to protect the safety-relevant parts of the operating area from unauthorized access.

100

Economy, banks, self-employed

§ 3 Hazardous Incidents Ordinance – 12th BImSchV

(1) The operator has to take the measures necessary according to the type and extent of the possible dangers

take precautions to prevent accidents; Obligations after other than

immission control regulations remain unaffected.

(...)

Due to its operator obligations, the company must be responsible for the

competent authorities control and document who has access and why

to the factory premises. Visitor management also serves to

Data protection, as it prevents unauthorized access to the factory premises

dere, and is therefore an important part of data protection law

access control.

On the other hand, Article 6 (1) (f) GDPR was cited as the legal basis.

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

(...)

f)

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.

(...)

The company has a legitimate interest in gaining access to

its locations, in particular to protect property, only to

authorized persons and to exercise the domiciliary rights accordingly.

There are overriding interests of the data subjects that are worthy of protection

not against.

Visitor management was discussed with representatives of the company concerned

mens discussed in detail in a personal conversation in my house.

Reading the data from the ID card (first name, surname, ID card

number and validity) by means of an optical reader on the basis of Art. 6

Paragraph 1 lit. c GDPR i. V. m. § 4 No. 1 lit. c and No. 4 Major Accidents Ordinance - 12.

BImSchV or Art. 6 Para. 1 lit. f DS-GVO I consider as data protection law

impermissible. § 4 No. 1 lit. c and No. 4 Major Accidents Ordinance - 12th BImSchV

already factually does not legitimize such data collection. Also

is data collection to protect property as a legitimate interest

not mandatory. In addition, there are overriding interests of those affected

towards people. Such data collection is only possible by means of consent

agreement of the data subject possible. This also makes § 20 paragraph 2 sentence 3

of the Personal Identity Card Act (PAuswG).

§ 20 PAuswG

(2) (...) Personal data are extracted from the ID card by photocopying

collected or processed, the data collecting or processing office may only do this

with the consent of the card holder.

(...)

On the other hand, I also consider the manual entry of data by hand

permissible without consent. The data collection process was

adapted according to my specifications in such a way that the use of the

optical scanner only takes place on the basis of consent. Granted the

Those affected do not give their consent, the data can be entered manually

become. Corresponding data protection notices can be found in the reception area

be viewed. These indicate that the use of the optical

reading device on a voluntary basis.

In addition, I have a further optimization of the security level with regard to

the safe storage of the collected data is advised.

11.5

Wage and salary accounting by tax consultants

The wage and salary accounting is carried out by tax consultants

not qualify as order processing. A relevant contract

for order processing i. s.d. Art. 28 DS-GVO is not to be concluded.

According to the previous legal situation, it was undisputed that the classic tax

Advisory activity not as order processing i. s.d. Art. 28 GDPR

is to qualify. This activity is carried out on one's own responsibility and with

independent decision-making power. However, it became very controversial

the classification of wage and salary accounting by tax consultants

discussed. Since tax consultants who carry out this work for employers

Employee data according to fixed rules and without own decisions

processing latitude, so far I have had an order processing i. s.d.

Art. 28 GDPR accepted. Correspondingly, with mixed performance

offered, d. H. the performance of both classic tax advice and

102

Economy, banks, self-employed

also the wage and salary accounting by tax consultants, every service

to be assessed separately. Then was regarding the payroll accounting

to conclude an order processing contract.

Art. 28 GDPR

(1) If processing is carried out on behalf of a person responsible, then this person only cooperates

Processors who offer sufficient guarantees that appropriate technical

and organizational measures are carried out in such a way that the processing

sounded with the requirements of this regulation and protecting the rights of

data subject guaranteed.

(...)

(3) The processing by a processor takes place on the basis of a

contract or any other legal instrument under Union law or the law of the

Member States that control the processor in relation to the controller

binds and in the object and duration of the processing, type and purpose of the processing

tion, the type of personal data, the categories of data subjects and the

Obligations and rights of the person responsible are defined. (...)

(...)

As a result of a change in the law, this view has to be revised. According to

Section 11 (2) of the Tax Advice Act (StBerG, Federal Law Gazette I p. 2451).

the processing of personal data by tax consultants and

other persons and companies mentioned in § 3 StBerG (e.g. business

auditors and tax consulting companies) in compliance with the applicable

free from professional duties. These are in the processing of all

personal data of their clients responsible according to Art. 4

No. 7 GDPR. According to the explanatory memorandum, the regulation applies

(BT-Drs. 19/14909 p. 59) for all activities of the tax consultant; the

The type of activity is therefore irrelevant.

§ 11 StBergG

(...)

(2) The processing of personal data by individuals and companies

§ 3 takes place without instructions, taking into account the professional duties applicable to them. The people

and companies according to § 3 are in the processing of all personal data

their clients responsible according to article 4 number 7 of the basic data protection

regulation (EU) 2016/679. Special categories of personal data pursuant to Article

9 paragraph 1 of Regulation (EU) 2016/679 may, in accordance with Article 9 paragraph 2 letter g

of the General Data Protection Regulation (EU) 2016/679 are processed in this context.

§ 3 StBergG

The following are authorized to provide commercial assistance in tax matters:

1. Tax advisors, tax agents, lawyers, established European

Lawyers, auditors and chartered accountants,

2. Partnership companies whose partners are exclusively those named in number 1

th people are

3. Tax consulting firms, law firms, auditing

companies and accounting firms.

(dropped out)

4.

This means that wage and salary accounting is carried out through tax

rater no longer qualify as order processing. A corresponding

relevant contract for order processing i. s.d. Art. 28 GDPR between

Client and tax consultant is not closed.

The processing of health data and other "sensitive" data

i. s.d. Art. 9 Para. 1 GDPR i. r.d. Activity of tax consultants is based

to Art. 9 Para. 2 lit. g GDPR i. V. m. § 11 paragraph 2 sentence 3 StBerG.

Art. 9 GDPR

(1) The processing of personal data revealing racial and ethnic

Origin, political opinions, religious or philosophical beliefs or the

trade union membership, as well as the processing of genetic data,

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

health data or data relating to the sex life or sexual orientation of a natural person

person is prohibited.

(2) Paragraph 1 does not apply in the following cases:

(...)

g) the processing is based on Union law or the law of a

Member State proportionate to the objective pursued

Respects the essence of the right to data protection and adequate and specific

Measures to safeguard the fundamental rights and interests of the data subject

provides, necessary for reasons of substantial public interest,

(...)

Finally, it should be noted that if the

Wage and salary accounting to other, non-tax consulting service providers

an order processing contract must still be concluded.

104

Economy, banks, self-employed

11.6

Collection of guest/customer data during the Corona pandemic

The collection of guest data by restaurants and customer data

by hairdressing companies in the course of the corona pandemic has various

data protection issues were raised. These led to

gen legal uncertainties and a high number of submissions to my

Authority.

After the end of the Corona-related closures, restaurants and

other catering establishments will be offering food and drinks again from mid-May 2020

offer for on-site consumption. The prerequisite for this, however, was that in addition to

the data of the guests in compliance with the rules of distance and hygiene

are recorded. A corresponding provision can be found in Section 4 Paragraph 2 No. 3

the Corona Contact and Operating Restriction Ordinance (CoKoBeV,

Valid from May 15th, 2020, GVBl. p. 309). This provides a legal basis

i. s.d. Article 6 (1) (c) (3) GDPR. The provision was later

Versions of the CoKoBeV slightly modified, changes in content

however, did not result from this.

§ 4 CoKoBeV

(...)

(2) From May 15, 2020, the establishments named in paragraph 1 may serve food and beverages

also offer for consumption on site if it is ensured that

(...)

3. Name, address and telephone number of guests to enable tracking

of infections recorded by the business owner

become; they have the data for a period of one month from the start of the visit

protected from inspection by third parties for the competent authorities

and to transmit it to them upon request and immediately after the expiry of the

Delete or Destroy Deadline; the provisions of art. 13, 15, 18 and 20 of the

General Data Protection Regulation on the obligation to provide information and the right to information

on personal data do not apply,

(...)

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

(...)

c) the processing is necessary for compliance with a legal obligation imposed by the

Controller is subject to;

(...)

(3) The legal basis for the processing pursuant to paragraph 1 letters c and e

set by

a) Union law or

b) the law of the Member States to which the controller is subject.

The purpose of the processing must be specified in this legal basis or with regard to

the processing pursuant to paragraph 1 letter e is necessary for the performance of a task

which is in the public interest or in the exercise of public authority which

responsible has been transferred. This legal basis may contain specific provisions
contain genes to adapt the application of the provisions of this regulation, under
other provisions on what general conditions governing the regulation of
Lawfulness of processing by the controller apply what types of data
are processed, which persons are affected, to which institutions and for which
Purposes the personal data may be disclosed, which purpose limitation
they are subject to how long they may be stored and which processing operations
and procedures may be applied, including safeguards
lawful and fair processing, such as for
other special processing situations in accordance with Chapter IX. Union law or that
Member State law must pursue an objective in the public interest
and proportionate to the legitimate purpose pursued.
(...)
Shortly after the CoKoBeV came into force, there was a high number
of complaints to my authority. Data collection was often
for simply visiting a restaurant or a café as unreasonable
considered reasonable. Some petitioners also feared the creation of any
Personality profiles, since the guest lists make it clear when
where they would have stayed. In the period that followed it was open
Keeping the guest lists more often the subject of complaints. Some innkeepers
laid out lists for all guests, so that third parties could see the data
other guests could see. Some complaints were directed against
the collection of inadmissible data, such as e-mail addresses. Further
there were several submissions alleging the improper use of the
criticized the collected guest data. These are, for example, for
men or other calls have been misused. In a few individual cases

Were these complaints justified? On my respective notice

the restaurants have seen their misconduct and in the future

behave in accordance with the law.

Many operators were unsure about how to deal with data protection

legal requirements can be identified. I could understand this well

since these are - in an already very stressful situation - next to the

various other pandemic-related requirements regarding distance and

Hygiene rules also with data protection regulations that are unfamiliar to them

faced.

To support the innkeepers I already shortly after the entry into force

of the CoKoBeV in May 2020 on my website

Handling of guest data published. The relevant requirements should

be summarized again below.

Only those included in § 4 Para. 2 No. 3 CoKoBeV are allowed to be guests

Data and thus only name, address and telephone number are recorded.

The collection of other data, in particular an e-mail address as well as

a signature of the guest is not permitted. manifestly incorrect information,

such as pseudonyms or "joke names" do not meet the requirements of the

CoKoBeV. However, since incorrect information was often given,

was introduced in a later version of the CoKoBeV (valid from October 19, 2020,

GVBl. p. 717) also added a regulation according to which the guests

are obliged to provide the data completely and truthfully and they

upon request, their identity card, passport, passport substitute or substitute identity card

submit for verification of their information.

A specific form of data collection is not intended. the gas

However, test data must not be accessible to the public or to other people

be visible. The data can be recorded by staff or

the guests can be given individual sheets to fill out. Also

Electronic data collection (e.g. using a QR code or a

app) is possible.

The operators are not obliged to provide information about the data collection

exempted according to Art. 13 DS-GVO. Nevertheless, it is advisable to start with the

To communicate the collection of the data (e.g. by means of a clearly visible

information in the restaurant and on the registration forms) that the data collection

exercise for the purpose of tracing chains of infection

of Art. 6 (1) lit. c GDPR i. 1 Clause 1 No. 2 lit. b CoKoBeV

takes place and that the provisions of Art. 13, 15, 18 and 20 DS-GVO no

Find application. The following passage is recommended: "The data

Data is collected for the purpose of tracking infection chains

Based on Art. 6 Para. 1 lit. c GDPR i. In conjunction with Section 4 Paragraph 1 Sentence 1 No. 2 lit. b

the Corona Contact and Operating Restriction Ordinance (CoKoBeV). The

Provisions of Articles 13, 15, 18 and 20 GDPR do not apply."

After the collection, the guest data is protected against inspection

to be stored by third parties, for example in a locked cupboard or safe,

to which as few people as possible should have access.

Since the guest data for a period of one month from the start of the visit

are to be kept available, it is advisable to keep the guest data accurate to the day and

to destroy them one month after the guest's visit. if the

competent authority the release of the guest data before the end of the

Month has requested, the guest data are to be handed over to them and

then to be destroyed immediately.

The guest data are regularly sent to the health authorities, in urgent cases

the local regulatory authorities, cf. § 7 CoKoBeV. The

Data may not be transmitted to any other body. These are too

not for any other purpose, such as making phone calls as a result of an unpaid

bill of a guest to use.

§ 7 CoKoBeV

Deviating from § 5 para. 1 of the Hessian law, for the implementation of this ordinance

about the public health service from September 28, 2007 (GVBl. I p. 659), last

amended by the law of May 3, 2018 (GVBl. p. 82), in addition to the health authorities

local regulatory authorities responsible if the health authorities are not reached in time

or can take action to avert an existing dangerous situation.

The deletion or destruction of guest data must be secure and data-

be carried out in a protective manner. Data captured on paper is about in a

to destroy document shredders or paper shredders. As to ensure

is that third parties do not gain knowledge of the guest data,

tearing it up by hand or simply throwing it away is sufficient

not the paper waste.

For the purpose of checking whether the data protection requirements are also met in the

Practice is sufficient, I have a questionnaire to 100 all over Hesse

Distributed catering establishments sent. It turned out that the companies

largely meet the data protection requirements.

The survey is carried out almost continuously in paper form on individual sheets.

The DEHOGA Hessen e. V. used. The

secure storage and destruction of data were the participants

mostly conscious. However, there were often uncertainties about

the correct retention period of one month. A release of

data was denied without exception.

Furthermore, in cooperation with DEHOGA Hessen e. V

corresponding information on the collection of guest data at restaurants

distributed.

With these measures, I was able to make a significant improvement in terms of

achieve compliance with data protection regulations. This showed

also reflected in the fact that the number of complaints to my authority

was noticeably declining. Many innkeepers thanked for the provided

Information with which you can comply with the data protection requirements in

could better meet the practice.

In addition to collecting guest data in restaurants, I was also busy

the data collection of the customers of hairdressing companies. Other than for guest

There were initially no statutory facilities for hairdressers in the CoKoBeV

Basis for collecting customer data. Nonetheless, the

Professional Association for Health Services and Welfare (BGW)

a guide to the collection of customer data, but some

data protection issues, in particular with regard to the legal basis

of data collection.

In order to also help the hairdressing companies to comply with data protection regulations

To support requirements, I released one in mid-May 2020

appropriate help on my website. My recommendations

largely based on the regulations of data collection

Restaurants according to the CoKoBeV. In the absence of an express legal basis

I consider the collection of customer data by hairdressing companies based on

of Art. 6 Para. 1 lit. f DS-GVO for admissible.

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

(...)

f)

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.

(...)

In the case of hairdressers, too, particular attention must be paid to the fact that the

Customer data cannot be viewed by third parties and the data is

destroyed within one month in accordance with data protection regulations. in the

different from the restaurants, hairdressers were neither informed

13 DS-GVO exempted, restrictions still existed

in fulfilling the rights of data subjects according to Art. 15 et seq. DS-GVO.

In a later version of the CoKoBeV (valid from October 19, 2020, GVBl.

p. 717) then became an explicit legal requirement for hairdressing companies

Data collection scheme created, based on the already existing

Regulation for restaurants, cf. Section 6 (3) CoKoBeV. Henceforth the

Data collection by hairdressers based on Article 6 Paragraph 1 Letter c

Para. 3 DS-GVO i. V. m. § 6 Abs. 3 CoKoBeV legitimized.

§ 6 CoKoBeV

(...)

(3) The operators of companies and facilities according to paragraph 2 sentence 1 have to ensure

that name, address and telephone number of the customers only

collected to enable contact tracing of infections; They have

the data is protected from inspection for a period of one month from the start of the visit

me by third parties for the responsible authorities and upon request to them

to be transmitted securely and in accordance with data protection regulations immediately after the deadline has expired

delete or destroy; the provisions of Art. 13, 15, 18 and 20 of the data

General Protection Regulation do not apply; the customers are over

inform of this restriction.

Although the number of complaints regarding data collection

Hairdressers, which was less than restaurants, also reached me

some submissions in this regard, in particular regarding the open conduct of

customer lists and misuse of customer data. Also

here, however, a steady decrease in complaints was recorded, so

that the data protection requirements on the part of the hairdressing companies

have been increasingly complied with in practice.

11.7

Secure document destruction at law firms

with persons subject to professional secrecy, such as lawyers

special duties of care in the data protection-compliant destruction of

Paper documents and working documents containing personal data

third party included.

One complainant turned to the HBDI, stating that he had

fully legible paper documents from a law firm in the paper

Waste container found in an apartment building. the complainant

rer sent photos of numerous documents as evidence. underneath

there was confidential correspondence with clients, account statements,

Invoices and other documents containing personal data. in a

In another case, the HBDI was told that paper documents were a

Law firm with confidential personal data about a

were spread out on the ground. Recover the designated documents

in the wrong hands, there is great potential for abuse.

Since those responsible were subject to professional secrecy,

who regularly deal with a large amount of confidential personal data

circumvent, the circumstances weighed more heavily than when it was a matter of responsibility

would have acted verbatim without the professional secrecy capacity. One

unauthorized knowledge of third parties has taken place at least in the first case

and could take place at any time in the second scenario.

Above all, there is always the risk that paper documents on the

way of disposal are lost. Even if this is analog processing

ted personal data results from the stored

There is a considerable spread due to the routes used by the waste disposal companies.

In any case, it should be noted that paper documents with personal

pulled data that does not come from the private sector, by means of a

document shredder or a qualified waste disposal service.

These are technical and organizational measures

i. S.v. Art. 32 DS-GVO, which ensures the security of the processing of personal

ensure related data.

Art. 32 GDPR

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

Type, scope, circumstances and purposes of processing and the different

probability of occurrence and the severity of the risk to rights and freedoms

of natural persons, the person responsible and the processor shall take suitable measures

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

to ensure level;

(...)

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

to be taken into account that are associated with the processing, in particular by - whether

accidental or unlawful - destruction, loss, alteration or unauthorized

Disclosure of or unauthorized access to personal data that

transmitted, stored or otherwise processed.

(...)

For this purpose, the state of the art is used for particularly sensitive data

at least security level P-4 according to the DIN/ISO 66399-2 standard

to fulfill. This security level prescribes a shredding using the

so-called particle cut (cross-cut). Similar occurrences are

already discussed in my previous activity reports

(cf. 48th activity report, p. 72 ff.). Even in an increasingly digitized world

World should be dealt with properly and destroyed safely

of paper documents.

After completing the investigation of the facts, I have the necessary

regulatory action taken.

12. Credit bureaus, collection agencies

credit bureaus, collection agencies

12.1

Scoring procedure of SCHUFA Holding AG

To improve the scoring results achieved, SCHUFA Holding

AG (SCHUFA) modified their scoring procedure and the modified scoring

procedure explained.

As a business secret, the SCHUFA scoring process is subject to a

special protection and must also be approved by SCHUFA in the course of fulfilling

Information obligations according to Art. 15 DS-GVO are not disclosed in detail

(Federal Court of Justice, judgment of January 28, 2014, Az. VI ZR 156/13, https://juris.bundesgerichts-

hof.de/cgi-bin/rechtssprachung/document.py?Gericht=bgh&Art=en&sid=d16415a2f-

250c4a65e28a44a9ee34a17&nr=66910&pos=0&anz=1). Opposite me is the

SCHUFA nevertheless discloses its scoring process within the framework

committed to my supervisory activities. SCHUFA is this obligation

complied without being asked after changes in the scoring process.

SCHUFA explained in detail both the changed procedure

as well as the reasons for the changes in the procedure. Additionally

SCHUFA presented a scientific report in which the

procedure is analyzed and evaluated.

The SCHUFA presentation and the content of the report showed that

that the procedures used meet the requirements for scoring procedures

according to § 31 Section 1 No. 2 BDSG. With the methods used

It is a question of both the content of the report submitted and the

also according to my knowledge about scientifically recognized mathematical

table-statistical procedures. The data used are to calculate the

Significant probability of repayment of a loan granted.

Neither from the description of the SCHUFA nor from the content of the report

doubts arose.

With the change to the previous procedures, the SCHUFA

used scoring methods to newer scientific developments

adjusted for the score value calculation. With the change in procedure,

improvements in selectivity and thus in score values are to be expected. The

I therefore see the change in the process as positive.

113

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

12.2

The implementation of the information obligation according to Art. 14 DS-GVO im

area of credit bureaus

In the event of third-party collection of personal data by

According to Art. 14 DS-GVO, a proactive and for the

data subject without cause from credit bureaus

the person concerned.

A significant number of complaints result from the information provided by credit bureaus
letters sent to those affected against the background of the information
obligation according to Art. 14 DS-GVO. If personal data is stored in a
collected from third parties and not directly from the data subject (so-called
"Third-party collection"), the person responsible is obliged to inform the data subject
person to provide the information listed under Art. 14 DS-GVO.
This includes i.a. Name and contact information
of the person responsible, the contact details of the data protection officer, the
Purposes and the legal basis of the data processing as well as explanations
to the rights of those affected. It should also be noted that credit bureaus
Information in principle not only with third parties, but also through third parties
can raise.
The information obtained from credit bureaus by sending information letters
Fulfilled legal obligation according to Art. 14 DS-GVO leads to the
Recipients regularly cause irritation, as the information is often incorrectly inter-
be valued. So far, a large number of recipients have not had one
knowingly perceived touchpoints with credit bureaus and passes
erroneously from abusive collection and processing of the data
personal data.
Credit bureaus are private commercial companies. She
collect information about the identity, the economic activity, the
creditworthiness, the willingness and ability to pay of companies and
private individuals. This information is stored and passed on to third
communicates if they have a legitimate interest in such information
have. In particular, credit bureaus may process various personal data
Data based on a balancing of interests according to Art. 6 Para. 1 lit. f GDPR

process. Among other things, the processing of identification data (e.g.

surname, first name, address, date of birth and previous addresses). This

Information is used to correctly assign the data and to avoid

of mistaken identity. In addition, the calculation

of score values by credit bureaus permitted, provided that the requirements are met

of Art. 6 (1) lit. f GDPR i. V. m. § 31 BDSG are fulfilled. doing so

114

credit bureaus, collection agencies

these are statistically based prognosis values for the future

Risks of non-payment, which, for example, serve as a decision

terium can be used to determine whether a purchase on account

Distance selling shops on the Internet is offered. Thus the implementation

the obligation to inform those affected with regard to knowledge of the

own score increasingly important.

A fact that is often recurring in official supervisory practice

In particular, address research by credit agencies

en in the case of undeliverable letters due to a move.

If, for example, a purchase on account results in a credit

Risk on the part of the creditor, there is a legitimate interest in the

Knowledge of the current address of the invoice addressee in order to

to assert claims. In this case determine

Credit agencies on behalf of the creditor the current address of third parties (e.g.

residents' registration offices) and then inform those affected about

the data collection and processing according to Art. 14 DS-GVO.

By means of an information letter according to Art. 14 DS-GVO, the person concerned

enables the person to carry out the data processing carried out in individual cases

to be able to understand. Basically, it is additionally recommended that the

To claim information according to Art. 15 DS-GVO. Therefore

credit bureaus are obliged to provide comprehensive and free information about the

to provide information about stored data. If an examination according to Art. 15

DS-GVO shows that personal data is incorrect

are kept in the database of credit bureaus, there are claims to

Correction, deletion or restriction of processing

Data according to Art. 16 to 18 GDPR.

As a result, the active information

obligation for credit agencies in the case of third-party surveys on a guarantee

the transparency of the data processing processes and facilitates in the

At the same time, follow the possible exercise of data subject rights.

12.3

Permissibility of the processing of (claims) data by the

collection agency

The processing of personal data of alleged debtors

on the part of the collection agency (hereinafter: IKU) is also in the cases of

mistaken identity or in cases where it turns out

that the claim on the part of the debtor already exists

Mandate of the IKU to the creditor or also after mandate of the

IKU was paid directly to IKU, initially permissible in principle.

I often receive complaints from affected persons who refer to the un-

immediate and complete deletion of your data from the data set

of the respective IKU.

The complaints are justified by the fact that the person concerned

not the debtor of the claim asserted or the claim in

has already been settled as part of the debt collection process. A storage of

Corresponding data from the IKU is therefore no longer required

and it has to be deleted.

In other, but rare cases, the debtor is executed

already have the claim to the creditor before IKU was mandated

paid. Data transmission to the IKU and storage there

of the data subject are therefore unlawful.

Basic information on the admissibility of data processing on the part of

of the IKU

In principle, the mandate of an IKU (equal to a law firm)

for the purpose of realizing outstanding claims due to private

tonomy allowed. For this purpose, the transmission of data (contract or

Claim data and data of the debtor, in particular names

men and address, the reason for the claim, the amount and the due date of the

Claim etc.) on the part of the creditor to the IKU is required and out

Not objectionable from a data protection point of view: The corresponding data

In these cases, data processing takes place on the basis of Article 6 Paragraph 1 Letter b

DS-GVO to enforce the debtor's fulfillment of the contract

with the creditor and on the basis of Article 6 (1) (f) GDPR

Protection of legitimate interests of IKU or the creditor.

The data subject consents to this data processing

therefore not necessary. If the data subject to the

If IKU revokes any consent that may have been granted (preventively), such a

revocation consequently stand there; this is from a data protection point of view

simply not relevant.

Art. 6 Para. 1 DS-GVO reads as follows:

116

credit bureaus, collection agencies

Art. 6 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;

b) the processing is necessary for the performance of a contract to which the party concerned

fene person is, or necessary to carry out pre-contractual measures, the

be made at the request of the data subject;

c) the processing is necessary for compliance with a legal obligation imposed by the

Controller is subject to;

d) the processing is necessary to protect the vital interests of the data subject

or to protect another natural person;

f)

e) the processing is necessary for the performance of a task carried out in the public domain

interest or in the exercise of official authority, which the person responsible

was transferred;

the processing is to protect the legitimate interests of the person responsible

or a third party, unless the interests or fundamental rights and

Fundamental freedoms of the data subject, the protection of personal data

require, especially when it comes to the data subject

is about a child.

Point (f) of the first subparagraph shall not apply to public authorities in the performance of their duties

processing carried out.

A right to deletion of data towards the IKU can be in favor

of the person concerned from Art. 17 Para. 1 DS-GVO under those mentioned there

conditions arise.

Art. 17 GDPR reads as follows:

Art. 17 GDPR

(1) The data subject has the right to demand that the person responsible

personal data relating to them are deleted immediately, and the person responsible

verwortliche is obliged to delete personal data immediately if one

the following reasons apply:

a) The personal data are relevant for the purposes for which they were collected or referred to

processed in any other way is no longer necessary.

b) The data subject withdraws their consent on which the processing is based

Article 6(1)(a) or Article 9(2)(a), and it

there is no other legal basis for the processing.

c) The data subject objects to the processing pursuant to Article 21(1)

processing and there are no overriding legitimate grounds for processing

or the data subject objects in accordance with Article 21(2).

the processing.

d) The personal data have been processed unlawfully.

e) The deletion of the personal data is necessary to fulfill a legal obligation

obligation under Union law or the law of the Member States,

to which the person responsible is subject.

f) The personal data was collected in relation to information services offered

mation company in accordance with Article 8(1).

(2) Has the person responsible made the personal data public and is he

obliged to delete them in accordance with paragraph 1, he shall take into account the

measures appropriate to the available technology and implementation costs,

also of a technical nature, to those responsible for data processing who

process related data to inform that a data subject of

you the deletion of all links to this personal data or copies or

requested replications of this personal data.

(3) Paragraphs 1 and 2 do not apply if processing is necessary

a) to exercise the right to freedom of expression and information;

b) to fulfill a legal obligation that requires processing under the law of

Union or the Member States to which the person responsible is subject, or

to perform a task that is in the public interest or is being exercised

public authority delegated to the controller;

c) for reasons of public interest in the field of public health pursuant

d)

Article 9 paragraph 2 letters h and i and Article 9 paragraph 3;

for archival purposes in the public interest, scientific or historical

Research purposes or for statistical purposes in accordance with Article 89 paragraph 1, to the extent

the law referred to in paragraph 1 likely to achieve the objectives of this

renders processing impossible or seriously impairs it, or

e) to assert, exercise or defend legal claims.

Data processing when the claim has been settled

to the IKU

In the event of the settlement of the claim amount to the IKU and thus the

Completion of the debt collection procedure initially appears to be in accordance with Article 17 (1) lit.

a DS-GVO in favor of the debtor a right to deletion

corresponding data. After all, these are for the purpose

for which you were collected (contract execution/legal prosecution/demand

tion management), no longer required: This purpose is defined by the

Compensation of claims omitted.

Nevertheless, further processing can also be further for other reasons

subsequently be permissible. This is the data processing to fulfill a

legal obligation to which the IKU is subject. Such

legal obligation of the IKU to further data storage arises

in particular from the tax and commercial law storage and

Documentation obligations to which the IKU is subject under § 147 of the Fiscal Code (AO)

118

credit bureaus, collection agencies

and Section 257 of the German Commercial Code (HGB). Then the corresponding

Corresponding business correspondence as well as accounting documents etc. each for one

be retained for a period of six years or ten years. Over and beyond

the data is required for the IKU in relation to one's own activity

settle the client and the debtor and, if necessary, the

Evidence of the entitlement of the collected or claimed

to carry fees. Furthermore, the data is required by the IKU,

to queries from the relevant data protection supervisory authority

To be able to answer within the framework of corresponding individual examinations. After

all this according to 17 paragraph 3 lit. b DS-GVO initially no claim

on deletion.

§ 147 AO and § 257 HGB read as follows:

§ 147 AO (1)

(1) The following documents must be kept in an orderly manner:

1. Books and records, inventories, annual accounts, management reports, opening

balance sheet as well as the work instructions required for their understanding and

other organizational documents,

2. the commercial or business letters received,

3. reproductions of commercial or business letters sent,

4. accounting documents,

4a. Documents according to Article 15 paragraph 1 and Article 163 of the Union Customs Code,

5. other documents, insofar as they are of importance for taxation.

(2) With the exception of the annual accounts, the opening balance sheet and the documents

Paragraph 1 number 4a, provided that the latter documents are official documents

or non-formal proofs of preference to be signed by hand

the documents listed in paragraph 1 also as a reproduction on an image carrier or on

other data carriers if this is consistent with the principles

Accounting conforms and ensures that playback or data is consistent

the received commercial or business letters and the accounting documents pictorially and

correspond to the content of the other documents if they are made legible,

are available at all times during the retention period, can be read immediately

can be made and evaluated automatically.

(3) The documents listed in paragraph 1 no. 1, 4 and 4a are ten years old, the others

to keep the documents listed in paragraph 1 for six years, unless otherwise specified

Tax laws permit shorter retention periods. Shorter retention

Deadlines according to non-tax laws do not affect the period specified in sentence 1. At

received delivery notes that are not accounting documents according to paragraph 1 number 4,

the retention period ends upon receipt of the invoice. For dispatched delivery notes,

which are not accounting documents according to paragraph 1 number 4, the retention period ends

with the sending of the invoice. However, the retention period does not expire if and

as long as the documents are relevant to taxes for which the assessment period

has not yet expired; Section 169 (2) sentence 2 does not apply.

119

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

(4) The retention period begins at the end of the calendar year in which the last

Entry made in the book, the inventory, the opening balance sheet, the financial statements

or the management report drawn up, the commercial or business letter received or sent

been made or the accounting document was created, the recording is also made

has been made or the other documents have been created.

(5) Who to keep documents in the form of a reproduction on an image carrier

or on other data carriers, is obliged to use those aids at his own expense

provide what is necessary to make the documents legible; on

At the request of the financial authorities, he has the documents in full immediately at his own expense

or to print out in part or to teach legible reproductions without aids.

(6) Are the documents according to paragraph 1 created with the help of a data processing system

been, the financial authority in the context of an external audit has the right to inspect the

to take stored data and the data processing system to check them

to use documents. As part of an external audit, you can also request that the

Data is evaluated automatically according to your specifications or you the stored documents

and records are made available on a machine-readable data medium

become. If the taxpayer informs the tax authority that his data according to paragraph

1 are with a third party, the third party has

1. the tax authority to inspect the data stored for the taxpayer

grant or

2. evaluate this data automatically according to the specifications of the tax authorities or

3.

the documents and records stored for the taxpayer

to make it available on a machine-readable data carrier.

The taxpayer bears the costs. In cases covered by sentence 3, the person with the external audit

entrusted public officials in § 3 and § 4 number 1 and 2 of the Tax Advisory Act

designated persons to announce his appearance within a reasonable period of time. Provided

an external audit has not yet started, in the event of a change of

data processing system or in the case of outsourcing of recording and storage

data from the productive system to another data processing system

sufficient if the taxpayer after the end of the fifth calendar year on which

the conversion or outsourcing follows, this data exclusively on a machine

readable and machine-readable data carriers.

Section 257 of the Commercial Code

(1) Every merchant is obliged to keep the following documents in an orderly manner:

1. Ledgers, inventories, opening balances, annual accounts, individual accounts

according to § 325 paragraph 2a, management reports, consolidated financial statements, group management reports as well

the work instructions and other organi-

sation documents,

2. the commercial letters received,

3. Reproductions of commercial letters sent,

4. Receipts for postings in the books to be kept by him according to § 238 paragraph 1 (book

receipts).

credit bureaus, collection agencies

(2) Commercial letters are only documents that relate to a commercial transaction.

(3) With the exception of the opening balance sheets and financial statements, the items listed in paragraph 1

ten documents also as a reproduction on an image carrier or on other data carriers

be kept if this corresponds to the principles of proper bookkeeping

and it is ensured that the playback or the data

1. with the received commercial letters and the accounting vouchers pictorially and with the

correspond in content to other documents if they are made legible,

2. Available for the duration of the retention period and at any time within

can be made legible within a reasonable period of time.

If documents have been produced on data carriers on the basis of Section 239 (4) sentence 1,

the data can also be stored in printed form instead of on the data carrier; from-

Printed documents can also be kept in accordance with sentence 1.

(4) The documents listed in paragraph 1 nos. 1 and 4 are ten years old, the others in

Keep the documents listed in paragraph 1 for six years.

(5) The retention period begins at the end of the calendar year in which the last

Entry in the trading book made, the inventory drawn up, the opening balance sheet

or the annual financial statements, the individual financial statements according to § 325 para. 2a or the

Consolidated financial statements have been drawn up, the commercial letter has been received or sent, or

the accounting document was created.

Rather, in these cases, pursuant to Art. 17 (3) (b) GDPR i. in conjunction with Section 35

Para. 3 BDSG instead of deleting the data, the restriction of

Processing of the relevant data of the data subject.

In the practice of case processing at the IKU, after the end of the

respective collection procedure, the data for any (collection) processing

blocked accordingly and in each case after expiry of the aforementioned

Retention periods deleted by the IKU.

§ 35 BDSG reads:

§ 35 BDSG

(1) Is deletion in the case of non-automated data processing due to the special

type of storage is not possible or only possible with a disproportionate amount of effort

If the interest of the data subject in the deletion is considered to be low, this exists

The right of the data subject to and the obligation of the person responsible to delete personal

additional data according to Article 17 Paragraph 1 of Regulation (EU) 679/2016

to the exceptions mentioned in Article 17 paragraph 3 of Regulation (EU) 679/2016.

In this case, the restriction of processing takes the place of deletion

Article 18 of Regulation (EU) 679/2016. Sentences 1 and 2 do not apply if

the personal data have been unlawfully processed.

(2) In addition to Article 18(1)(b) and (c) of Regulation (EU) 679/2016

Paragraph 1 sentences 1 and 2 apply accordingly in the case of Article 17 paragraph 1 letter a and

d of Regulation (EU) 679/2016, as long as and to the extent that the person responsible has reason for the

Assumes that the interests of the data subject worthy of protection are protected by deletion

would be affected. The person responsible informs the data subject about the

Restriction of processing, unless notification proves impossible

or would require a disproportionate effort.

(3) In addition to Article 17 paragraph 3 letter b of Regulation (EU) 679/2016 applies

Paragraph 1 accordingly in the case of Article 17 paragraph 1 letter a of the Regulation (EU)

679/2016, if a deletion is subject to statutory or contractual retention periods

oppose

Data processing when the claim has been settled

against the creditor

The above principles regarding the storage or

Storage obligation on the part of the IKU as well as the aforementioned deletion period

ten also apply to those cases in which the person concerned

Commitment directly to the IKU even before the IKU was mandated

creditor has settled.

Such cases are usually based on a temporal "overlap"

of the receipt of payment by the creditor and the data transmission

the IKU.

Due to the payment made, the mandate of the IKU was unnecessary

tig: After all, the former debtor had his/her contractual

obligation already fulfilled.

Therefore, under civil law, there is generally no right to payment

Costs of such an assignment by the debtor. These hit a lot

more the creditor. It therefore has no fundamental interest in this

unnecessary assignment. Nonetheless, this does occur in individual cases.

In these cases, the GDPR fundamentally restricts private autonomy

not a. Such an accidental assignment is therefore at least out

not illegal per se for reasons of data protection. The assertion

A request for a commission is only possible if the

IKU has the claim data. This data transfer is therefore

necessary part of the mandate of an IKU and thus in accordance with Art. 6

Paragraph 1 sentence 1 lit. c GDPR permissible. However, it does not follow from this that every

Transmission based on a contractual obligation in accordance with Article 6 (1).

Sentence 1 lit. c GDPR is permissible. Becomes a civil contract only

to legitimize data transmission or are merged into one

such a contract to legitimize data transmission

122

credit bureaus, collection agencies

Regulations included, this contract can not transfer data

legitimize.

In this case, too, the successful acceptance of the collection mandate

a business transaction occurred at the IKU. This business transaction solves for

the IKU the above mentioned documentation and storage

obligations. Consequently, the corresponding documents are on the part of the IKU

or data also in this case constellation - in the for the collection processing

processing locked files – with the limited purpose of processing

be kept or stored for periods of up to ten years.

Nevertheless, in such cases, the creditor has due to his obligation

Measures to minimize data in accordance with Article 5 (1) (c) GDPR and correctness

according to Art. 5 Para. 1 lit. d GDPR carefully before mandating an IKU

to check whether a mandate is required. Was such a test

not done or no adequate prevention procedures

of unnecessary mandates implemented, can still be a violation of

the DS-GVO are available on the part of the creditor.

Data processing in case of mistaken identity

Even in the event of a mistaken identity, the legal situation is as follows

described above. By asserting the claim on the part of

of the IKU - also towards the inappropriate debtor or the

confused person - is also a business transaction on the part of the IKU

originated, which the corresponding documentation and storage

obligations justified. Premature deletion of the data of the confused

Person is therefore not considered in these cases either.

The reason for such a mix-up of persons is often the fact that

that the actual debtor has moved to an unknown address. this leads to

to postal returns regarding the invoices or reminders, what

again on the part of the IKU an address research at a business

prospectus or an address service provider. Here it can be negative

case (e.g. in the case of people with the same name who live in the same city

wohn(t)en etc.) by the credit agency or the address service provider

erroneously to an inaccurate assignment of the requested data set

to the data record stored there or an applicable assignment

to an inaccurate data record - and thus to the mistaken identity

lung—come.

With the subsequent information from the credit agency or the address service

supposedly new address data of the person/their transmitted to the IKU

alleged debtor is now as part of receivables management

ments written to the mistaken person by the IKU. This is

naturally extremely unpleasant for those affected in every respect.

In such a case, it is for those affected - to avoid further in-

collection measures and associated inconveniences – recommended

worthless to immediately contact the IKU and this

to point out the existing confusion of persons. This can

the fastest possible clarification of the facts, a corresponding

Correction of the data record of the IKU or the creditor as well as the setting

ment/termination of the debt collection procedure against the erroneously claimed

taken mistaken person be brought about.

Experience has shown that in such case constellations, an immediate

Examination of the facts on the part of the IKU as well as the cessation of the collection

proceeding against the data subject. Finally, there is part

of the IKU has an original self-interest in being both legally compliant

to behave, as well as to the existing claim against the /

of the actual debtor.

In principle, the IKU - if it becomes aware of a person

confusion - to take appropriate precautions, a mixture

of the data of both persons to avoid. It is therefore recommended

wise to make a corresponding separation of the data records or

in the data set or data sets of the IKU the data of the mixed up

Mark the person as such to avoid future confusion

to avoid.

In the case of such a mix-up of persons exists - in addition to the law

of the actual debtor to provide information - also in favor

DS-GVO towards the IKU.

If the confused person requests information according to Art. 15 DS-GVO,

it is imperative for the IKU to ensure when providing information that

that the data of the actual debtor (e.g. his/her

Personal details, billing data, etc.) to the mistaken person

but only the data on this mistaken person

(e.g. their personal details and, if applicable, the origin of the address data

the mistaken person (credit agency, address service provider), as well as

if applicable, the addressees to whom the IKU sent data of the mistaken person

submitted).

This also applies vice versa, of course, in the case of a request for information from the

actual debtor: On the part of the IKU, only the

credit bureaus, collection agencies

Data that are processed about the debtor are disclosed,

but not data relating to the mistaken person.

Art. 15 GDPR reads:

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

drawn data have been disclosed or will be disclosed, in particular

to recipients in third countries or to international organizations;

if possible, the planned duration for which the personal data will be stored

or, if that is not possible, the criteria used to determine that duration;

e) the existence of a right to rectification or erasure of data concerning them

personal data or restriction of processing by the

responsible 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 are not collected from the data subject,

d)

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.

Based on the information given to her, the confused person

son - in particular by naming the origin of the data - ultimately

enabled, for example, to contact the credit agency

or the address service provider who sent the incorrect address data to the

submitted to IKU, with the indication that a personal

there is a change and a corresponding data correction to be made there

has to prevent future confusion of persons and thus incorrect information

to avoid grants.

In addition, there are also counter-

via the credit agency or the address service provider

other data protection rights, such as the right to information

according to Art. 15 GDPR. This information can also be used to get confused

person, if necessary, determine where the data relating to their person came from,

stored by the credit agency or the address service provider

are, originate.

In any case, such action on the part of the data subject is permitted

recommend. Furthermore, the confused person has the opportunity to

to the data protection supervisory authority responsible for the companies concerned

to contact authorities. Their responsibility usually arises in each case

from which federal state the (main) headquarters of the company is located in

registered in the commercial register. This data can often be found in the imprint

can be found on the company's website.

Furthermore, the credit agencies or address service providers are

th, through the feedback that has been given, if necessary, the existing ones

Correct data records in order to prevent future confusion of persons

avoid. In addition, these should ensure the quality of the

Regularly check the processes of assigning the data records (e.g.

wisely by evaluating and analyzing any error rates within the framework

the assignment and disclosure process) and on the basis of this

Optimize results if necessary.

web, advertising

13. Internet, advertising

web, advertising

13.1

Cookies on the test bench - cross-country tracking test on newspaper websites

Cookies are essential for the Internet in its usual form
however, often also for services that are problematic in terms of data protection law
used. Therefore, together with several German supervisory
authorities in detail the corresponding practice on the websites of large
newspaper publishers.

Noticeable notices and pop-up windows asking for approval
is asked to set cookies, have been with the Internet user for some time
ubiquitous. This puts the topic of cookies more in focus
made public. However, the use of cookies is by no means
new, they have been around since the mid-1990s and thus from the point of view of most people
Internet users always. Cookies are files that the providers
Store accessed websites on the user's device and in which
they store certain, individual values and information and
set use can be read out again. Thanks to this technique
Information, settings or inputs of the user permanently
are kept (e.g. language settings, contents of a shopping cart, etc.).
The use of cookies is often necessary for certain, often considered
technically taken for granted functions of websites at all
to allow. Of such technically necessary cookies goes in all

generally no major threat to the rights and freedoms of the users concerned

break out The partly widespread view that cookies are generally dangerous

or questionable under data protection law, is therefore not correct.

Cookies, along with similar technologies (e.g. fingerprinting

etc.), but also frequently used to inform the users of one (or more

rerer) website(s) to follow or "track". In doing so, an individual

User feature generated and stored, based on which the user or

the device he uses reliably for all future uses

can be recognized. So can the behavior of the individual user

observed over a long period of time and sometimes in great detail

become. The information collected results in a user profile that

precise information about the characteristics or preferences of the respective

user may contain. Depending on the design of the underlying

Tracking process, such profiles are very comprehensive and not on

individual websites limited. This is all the more true when it comes to profiling

access is made to globally active service providers and their services,

which assigns usage behavior from different usage contexts

merge and aggregate into one profile.

Tracking services, for example, play an important role in analysis

and optimization of the respective website (web analysis). The more accurate one

The website operator knows which user groups are determined in which way

Use areas of his service, the sooner he can his offer and the

Align advertising placed there accordingly. Using various tools

for web analysis, which are offered by various external service providers

den, a website operator can get a comprehensive picture of usage

received from his website.

The creation and evaluation of

User profiles via tracking but for advertising. Through the profiles

an individual and thus promising approach to the

user with potentially relevant advertising. Will example

Wise advertisement in the same place on a young mother's website

for toys, while a senior citizen was shown an advertisement for hearing aids,

this promises advertisers a lot more success than if all

Users see the same advertisement for a product that is personal to them

may be irrelevant. Accordingly, an advertising space with personal

nalized advertising by the provider of the website also more profitably marketed

become. The corresponding advertising services are generally not provided by

operated by the operators of the websites themselves, but by a large number

from external service providers who collect user data for their own purposes

use and process.

Unfortunately, there are many legal ambiguities when it comes to cookies and tracking.

ten. Together with the GDPR, a European

sche ePrivacy regulation with special rules for cookies and tracking

come into effect. For political reasons, the legislative process

but still not finished. At the same time, they still throw

always valid, but meanwhile outdated European ones

ePrivacy Directive and its German implementation in the Telemedia Act

Interaction with the regulations of the DS-GVO some legal questions

on. Despite several rulings by the ECJ and the BGH, these could

been only partially clarified in recent years. Against this background, the
Data protection conference a comprehensive guide for providers of
Telemedia services published the views of the regulators
reflect and the providers assistance for the legal classification
of the various processing activities (see 48th activity report
from 2019, 13.2).

128

web, advertising

Some of the website operators or industry associations have their own
Concepts developed to provide information about cookies and the collection of
approvals for data processing as uniformly as possible and according to your own
to make the concept legally secure. For example, the European
schen digital marketing industry association IAB Europe the so-called transparency
and Consent Framework (TCF), which is also used by many German
used by website operators. With this framework, the municipality
communication between the various providers is standardized and that
Obtaining consents across multiple providers unified
and be relieved. Whether this standard actually meets the requirements
ments of European data protection law, was previously able to
not be finally clarified, but will be by many supervisory authorities
doubted.

An industry that markets advertising space particularly intensively and
nance their often free offers often to a special extent
The publishing industry with its web portals is using tracking services
Newspapers and magazines. Newspaper websites often use several tra-
cking services from various service providers in order to generate as much revenue as possible

to achieve the advertising placed there.

Together with several other German data protection supervisory authorities

I am therefore conducting a transnational

comprehensive, coordinated data protection review to give me a picture of the

to provide tracking practice for large newspaper companies and, if necessary,

to prevent improper practices. The authorities involved have

developed questionnaires and supplementary documents with which the

audited companies were asked to submit their respective practices to the

use of tracking services or when setting cookies.

In addition, technical and legal auditing standards have been defined

in order to ensure that the examination is as uniform as possible across the federal states

guarantee.

I've made several major newspaper companies as part of the exam

Hessen written and comprehensive information about their tracking

xis caught up. At the same time, the respective web offers became technical

secured and extensive technical analyzes carried out.

In the extensive examination, together with the supervisory

authorities of the other federal states involved uniform criteria for the

Evaluation and evaluation of the test results. In this way

will contribute to a uniform and comparable evaluation of the results

made possible for everyone involved. After completing the evaluation I will how

certainly also the colleagues from the other federal states, constructively,

if necessary, but also sanctioning the operators of the tested services

and websites and initiate any necessary changes.

With those at the exam, also together with colleagues from other places

federal states, standards developed and knowledge gained

also becomes a basis for the future examination of others

Providers and websites created. In this way, a legally compliant

Practice in tracking and the use of cookies can be ensured.

13.2

No advertising with Corona data!

In the summer of the year under review, when visiting restaurants,

the provisions of the Corona Contact and Operating Restriction Ordinance

tion by the business owners the name, the

collect the address and telephone number of the guests. The data was allowed

solely to enable the tracking of infections (co-

rona contact tracing) used by the authorities responsible for this

become. Any further data collection or use

the data for other purposes such as B. for advertising was inadmissible.

Due to § 4 para. 1 No. 2b of the Ordinance on the Restriction of Social

Contacts and the operation of facilities and offers based on

of the corona pandemic (corona contact and operational restrictions

ordinance) of May 7, 2020 in the version effective on August 15, 2020

changes due to Art. 3 of the Seventeenth Ordinance on the Adaptation

of the ordinances to combat the corona virus of August 11th

2020 were the business owners of restaurants

and accommodation establishments in Hesse are obliged to provide the names and addresses

and collect phone numbers of their guests. The collected guest data

were to be kept or stored for one month, third parties were allowed

not known and were for convenience only

the tracking of infections (corona contact tracking) by the

authorities responsible for this.

§ 4 (Corona Contact and Operational Restriction Ordinance)

(1) Restaurants within the meaning of the Hessian Restaurant Act of March 28, 2012 (GVBl.

p. 50), last amended by the law of December 15, 2016 (GVBl. p. 294), canteens,

Hotels, canteens, ice cream parlors, ice cream parlors and other businesses are allowed to serve food and drinks

(...)

130

web, advertising

(2) offer for consumption on site if it is ensured that

(...)

b) Name, address and telephone number of the guests solely to enable the

Tracking of infections by the business owner

be recorded; these have the data for a period of one month from the beginning of

Visit protected from inspection by third parties for the responsible authorities

available and to transmit to them upon request and immediately after

to delete or destroy securely and in accordance with data protection regulations when the deadline expires; (...)

(...)

To meet this requirement, many restaurants and inns have been

Data collection forms distributed to the guests, all of which are to be

should be kept sorted at the time of the exercise. After the first month

were to destroy every day those data collection forms for which

the retention period of one month had expired. In many larger ones

and well-frequented companies collected a great deal in this way

additional paper documents, for their safe keeping significant

space was required and effort was made. To save space, effort

to reduce, to minimize the risk of inspection by third parties and after

one month to always meet the obligation to destroy on time

can, were already a short time after the corona contact

and Operating Restrictions Ordinance more and more automated systems

in the form of smartphone apps or online applications for survey and

Storage of guest data by the innkeepers and restaurant operators

deployed.

Through the tip of a guest, I was drawn to such an automated

System for data collection alert in which a Hessian restaurant

its guests via a QR code attached to each table, which

to be scanned with the smartphone, to an online data collection form

directed. In this online data collection form, which is after the above

attached text should actually only serve to collect the data

must be made available to the health department in the event of a chain of infection

Must be tracked was by the restaurant owner next to the

data collection fields required for corona tracking

"Name", "Address" and "Telephone number" also the data collection field

"Email" has been attached. There was additional text under the form

"I consent to my data being used for marketing purposes until revoked

by which restaurant and affiliated companies can be used".

An option field was placed in front of this consent text for advertising

was already pre-assigned with a tick.

Immediately upon receipt of notice of this data collection practice

and the intended use of Corona tracking data for advertising

I have pointed out to the restaurant operator that the

data to be collected to combat the corona pandemic

may only be used for the purpose of corona tracking.

Advertising use of the collected data is subject to the regulation

clearly stated strict earmarking of the data. In addition

do not include e-mail addresses under the Corona contact and

Data to be collected under the Drive Restriction Ordinance and may therefore

not be collected on the basis of this provision either.

For an effective advertising consent, it would also be necessary that

it is clear from the consent text which affiliated companies

of the restaurant operator, this is about which sectors these companies

men belong and whether the data subject in advertising by letter post, e-mail, telephone

or SMS agrees. The one attached under the data collection form

Consent text was for a legally effective consent in advertising

far too vague and in relation to the intended advertising medium

undifferentiated.

In addition, for effective consent in accordance with Art. 4 No. 11 DS-GVO

and recital 32 sentence 3 a clear, active, affirmative action by the

Affected would be required:

Article 4 GDPR

For the purposes of this Regulation, the term means:

(...)

(11) "Consent" of the data subject any voluntarily for the specific case, in informed

ter manner and unequivocally given 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.

(...)

Recital 32

Consent should be given through a clear affirmative action that

is stated willingly, for the specific case, in an informed manner and unequivocally,

that the data subject with the processing of personal data concerning them

Data agrees, for example in the form of a written declaration, which can also be sent electronically

can be made, or an oral statement. This could be about clicking on a

box when visiting a website, by selecting technical settings

for information society services or by any other declaration or behavior

132

web, advertising

ten way happen, with the data subject in the respective context unambiguous

your consent to the intended processing of your personal data

signaled. Silence, boxes already ticked or inaction of those concerned

Person should therefore not constitute consent.

(...)

Since the option field attached to the consent text already has a

Hook was preassigned was a clear affirmative action by the guest

to grant advertising consent is no longer possible. default

Consent solutions that no longer require active action by those affected

require, therefore always lead to the ineffectiveness of the consent.

The company that ran the restaurant and also for the online

was responsible for data collection, it was clarified that due to the

Invalidity of the previously given consents all already with this one

procedure collected e-mail addresses of guests are to be deleted.

In addition, I have strongly suggested to the company that anyway

unsuitable consent text, the associated pre-assigned option field and

the email address data collection field from the survey form

to remove. Because even if the pre-assignment of the radio button is removed

and an effective consent text would be attached that

genes of clarity and specificity of consent is sufficient, and additional

Selection fields for the desired advertising medium (letter, e-mail, telephone,

SMS) would be attached, this would be due to the

purpose of the data different claims (e.g. to the possibility of

Acknowledgment by third parties and the deadlines for data deletion).

whole series of both organizational and data protection pro-

entail problems that would require extreme effort and

nevertheless could hardly be solved in a legally clean manner.

The company then added the data collection field "e-mail" as well

the insufficient consent text and the option field completely and

removed from the online data collection form without replacement. The up to

E-mail addresses collected at this time were not yet available for dispatch

used by promotional e-mails and have been completely deleted.

14. Technology, organization

technology, organization

14.1

Transmission of personal data by email

For communication both with and between public and

private bodies, the use of e-mail is widespread and has

gained even more importance during the SARS-CoV2 pandemic. From

Those responsible are the specifications of Art. 5 Para. 1 lit. f, 25 and 32 Para. 1

GDPR to be met if communication content or metadata

have personal reference. For the core area of transmission, the

Conference of the independent federal data protection supervisory authorities

and the federal states (DSK) at their 99th meeting an orientation guide (OH)

adopted. The implementation of this OH requires that everyone at the com-

actors involved in communication make their contribution.

On May 12, 2020, the DSK passed the OH developed in the AK Technik

“Measures to protect personal data in transit

by e-mail", see also Appendix I 3.1. This focuses on requirements for

Setting the requirements of Article 5 Paragraph 1 Letter f and Articles 25 and 32 Paragraph 1

GDPR. The successful implementation of these requirements can only be

interaction of all actors succeed.

For a better understanding, the e-mail communication process is first

cation shown schematically. Only those aspects are mentioned here

taken into account that are relevant for the further explanations in this article

are. The representation forms the basis for a closer look at the

Actors involved in e-mail communication and their mutual dependencies

to enter into Building on this, the main ones are discussed separately

requirements for the individual actors.

Schematic flow of email communication

Figure 1 provides a schematic overview of the for this

Post relevant aspects of email communication.

Figure 1: Schematic representation of e-mail communication

It provides an example of the process of sending an e-mail from a

human sender to a human recipient. Here

it is assumed that sender and recipient are different

Those responsible within the meaning of the GDPR belong, for example, to two independent ones

Company. In addition, the e-mail to be transmitted must be between two

separate e-mail servers over one or more networks

become.

This scenario serves as the basis for further explanations. a we-

essential feature is that the selection of the recipient and the

The content is deliberately created by one person. Further

possible scenarios are not considered in detail below, such as the

Sending automatically generated emails without human intervention

or the sending of e-mail, within the sphere of influence of an individual

responsible.

At the e-mail communication are the following relevant components

involved.

- Sender's email client (MUA-1) - An email client, in English

Mail User Agent (MUA), is used by a sender to create the e-mail

and to send them. This can be, for example, a on the

E-mail program installed on the sender's computer or a

Trade web-based user interface.

technology, organization

– Sending email server (MTA-1) – This server or IT service, in

English Mail Transfer Agent (MTA), takes delivery from MUA-1

receives certain e-mails and ensures their transmission to the

next station.

- Name service (ND) - A name service is used to determine relevant

Information, such as about receiving e-mail servers for a specific

E-mail address.

– Receiving email server (MTA-2) – This server or IT service

receives e-mails and holds them for retrieval by e-mail clients

of recipients ready.

- Recipient's email client (MUA-2) - This email client is used by the

Recipients used to retrieve and display emails. Analogous

Different implementations are also possible here compared to MUA-1.

Due to the numbering contained in Figure 1, the schematic

The process of e-mail communication can be traced.

1. The sender composes an e-mail using functions

features of the MUA-1 and provides the e-mail with the e-mail address of the

receiver.

2. Using the appropriate functionalities of MUA-1, the finished e-mail

transmitted over a network to MTA-1. With this network it can

be, for example, a company network or the Internet. an over

Transmission across multiple network boundaries is also possible.

3. After receiving the e-mail, it is stored by MTA-1.

This storage and the associated data protection

cial requirements are not considered in more detail here, since they are not

attributable to the actual transmission. However, they are from

also to be fulfilled by those responsible.

4. MTA-1 uses a network to determine the (network

factory address of the MTA-2 if this is not already known. At

the network is i. i.e. R around the internet.

5. MTA-1 transmits the email based on the previous step

determined address to MTA-2. Transmission is also via

a network.

6. After receiving the e-mail, it is stored by MTA-2

and made available for the recipient to retrieve via their MUA. anal

log to step 3, this storage and the associated

Requirements not considered further in this article.

7. Using the appropriate functionalities of MUA-2, the e-mail is sent via

retrieved a network from MTA-2. It can be analogous to step 2

in this network, for example, a company network, the Internet or

even multiple networks.

8. The recipient reads the e-mail using the information provided by MUA-2

provided functionalities.

The horizontal line between content and transport is for presentation

the conceptual separation between these two levels of

email communication.

At the content level, step 1 is the composition of the e-mail content

on the sender side. Step 8 represents the reading and processing in the same way

of the e-mail content on the recipient side. Step 9 clarifies

light that the actual content-related communication between the sender and

recipient done. Any end-to-end

Encryption located.

Steps 2, 4, 5 and 7 each form a communication on the trans-

port level. Such communication occurs via one or more

networks. It should be noted that i. i.e. R. to different

networks acts. For example, sending an email between MUA-1

and MTA-1 take place via a company network if the person responsible has one

operates its own e-mail server within its network. In contrast

can transfer the mail from MTA-1 to MTA-2 over the internet

take place. A direct transmission between MTA-1 and MTA-2 is not

the rule. Rather, several intermediate stations are often involved.

However, these are of secondary importance for this contribution. In the

Transmission between each intermediate station should be one

Transport encryption is used.

Name services will not be discussed in more detail below. she played

However, within the framework of the fulfillment of specific requirements of the OH

important role, for example in connection with a qualified transport

encryption in chapter 5.2.

The basis of e-mail communication is thus openness

and decentralized infrastructure. This is how those responsible can

e.g. one or more components involved in the communication themselves

operate. There are various options available for concrete implementation

Disposal. For example, a large number of alternative implementations are

available from different manufacturers as a basis for the operation of MTAs.

Actors in email communication

The requirements for the protection of personal data under

of e-mail communication aimed at the different at the

technology, organization

actors involved in communication. In this post, the following

actors differentiated.

I. Email Providers – These are providers of email

infrastructures. They offer this to their customers, for example in the form of

E-mail mailboxes and associated web-based management interfaces

place. Web-based MUAs may also form part of the offerings of

email providers. The offers from e-mail providers are common

more or less standardized.

II. Organization as a customer of an email provider - This is about

are institutional customers of e-mail providers.

III. Organization with its own email infrastructure – Organizations that

operate an e-mail infrastructure themselves fall into this group of

actors.

IV. End Users - End users are individuals who use email as a means of

resources and who belong to an organization as the responsible party.

The end users are those already in the process

sender and recipient presented in the e-mail communication. In

This article does not go into detail about private e-mail use.

e.g. by customers of a company.

Organization II and III are responsible in the context of this article

according to Art. 24 DS-GVO. E-mail providers act as order

processor according to Art. 28 DS-GVO.

Figure 2 shows the actors and their relationships with each other

shown schematically in the event that a responsible organization

uses the e-mail infrastructure of an e-mail provider.

Figure 2: Inclusion of e-mail providers

The gray highlighting serves to demarcate the area of influence of the

respective actor. These areas of influence are already shown in the figure

1 shown components e-mail client (MUA) and e-mail server (MTA)

assigned.

The assignment serves to create references between the influencing factors

range of the individual actors and the components of the e-mail communication

cation. It depends on the control over the respective components.

For example, in Figure 2, the MTA used by an organization II

operated by an email provider. Accordingly, the MTA dem

Assigned to the email provider's sphere of influence. remain unaffected by this

any configuration options, the organization II from the e-mail provider

in relation to MTAs.

Analogous to this, Figure 3 forms actors, components and influencing

che in the case of complete self-operation of the infrastructure by a

responsible organization.

Figure 3: In-house operation

In the following, the spheres of influence of the individual actors are explained in more detail

received.

I. Email Provider

By assigning an MTA to the sphere of influence of an email provider

it is emphasized that an email provider has at least the essentials

aspects of the MTAs provided to its customers. Which includes

etc. the design of the underlying IT infrastructure, the selection

the software used and making the appropriate configuration

tion settings. The assignment to the sphere of influence of the email provider

This does not mean that an organization II has no influence on the MTA

can take. For example, an e-mail provider of an organization II

Provide web-based management interface through which they

Can influence parts of the behavior of the MTAs used.

140

technology, organization

When sending e-mails via an MTA, there are dependencies on

visible in the design of the corresponding MTA on the receiving side.

These arise z. B. from those supported by the receiving MTA

Possibilities for transport encryption. Conversely, this also applies to

receiving emails.

II. Organization as customers of an e-mail provider

Type and scope of the opportunities provided for Organization (II).

Configuration and influencing the behavior of an email pro-

Each MTA operated can vary greatly. In terms of data protection

Context here are primarily options for defining, implementing and

Application of technical and organizational measures within the meaning of Art.

32 GDPR of particular importance. Here, with the selection of a

E-mail provider or an offer from the same already provides the framework for

the level of protection that can be guaranteed by Organization II as controller

in relation to the MTA(s).

The MUA used by an end user is shown in Figure 2 with the influence

assigned to the associated organization. This will emphasize

emphasized that the organization determines the design of the MUA. In

usually it is determined by an organization which software is classified as MUA

is used. This software is designed by the organization accordingly

configured provided to the end users of the organization. This

the organization agrees on the essential framework for e-mail use

by their end users.

In shaping this framework, Organization II is both forward

framework specified above by the e-mail provider as well as from supplementary

dependent measures that are not exclusively implemented in the MUA

can become. This includes e.g. B. the creation of the conditions for

Use of end-to-end encryption. In this context

II is also an organization of supporting compatible procedures

by those responsible with whom end-to-end

to be communicated.

III. Organization with its own email infrastructure

As shown in Figure 3, both MTA and MUA lie in

flow area of an organization with its own email infrastructure (III). here

out it follows that such an organization includes both components of the

E-mail communication largely under control. Accordingly

Does the organization, compared to the explanations in the two previous

addressed sections, a greater degree of freedom in terms of

Design of the technical and organizational measures in accordance with

Art. 32 GDPR. This is especially true with regard to dependency on

an email provider. At the same time, it often involves a higher effort

compared to using an e-mail provider.

The comments on email providers regarding the dependencies on

the MTAs of the communication partners when sending and receiving

E-mails apply in the same way.

IV. End Users

End users use an organization (I or II) provided

ten MUA for writing, sending, retrieving and reading

from emails. As shown in Figures 2 and 3, the

dete MUA not in the sphere of influence of the end user. This does not mean

that end users have no influence on data protection aspects of the

have e-mail transmission. However, the possibilities for influence are

by the framework conditions defined by the organization

gig. Are, for example, on the part of the organization the requirements for a

End-to-end encryption has been created so an end user can

basically use them for e-mail communication. The creation of the

Prerequisites are not limited to the MUA. Nevertheless must

MUA also supports end-to-end encryption.

The ability to use the information provided by the associated organization

The framework conditions provided often also depend on the recipient side

away. Only if the necessary prerequisites have been created on this

Can the measures provided actually be used?

men. For example, the use of end-to-end encryption requires

that both sides support them in a compatible way.

Requirements for the actors

Based on the explanations in the previous sections,

Following on the resulting requirements for each stakeholder

received. Here, organizations with and without are no longer distinguished

inclusion of an e-mail provider.

I. Email Provider

When designing their offers, e-mail providers must

take into account the demands of their customers. Only if they meet their customers' requirements

provide corresponding e-mail infrastructures, these

technology, organization

in the first place in the position required according to Art. 32 DS-GVO

To take action. Accordingly, e-mail providers are faced with a

central role in creating the conditions for implementation

data protection requirements.

In order to enable, for example, those responsible, according to Chapter 4.2.1 of the OH

to meet a normal risk in terms of confidentiality,

an e-mail provider must have mandatory transport encryption

support. Better than strict implementation would be the provision of

Possibilities of influence for those responsible, such as selective deactivation

for individual domains or email addresses. Ideally, end users could

when sending an e-mail via their MUA, whether an obligatory

toric transport encryption should be used or not.

A responsible person who uses an e-mail provider is with the

Design of its e-mail infrastructure heavily on that of the e-mail provider

predetermined framework. Through these framework conditions

the e-mail provider essentially determines which measures are to be taken by the

can be literally implemented. Accordingly, an e-mail provider influences

also indirectly the freedom of action of end users. The framework

Conditions can vary from email provider to email provider and from offer

vary on offer.

II. Organization

Organizations are strongly advised, if they use an e-mail pro-

viders already planned and necessary measures at the time of selection

to consider. This includes in particular the implementation of a

Risk assessment for the application scenarios of e-mail communication. Out of

the resulting results can be appropriate requirements

to derive offers from e-mail providers, which then serve as criteria

the selection of an e-mail provider or its offer in combination

with the other selection criteria.

Those responsible must check the assurances of the e-mail provider and

the options granted in accordance with Art. 28 (3) (h) GDPR

to use. The implementation of a mandatory transport encryption is

e.g. essential to ensure that actually transport

encrypted communication. In contrast, analyzes in my

IT laboratory to point out that in case of doubt a transport lock

ment does not have to be applied, even if this is supposed to be the case

would be supported by the MTAs involved. Reasons for this can

e.g. incompatibilities or error situations.

When the e-mail infrastructure is operated by those responsible, im
Essentially the same aspects as when using an e-mail pro-
to be taken into account. In addition, technical and organizational
measures for the provision, operation and maintenance of the infrastructure
seize. By operating it yourself, compared to using a
email provider i. i.e. R. greater scope for decision-making and the
operation-specific framework conditions play an important role,
such as control over the infrastructure used.

In addition, further technical measures must be taken
for example in relation to the selection and configuration of the end users
provided MUA. Here, too, the person responsible is essentially
areas from the framework set by any e-mail provider
conditions dependent. This applies e.g. B. for options for connection
from MUAs to MTAs.

In addition, communication partners should implement their technical
Technical and organizational measures are supported. This should be
be done by creating the necessary conditions, for example
by supporting appropriate standards for a qualified
Transport encryption (chapter 5.2 of the OH) or the support of a
End-to-end encryption (chapter 5.3 of the OH).

It is not sufficient if those responsible have technical framework
conditions for the use of e-mail communications in compliance with data protection law
create cation. In addition, according to Art. 32 DS-GVO, they must also
organizational measures are taken. These include in particular

the specification of specifications when using the provided platform

by end users. End users must also be appropriately sensitized and

to be trained.

It should be noted here in particular that the end users can implement

specifications have to be made. So it should end users i. i.e. R. not

be possible to ensure transport encryption if technically

no mandatory transport encryption is supported.

The measures taken must be in accordance with Art. 32 Para. 1 lit. d GDPR

with regard to their effectiveness in ensuring the safety of the processing

be regularly reviewed, assessed and evaluated.

Finally, potential breaches of protection must be

identified and related data according to Art. 33 DS-GVO

be traded. Thus, analyzes of statistical data on outgoing

E-mail traffic in my IT laboratory Indications of potential violations

tion scenarios. Examples of this were

technology, organization

– the sending of non-transport-encrypted e-mails to communication

partners for whom at least a normal risk in terms of trust

probability of personal content is obvious,

– the non-transport-encrypted sending of e-mails to communication

tion partner for which a transport encryption would be expected and

– the sending of e-mails in which the recipient is addressed

obvious typographical errors have been made.

In all of these cases, further analyzes are required.

III. End User

The scope of action of end users is limited by that of the person responsible
provided email infrastructure. This applies both in technical
cal terms as well as in relation to the specifications made for them
Use of the provided infrastructure. In addition, there are the specific
Circumstances of the communication partners, such as the support of a
End-to-End Encryption.
When using e-mail as a means of communication, end users must
tion make appropriate use of the room for maneuver given to them. So
do they have to i.e. R. when you intend to send an e-mail first of all
existing risk for the rights and freedoms of data subjects determine
and then proceed accordingly, for example by using a
End-to-end encryption in line with Chapter 4.2.2 of the OH im
Case of high risk of breach of confidentiality
of content data.
Conclusion
The OH passed by the DSK provides a good basis for design
technical and organizational measures to meet the requirements of
DS-GVO to the protection of personal data during transmission
ensure email. The open and decentralized architecture as a basis
of e-mail communication, the optional use of supplementary standards
as well as the large number of communication partners and dependencies between
these lead to not inconsiderable challenges in terms of
implementation of these requirements.
Controllers must take their end users by taking technical
and organizational measures to enable the provided
te e-mail infrastructure in compliance with data protection law. At

Involving an e-mail provider is the early consideration

data protection requirements already when choosing a provider

145

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

special meaning. Significant subsequent adjustments on by

the framework set by the selected e-mail provider should only be difficult

to be possible. The same applies to the realization of a self-operated

email infrastructure. It is true that a responsible person has control over the

IT infrastructure used, but subsequent changes are also likely here

be associated with significantly higher costs.

Organizations and email providers are called upon to meet the requirements

to establish the protection of personal data during transmission

ensure by email. This includes in particular the support

tion of supplementary standards, as referenced in the OH of the DSK. The

Support for such standards is not an end in itself.

Rather, they form not least a necessary prerequisite for

communication partners for their part to be able to

ments to the protection of personal data when transmitting

ensure email.

14.2

Additional reference measures to the standard data protection model

Provide the Standard Data Protection Model (SDM) and reference measures

responsible persons and processors orientation, which technical

organizational measures to be taken to ensure processing

to design and provide personal data in compliance with data protection regulations,

to operate and maintain. Corresponding contributions regarding the

progressive development of the SDM can also be found in Section 47 (Section 4.10.1)

and in the 48th activity report (Section I 14.4).

Development of the Standard Data Protection Model (SDM)

In November 2019 a new version of the SDM manual is available from the

Conference of the independent federal data protection supervisory authorities

and the countries passed without a dissenting vote. In doing so, he became

Life cycle of a data protection management integrated into the manual

and the corresponding reference measure resolved in the 47th Activity

report was shown separately. Essential articles in the GDPR for

technical assessment of the processing of personal data

explained. Statements on the basics of data protection management, such as

planning or specifying, controlling or checking, that

Assessing and improving technical and organizational measures

ment for processing activities are accordingly in the 48th activity report

shown.

technology, organization

The SDM includes the mentioned manual and will be gradually

reference measures added. Each reference measure includes a

provision of a technical-organizational measure by means of which a

data protection compliant processing is to be guaranteed.

In 2020, more reference measures were published, which frequently

also referred to as building blocks. The new building blocks relate

to the "retention", the "correction", the "restriction of a processing

processing" and "separating" as a specification of protective measures

for data protection-compliant implementation of processing activities. The

The designations now chosen for these measures are intended to clarify

that in the concrete implementation of data protection requirements

various activities by those responsible or the order processors

tern are required. Technical and organizational measures must be taken to ensure that

Measures regularly in the operation of the systems and services for a period of time

be subject to regular revision. This is in the already referenced

created data protection management. In addition, the reference measures

"Document", "Delete and Destroy" and "Log" correspond to

accordingly adjusted.

These publications, other modules and any updates

can be found on the SDM website at https://www.datenschutz-mv.de/daten-

schutz/datenschutzmodell/ (last accessed: 06.11.2020), the

from the nationwide technical working group of the conference of independent

data protection supervisory authorities of the federal and state governments.

Conclusion and Perspective

The SDM manual basically offers through the description of protective

Measures orientation, what in particular from the point of view of the technical

Data protection for the implementation of processing activities is to be done.

Protective measures are technical and organizational to be taken

Measures that ensure data protection-compliant implementation of the respective processing

work activities. Using the reference measures or

of the modules, information is given as to which measures are technically

organizationally specific for systems and services and their operation in the long term

are to be provided and maintained. In this way, each processing

processing processes are implemented in accordance with data protection regulations, the components

of specific processing activities. From a technical point of view,

such components or processing operations are therefore subject to data protection law

be evaluated with regard to their suitability and possible appropriateness.

147

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

The SDM is on the right track, mutually dependent

ties between data protection requirements and to implement

to explain protective measures. Conversely, seized

technical-organizational measures through the reference measures or

Check building blocks for their effectiveness, which also makes a contribution

for the application of Article 32 (1) (d) GDPR.

Perspective is in the context of data protection certifications

something similar to be considered, see specifically 47th activity report, in

the requirements for accreditations of certification bodies and

Data protection certifications in accordance with Art. 42 and Art. 43 GDPR in

Basic features are shown. In accordance with Art. 43 (1) lit. b GDPR

The applicable technical standard EN ISO/IEC 17065 requires the follow-up standard

DIN ISO/IEC 17067 the specification of test criteria, test system and

-methods. Data protection requirements are fundamentally test

criteria. A test system is also required, which is defined by the generic

Protective measures of the SDM for technical data protection covered

can be. Furthermore, the existing blocks can also be used

Feed requirements to required test methods.

148

fine proceedings, data protection violations according to Art. 33 DS-GVO

15. Fine proceedings, data protection violations according to Art. 33

GDPR

fine proceedings, data protection violations according to Art. 33 DS-GVO

15.1

Reports according to Art.33 GDPR in times of the corona pandemic

Misdelivery, hacker attacks and loss and theft of data

likes and documents remain the most common causes for the reports

of personal data breaches in Hesse. The

However, the corona pandemic is also leaving behind data breaches and the

Reporting behavior of the responsible bodies visible traces.

With a total of 1,433 reports, the number shown to me remains the same

Data breaches in the year under review on the previous year (1,453

reports) reached a high level, see also Part I Clause 17.1 and 17.2. In the

The majority of the reported data breaches were again about incorrect shipments

by post, email or fax, hacker attacks including phishing and

Malware incidents, loss and theft of data carriers and

Documents. For this reason I summarize the most important ones to consider

Aspects of these typical case constellations briefly summarized again.

Mistransmission of data

The most common cause of data breaches reported to me

according to Art. 33 DS-GVO was the wrong sending of data. Most of these

Incidents involved health, employee or customer data and

are often based on individual human or technical errors. In

In these cases, the responsible authorities have assured me that

Speaking measures, such as employee training and review

and adjustment of internal processes that have been taken to ensure the re

prevent such incidents from occurring.

Hacker attacks, phishing, malware

Another important part of the reports from the year under review dealt with

dealing with criminal access from outside in the form of hacking, phishing and

malware attacks. In this context, it is important for me to point out again

to point out that in order to ward off such unlawful attacks

appropriate technical and organizational measures in advance

measures to be taken. These are particularly under consideration

the current state of the art, the implementation costs, the type, the

the scope, circumstances, purposes and risk of the processing

take in order to achieve an appropriate level of protection (cf. Art. 32 Para. 1

GDPR). In addition, I consider prompt and effective action

to eliminate or minimize damage, e.g. B. by analysis of infected

systems, resetting compromised passwords, performing

of updates, but also contacting relevant authorities and the

Affected, for essential.

In my 48th activity report 2019 I already reported under number 4.3

details on how to deal with phishing incidents. The ones explained there

Principles relating to the technical and organizational precautions

ments and measures are also applicable to other types of external attacks

to use.

Loss or theft of data carriers and documents

In the year under review, in many cases facts were brought to my attention,

where documents, packages or USB sticks are lost in the mail

went. In addition, burglaries with theft of property

advice and documents to make a corresponding report

my authority. Also to avoid such case constellations, a

Security and data protection concept with comprehensive technical and

organizational measures are implemented. For hardware devices

it is above all a secure encryption of the hard disk after the

current standards, which should always be checked. Wear in other cases

Measures to secure buildings and premises (warning system,

safe-keeping, lockable rooms and cupboards, safes) as well as

Sensitization of the employees to a data protection compliant solution.

Effects of the Corona Pandemic

In addition to the already known problems, as in all

other areas, including reports under Art. 33 GDPR

current corona situation noticeable. Especially at the beginning of the pandemic

many responsible bodies could not fulfill their reporting obligation within the

The period of 72 hours stipulated by the legislator (cf. Art. 33 Para. 1

DS-GVO) after becoming aware of the incident. Some messages

were submitted late. Those responsible gave reasons for this

Among other things, the fact that many employees work from home or

were on short-time work and this led to delays in the processes. The

Delays resulted from the fact that initially new ways of working

integrated and many processes had to be reorganized. Added

e.g. B. technical hurdles, limited accessibility and the sometimes high

fine proceedings, data protection violations according to Art. 33 DS-GVO

Corona-related workload of the responsible employees from the

affected areas.

Since the statements made by the responsible authorities in this regard are good

were justified and comprehensible and the 72-hour period was not unreasonable

was relatively exceeded, I finally saw with the previous ones

examined cases from sanctioning.

The current events surrounding the corona pandemic were reflected

not only with the reporting deadlines, but also with the reported ones

facts themselves. I received several messages from

Responsible persons from the public and non-public area

which the data on a Covid-19 disease z. B. by employers,

School or doctor's office inadmissibly unintentionally either openly

placed or sent to the wrong recipient. Over and beyond

I have individual reports about mix-ups in test results

as part of a corona test. Two of the reported incidents took place in

As part of the establishment of corona vaccination centers and the associated

employee acquisition. Individual data breaches occurred within the framework

the use of video conferences or the forwarding of official

Data to private end devices (e.g. by high-risk patients, to be sent from home

being able to work from). In these cases, the responsible

Take the necessary steps to ensure that any

to repair the damage done. The persons concerned were, in accordance with Art. 34

DS-GVO informed about the data protection violations.

Finally, it should be noted that due to the corona pandemic in comparison

no particularly serious ones compared to the previous reporting period

Personal data breaches have been reported

and no increase in the number of data breaches reported

is listed. However, it should be noted that in the current situation

significantly more intensive and often under time pressure sensitive health data

to the special categories of personal data i. p. of Art. 9

DS-GVO are processed. Since this data is particularly

are worthwhile is an increased degree of care in handling the data

as well as special preventive measures in the current time more than

ever required.

151

15.2

Reporting data breaches to the police – application of the

Section 60 HDSIG in practice

Since the HDSIG came into force (May 25, 2018), there has also been a reporting obligation

for violations of the protection of personal data in the field of

Directive (EU) 2016/680.

Examples of reportable facts:

– A police officer asks numerous questions without official reference

Cases of several family members in the police information system

and in the registration register.

– A police officer asks his ex-wife in the Mel-

deregister to find out whether these

is remarried.

– An employee of the police wants to organize a class reunion

and queries several people in the population register in order to

to obtain writings.

– A mother confronts her daughter's boyfriend with the fact that he is a "drug

gendealer" and she therefore told her daughter that she would continue to deal with him

have forbidden. The father works for the police and was in the police department

Information system researched after his daughter's boyfriend and

communicated the result to his wife.

– An employee of the police wants to rent an apartment and

checks the interested parties in the police information system, since they

only wants to rent the apartment to a person in good standing.

– A police officer is asked by a friend to give her a

Address of the owner of a vehicle after an accident allegedly caused by her

to get a gentle minor accident. But in fact it is

the car of the new girlfriend of her friend's ex-husband, that

is scratched and badly damaged a few nights later.

The obligation to report according to Section 60 HDSIG applies to public bodies in the

of Hesse within the scope of the third part of the HDSIG or § 40

HDSIG implementing Directive (EU) 2016/680. addressees of the standard

in particular the Hessian police, the Hessian judiciary, the Hessian

State Office for the Protection of the Constitution, but also fine offices and municipalities,

insofar as they are active in the prosecution of administrative offences.

152

fine proceedings, data protection violations according to Art. 33 DS-GVO

§ 60 HDSIG

(1) The person responsible has a violation of the protection of personal data

immediately and if possible within 72 hours after it has become known to him,

to report to the Hessian data protection officer, unless the

Violation is not expected to pose a risk to the rights and freedoms of individuals

people. If the report is sent to the Hessian data protection officer or the

Hessian data protection officer not within 72 hours, that's a reason

to add for the delay. Section 59 (1) sentence 2 applies accordingly.

(2) If the processor is subject to a personal data breach

known, he reports this to the person responsible immediately.

(3) The report according to paragraph 1 must contain at least the following information:

1. a description of the nature of the personal data breach,

which, as far as possible, information on the categories and the approximate number of affected

fenen persons, to the affected categories of personal data and to the

has to contain an approximate number of the personal data records concerned,

2. the name and contact details of the data protection officer or a

other contact point for further information,

3. a description of the probable consequences of the violation of the protection of personal

personal data and

4. A description of those taken or proposed by the controller

Personal data breach handling measures

and, where appropriate, the measures to mitigate their potential adverse effects

Effects.

(4) If and to the extent that the information pursuant to paragraph 3 is not provided at the same time

can be, the person responsible has this information without unreasonable further

Gradually provide delay.

(5) The person responsible must document violations of the protection of personal data

mention. The documentation has all the facts related to the incidents,

their impact and the remedial actions taken.

(6) Insofar as a violation of the protection of personal data

ne data are concerned, by or to a person responsible in another

member states of the European Union are those specified in paragraph 3

information to the person responsible there immediately.

(7) Section 37 (4) applies accordingly.

(8) Further obligations of the person responsible for notifications of violations of the

protection of personal data remain unaffected.

A processing of personal data takes place in particular,

qualitatively and quantitatively, at the Hessian police. their activity

allowed in the area of criminal prosecution and preventive processing

processing of personal data on a large scale. Next to the

The Hessian police operates data from the case and transaction processing

a state-wide police information system (POLAS-Hessen), in which

data from criminal proceedings are also stored for preventive purposes

may. Furthermore, insofar as the individual activity requires it,

Access options to other file systems and also the population register.

The work of the police requires an authorization structure that

large number of employees fast and convenient access to

this data allows.

Not just with the abusive ones that have become public knowledge

and thus illegal queries in these systems, it became apparent that

the actual possibilities in individual cases of officials about the

be used beyond legal admissibility.

Since it is i. i.e. R. is data that is particularly worthy of protection

an unlawful query always be checked whether a reportable

Violation according to § 60 HDSIG in the area of responsibility of the respective po-

license presidency.

According to Section 60 (1) HDSIG, violations of the

protection of personal data if the violation of

not likely to pose a risk to the rights and freedoms of natural

people.

The person responsible is thus first required to make a forecast that

regularly requires more background information than the mere fact

that the employee A can trace the person B in a file system

asked. As far as no within the legally required period

Information can be obtained that leads to a risk exclusion,

a report will have to be made to my authority on a regular basis.

Queries are made in police or police-accessible file systems

on a large scale, which are based on a wide variety of trigger constellations

lay. An example would be the classic traffic control,

but also checks in connection with manhunts

and investigations.

In a first step i. i.e. R. determined via plausibility checks

be whether the query is related to a specific police

referred or not. If there is no documented referral

bar/comprehensible, there are still numerous case constellations,

in which the / the staff member / n nevertheless in the context of his

official activity and thus lawfully. One

However, such a review is often only possible with the involvement of/

of the employee concerned. As far as the assessments show,

that a lawful data request cannot be assumed must be

In individual cases, the prognosis already mentioned above can be made.

154

fine proceedings, data protection violations according to Art. 33 DS-GVO

A risk to the rights and freedoms of natural persons is fundamentally

be likely to be affirmed if collected data was passed on to third parties,

regardless of whether it is data on a police referral or

also reporting data. This is by no means always and often the case

also difficult to prove.

The provision of § 60 Para. 1 HDSIG obliges the responsible

continue to follow up a detected violation within 72 hours

to report to my authority when it becomes known. For this stand on mine

Website forms available.

In numerous cases, the data protection officers of the hessi-

schen police headquarters with the question of when the time of disclosure

to be accepted in order to make a report in accordance with § 60 HDSIG in a timely manner.

Due to the heterogeneity of the underlying facts, this

time cannot be generally determined. Rather, this

regarding representatives of the responsible body, promptly the

Degree of probability to gain in order to make an appropriate decision

with regard to triggering a message. this will

always be the case if the person responsible has a justified

degree of certainty that the incident resulted in a risk to persons

gener data. The responsible body is given a short

Period of time for investigation to determine whether a

violation exists or not. A high probability of occurrence for a

Violation of the rights and freedoms of natural persons and the possible

The seriousness of any consequences is regularly reported at an early stage

make necessary.

If reports are not made or not made in a timely manner, this can

entail official measures according to § 14 para. 2, 3 HDSIG. In the

In 2020 I did not report or did not register in time

complained about in several cases.

The information that a report according to § 60 HDSIG must contain is

listed in Section 60 (3) HDSIG. Not listed and therefore not part of a

such notification is generally personal data, except

if applicable, the name and contact addresses of the data protection officer

ten or another point of contact for further information. Therefore

the legal regulation does not require the reporting of the data of the "perpetrator"

and "victim", ie not the personal data of the unlawful

officials acting and the data subject. The reporting procedure

according to § 60 HDSIG has only two bodies involved, the data protection law

responsible body and my authority.

This procedure is therefore an individual and personal one

Sanction proceedings of my authority in its function as prosecuting authority

to demarcate. However, such a procedure can be initiated indirectly through a notification

be released to me according to § 60 HDSIG. This is always the case

if the reported facts indicate that a staff member

the responsible body about his/her internal regulations

Powers in the form of a so-called employee excess (see 48. Activity

report, p. 129 ff.) and her/his actions are no longer the

responsible body can be attributed. This officer can

then in its data protection assessment the regulations of the DS-

subject to GMOs and are therefore also subject to a fine.

156

fine proceedings, court proceedings

16. Fine Proceedings, Court Proceedings

fine proceedings, court proceedings

16.1

Fine proceedings in 2020

Repeated violations of the regulations on the rights of data subjects

lead to high fines. But also excess staff in the public sector

and non-public area continues to represent an essential data protection

legal problem in Hesse.

A large number of the regulations to be carried out by me in the reporting period

adversarial proceedings, there were inadmissible data processing by employees

ter public and non-public bodies for private purposes - the so-called

Excess employees - based (see also Part I No. 17.2). In particular, it came in

often happened in the past that employees of public bodies

fetch data from official systems and obtain them for official purposes

use information for private purposes. So I have in the reporting year

22 administrative offense proceedings against employees of the Hessian police

and two proceedings against employees of job centers

initiated in Hesse. Most of these operations are still in progress

investigation or hearing stage.

The number of procedures against employees of the Hessian police was
taken as an opportunity, in cooperation with the Hessian Ministry
of the interior and for sport as well as the individual police headquarters the processes
improve in the investigative process. I therefore expect a speedy one
completion of these cases.
Another essential part of the procedures I initiated dealt with
dealing with the violations of data subject rights according to Chapter III of the DS-
GMO. With regard to this problem, a total of 13
new proceedings pending.
Also issues related to the current corona pandemic
were the subject of the administrative offense proceedings to be punished by me.
These cases often involved improper use of data,
which were collected using so-called "corona lists". In individual cases
driving, where the seriousness of the offense as well as the overall circumstances
of the case allowed this, I decided accordingly for reasons of opportunity
§ 47 OWiG for sanctioning by means of a warning according to Art. 58
Paragraph 2 lit. b GDPR instead of imposing a fine. Not this
most recently due to the extraordinary situation that has occurred and the
tense financial situation of the responsible departments concerned.

Fine for misappropriation of data within the scope of a
Corona tests
After filing a criminal complaint by the person concerned and submission
of the proceedings by the public prosecutor's office, I was dealt with a case

which was about excess staff in the non-public area. The incident
occurred in a company that was in a test center COVID-19
tests performed. The affected employee contacted shortly after the test
a young lady via whatsapp to get to know her. The responsible
identified himself as an employee of the company and raved about
their "charisma", which is also the reason for the procedural
contact was. As part of the investigations carried out,
the identity of the employee can be established beyond doubt.
In the present case, the employee in question used the
conducting a corona test, the data provided by the complainant
for private purposes and thus violated the principle of earmarking
Article 5(1)(b) GDPR. After that, personal data for
specified, explicit and legitimate purposes and must not
processed in a way that is incompatible with these purposes
become. The contact details of the patients as part of the corona test
rens are to be collected and stored solely for the purpose of
to inform these persons of the test result and, if necessary
in a positive case, contact by the competent authorities
allow health authorities. The use of this data to others
purposes is not permitted. The procedural contact
via WhatsApp was present to fulfill the of the accused
tasks not required. An exception after
Art. 6 para. 4 GDPR was not relevant. There was also consent from
the complainant to the use of their data for other purposes
no time before.
This violation was not within the scope of entrepreneurial activity

attributable to the employer. The employee committed the irregular

Act from his workplace, using the resources available to him

available work equipment, but not in the exercise of his professional

activity, but exclusively for private purposes.

The violation was reported by me in accordance with Article 83 (5) (a) GDPR i. in conjunction with Art. 5

Paragraph 1 lit. b DS-GVO punished with a fine of 300.00 €. at the repentance

When measuring the money, it was taken into account that only one person from the in

The facts in question were affected and only a few data were inappropriate

were used. In addition, was in favor of the person responsible

see that so far no data protection law objections against

158

fine proceedings, court proceedings

submitted him. As part of the hearing in administrative offense proceedings

the person concerned did not provide any information. Based on the present

knowledge, the net income was estimated and used as the basis for the

fine calculation used. Taking into account all relevant

Due to the circumstances, a fine in the lower range appeared in individual cases

of the fine framework of Art. 83 Para. 5 DS-GVO with € 300.00 as effective,

sufficiently dissuasive and proportionate. The fine is

not yet legally binding.

In my 48th activity report, under item 15.1, I already reported

comprehensive about the excess of employees in the public sector. based on

Case described here, it becomes clear that this type of irregular

trade is also present in the non-public area and for self-

actively acting employees of companies from the free market economy

the same principles apply in this regard.

Fine for repeated violations of the duty to provide information

I was contacted against a small corporation based in Hesse
several complaints from citizens alleging violations of the
Rights of data subjects according to Art. 15 i. in conjunction with Art. 12 GDPR. After
two of these complaints were finally examined in the supervisory procedure and
If violations were confirmed, I initiated fine proceedings. In one case
the complainant requested the provision of information under Art. 15
DS-GVO and the deletion of his data according to Art. 17 DS-GVO. After
However, he was only informed that the authentication was carried out
that only data that he had entered himself were stored. In the
As a result, the data was deleted so that the requested information was no longer available
could be granted. In the second case, the request for information
of the complainant initially not processed. Only after intervention
my authority was the submitter - with a delay of more than
three months - informed.
In both cases, contrary to Art. 15 DS-
GVO no information on the personal data of the data subject
granted within the period of Art. 12 Para. 3 S. 1 DS-GVO. The two violations
were by me according to Art. 83 Para. 5 lit. b i. in conjunction with Art. 15 i. In conjunction with Art. 12 Para. 3
S. 1 DS-GVO with a fine of a medium five-digit number
amount punished. When assessing the fine, the highlighted
Significance of the administrative offense and the medium degree of severity of the
breach taken into account. The generally frequently exercised information
right from Art. 15 DS-GVO takes within the framework of the rights of those affected
prominent position and represents an indispensable prerequisite

for the assertion of further data protection claims

Among other things, the responsible company benefited from the fact that
only one customer was affected by the incidents
the facts have been admitted and regretted and the proceedings
lasted an average amount of time.

In order to increase the fine, however, it had to be taken into account that the two
violations at issue occurred in quick succession. This
indicated a systematic error or an organizational problem
in the company and an increased level of breach of duty by the person responsible
towards. This was supported by the fact that in both cases the lawful procedure
when processing requests for information according to Art. 15 DS-GVO
was secured. Furthermore, it had a negative impact on the company
from the fact that the present case is not a first infringement in connection with
hang with data protection requests for information. Much more
was already due to a violation of § 43 Para. 1 No. 8a BDSG
a.F. i. In conjunction with Section 34 (1) sentence 1 BDSG old version from 2017, a regulatory
adversarial proceedings against the then and current managing director
of the company and in mid-2018 with a final judgment of the
District Court Wiesbaden because of a negligent, not fully granted
information, a fine of EUR 1,000.00 was imposed.

So that the fine has the effect intended by Art. 83 Para. 1 DS-GVO
unfolded, was the company's actual economic ability
to include. Based on the information in the annual financial statements of the company
I assumed that the total fine that had been pronounced

does not exceed the performance of the company and for them too

does not constitute a disproportionate burden. After weighing all the pros and

The fine lies against the criteria speaking against the responsible body

far in the lower range of the fine framework. The procedure is not yet

legally concluded.

16.2

Between measures and sanctions – evolution of the

Implementation of Art. 58 Para. 2 GDPR in practice

Art. 57 (1) lit. u GDPR obliges the HBDI, internal directories

according to Art. 58 Para. 2 DS-GVO. The balance sheet shows that the

interplay between measures and sanctions has developed positively.

According to Art. 57 Paragraph 1 lit. u GDPR I am obliged to keep internal directories

about violations of the GDPR and according to Art. 58 Paragraph 2 GDPR

measures taken on my territory, i.e. within my jurisdiction

160

fine proceedings, court proceedings

area of activity to create. By the end of 2020, I will be 31 in the reporting year

Warnings according to Art. 58 Para. 2 lit. b DS-GVO issued; I have

an instruction according to Art. 58 Para. 2 lit. c DS-GVO to the person responsible

or processors, the data subject's requests for exercise

to comply with the rights to which it is entitled under the GDPR; I

have eight instructions according to Art. 58 Para. 2 lit. d DS-GVO, the processing

ment processes, if necessary, in a specific way and within a

to bring them into line with this regulation within a certain period of time,

spoken; In addition, I have four measures under Art. 58 Para. 2

lit. f GDPR, according to which a temporary or final restriction

pronouncement, including a ban, and two

Fine notices pursuant to Article 58 Paragraph 2 lit. i i. V. m. Art. 83 DS-GVO imposed,

s.a. Fig. Part I No. 17.2.

Development of remedial powers according to Art. 58 Para. 2 DS-GVO

For supervisory practice and also for those responsible and

arbeiter was the remedial instrument according to Art. 58 Para. 2 DS-GVO in

still new territory for the first two years. The development in the year under review shows

clearly that slowly a routine in the application of the available

existing wide range of measures according to Art. 58 Para. 2 DS-GVO occurs.

Art. 58 Para. 2 GDPR

Each supervisory authority has all of the following remedial powers that it has

allow,

a) to warn a controller or a processor that intended

Processing operations are likely to violate this regulation,

b) to warn a controller or a processor if he is using

processing operations has violated this regulation,

c) instruct the controller or the processor to comply with the requests of the

data subject to exercise the rights to which they are entitled under this regulation

correspond to,

d) instruct the controller or the processor to carry out processing operations

where appropriate, in a specific manner and within a specific period of time

to comply with this regulation

e) to instruct the person responsible who is affected by a breach of the protection of

to notify the data subject accordingly of the data obtained,

a temporary or permanent restriction of processing, including

a ban on imposing

f)

g) the correction or deletion of personal data or the restriction

Articulation of the processing pursuant to Articles 16, 17 and 18 and the notification of the

Recipients to whom these personal data are sent pursuant to Article 17 paragraph 2 and

Article 19 were disclosed to order such measures,

h) to revoke a certification or to instruct the certification body to issue a certification in accordance with

revoke the certification granted under Articles 42 and 43, or the certification

to instruct the body not to issue a certification if the requirements for the

certification are not or no longer fulfilled,

to impose a fine under Article 83, in addition to or instead of in

measures referred to in this paragraph, depending on the circumstances of the individual case,

the suspension of the transfer of data to a recipient in a third country

or to an international organization.

i)

j)

The concept of Art. 58 Para. 2 DS-GVO is for the supervisory practice

big win to ensure compliance with GDPR norms.

From the conception of the standard it is clear that the supervisory authority does not

only fines are available for violations of the GDPR

to react. The remedial measures according to Art. 58 Para. 2 DS-GVO are

in the overall package what the sharp blade of the sword of supervision

matters.

In addition to the possibility of warning according to Art. 58 Para. 2 lit

gives the supervisory authority the option to prevent a violation

take action, the remedial measures under Article 58 (2) lit. b to j

GDPR if a violation has been identified.

The powers of remedial action according to Art. 58 Para. 2 lit. b - j can in turn

divided into sanctions and measures.

The focus of supervisory action is on shutting down the

violation. This is usually followed by an examination as to whether there is a sanction

may, and the decision on which sanction in the specific individual case

should be applied. In exceptional cases, this can already be closed

take place at an earlier point in time.

Measures

The measures according to Art. 58 Para. 2 lit. c-h and j DS-GVO can be structured

tour They reveal a system that has escalation levels.

The instruction according to Art. 58 Para. 2 lit c DS-GVO refers specifically to the

Applications made in the context of the rights of those affected. If for example

wrongly refuses to provide information in response to an application under Art. 15 GDPR

then I can instruct the responsible body to deal with this matter

to fulfill. If the instruction is not fulfilled, I have the option of the

Combine decision with administrative coercive measures.

With Art. 58 Para. 2 lit. d GDPR, the regulation gives me the opportunity

an instruction to controllers or processors

fine proceedings, court proceedings

enacted and to instruct them to carry out processing operations, if necessary

specific manner and within a specific period of time in accordance with

bring the GDPR. If this measure is unsuccessful,

there is an escalation level for this. Because then measures according to Art.
58 Para. 2 lit. f DS-GVO may be suitable for a data protection
to achieve shape state. Then there is a situation that may
would justify the processing temporarily or under certain circumstances
to even finally restrict or even issue a ban on processing
to speak. This must be checked in each individual case.
I have not yet had to express measures according to the letters g, h, j
chen. Art. 58 Para. 2 lit. g DS-GVO grants me the right to have the correction
or deletion of personal data or restriction of
Processing pursuant to Articles 16, 17 and 18 and informing the recipient
catcher to whom this personal data is transferred in accordance with Art. 17 Para. 2 and Art.
19 were disclosed to inform about such measures. That would
basically the escalation level to a measure according to Article 58 (2) lit. c
GDPR. Art. 58 (2) lit. h GDPR will play a role in practice,
if the certification according to Art. 42 and 43 DS-GVO is filled with life.
No permits have been granted to date. According to Art. 58 (2) lit. j
DS-GVO I am allowed to suspend the transmission of data to a
Arrange recipients in a third country or an international organization.
But I did not make use of this in the year under review either.
sanctions
In addition to or in lieu of the appropriate measures taken pursuant to this
regulation were imposed, should the supervisory authority impose sanctions
eventually impose fines (see Recital 148 GDPR). In the
case of a minor infringement or if the
hanging fine a disproportionate burden on a natural
Person would cause, instead of a fine, a warning

be granted. The sanctions referred to in recital 148

can be found between the powers of remedial action in Article 58 (2) under letter b

and i DS-GVO again.

I have already heard about the fine proceedings in my 47th and 48th employment

report reported. The fine procedure is the ultima ratio. For minor

violations in the reporting year, I have the option of issuing a

warning exercised. There was always a consideration about that

appropriate, necessary and proportionate means.

In the year under review almost twice as many as in the previous year

warnings issued. The peculiarity of this warning is

that it is pronounced without a warning money. The procedure over the

Warning is based on the Hessian Administrative Procedure Law

law and not according to the provisions of the Administrative Offenses Act. At

my decision on the type of sanction I have the requirements

from Recital 148 S. 3, which deals with the criteria according to Art. 83 Para. 2

DS-GVO largely covered, taken into account and included in my decisions

information about the type of sanction.

16.3

Development of the administrative court proceedings at the HBDI

Since the GDPR came into force in May 2018, the number of administrators has

court proceedings increased sharply. Those affected turned

in the field of credit bureaus against the final decision in the supervisory

procedures, in the field of video surveillance and employee data

protection were the measures adopted in accordance with Art. 58 Para. 2 DS-GVO and from the area of employee data protection, the determination of attacked for violations.

Since the beginning of 2019, I have noticed a significant increase in lawsuits against my supervisory decisions before the administrative court. With the European data protection reform became the right in Art. 78 Para. 1 DS-GVO strengthened on effective legal remedy against a supervisory authority and that before May 25, 2018 rather informal action has turned into an administrative formal action transformed.

Art 78 para. 1 GDPR

Every natural or legal person has, without prejudice to any other legal or out-of-court legal remedy, the right to an effective one judicial remedy against a legally binding decision affecting them a supervisory authority.

Affected parties and court proceedings

Affected parties who submit a complaint to me are, according to Art. 77 Para. 2 DS-GVO by me about the status and the results of the complaint and about the possibility of appeal under Article 78 GDPR.

fine proceedings, court proceedings

Art. 77 Para. 2 GDPR

The supervisory authority to which the complaint was lodged shall inform the complainant about the status and the results of the complaint, including the Possibility of a judicial remedy under Article 78.

According to Art. 78 Para. 1 DS-GVO i. in conjunction with § 20 BDSG

object to a legally binding decision affecting them. dar

In addition, the data subject may, in accordance with Article 78 (2) GDPR

against me with an effective remedy if I fail to do so

deal with a complaint or not within three months

about the status or the result of the data collected in accordance with Art. 77 DS-GVO

report the complaint.

Controllers, Processors and Legal Proceedings

According to Art. 78 Para. 1

i. V. m. § 20 BDSG and the VwGO against my measures according to § 58 para.

1, 2 and 3 GDPR. Excluded are the fine procedures, the

according to § 41 BDSG according to the OWiG, the StPO and the GVG.

Competent administrative court

Is locally responsible for complaints against my administrative decisions

according to § 20 Abs. 3 BDSG the Administrative Court Wiesbaden and second

Instance of the Administrative Court in Kassel.

To the statistics

Since the beginning of 2019, 46 administrative court proceedings on data protection

questions have become pending. At the end of 2020 I still had 24 procedures planned

open to the Administrative Court of Wiesbaden (Part I, Item 17.2.).

The court proceedings are carried out by my authority itself, through the legal

at, which is also responsible for carrying out the fine proceedings.

The focal points of the administrative court proceedings were questions from the

Departments of credit agencies, employee data protection, video surveillance

and information rights according to Art. 15 DS-GVO.

The majority of administrative court proceedings were directed

gen notices, the person filing the complaint i. s.d. Article 77 paragraph 2

DS-GVO opened that after examining the complaint

be that there is no violation. In the two lawsuits for failure to act

165

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

According to Art. 78 Para. 2 DS-GVO, it turned out that this

were unfounded.

The two procedures for video surveillance from 2019

and 2020 were successfully completed in 2020. The lawsuit against

Measures ordered to create a data protection compliant

Video surveillance could through the insight of the plaintiff after a

On-site appointment scheduled by the court by means of execution according to § 161 VwGO

be completed successfully.

It has remained open so far whether the determining administrative act, the one

Breach of the GDPR without issuing a warning as a

Minus to the warning according to Art. 58 Para. 2 DS-GVO determines a right

moderate completion of proceedings. It is currently represented that one

such a decision as a minus to the warning on Art. 58 Para. 2 lit. b

GDPR can support.

The administrative court proceedings were predominantly

withdrawal according to § 92 VwGO or settlement or under the conclusion of a

comparison ended.

166

Labor Statistics Privacy

17. Labor Statistics Privacy

Labor Statistics Privacy

17.1

facts and figures

The statistical evaluation of the workloads under this number corresponds

the formal requirements specified by the data protection conference

to be able to make a nationwide statement. These values are e.g. the

European Commission and the European Data Protection Board

according to Art. 59 DS-GVO.

facts and figures

a. "Complaints"

Number of complaints received under the GDPR in the reporting period

went. Such operations are considered complaints upon receipt

counted, which are received in writing and in which a natural person submits a

personal concern to which Art. 78 DS-GVO is applicable.

This includes duties. Telephone complaints will only then

counted if they are put into writing (e.g. by annotation).

b. "Consultations"

Number of written consultations. This includes summarily consulting

by those responsible, affected persons and their own government

tion.

Not: (telephone) oral consultations, training courses, lectures, etc.

c. "Privacy Breach Notifications"

Number of written reports

i.e. "Remedial Actions"

Number of measures taken in the reporting period

became.

(1)

(2)

(3)

(4)

(5)

e. "European Procedures"

(1) Number of proceedings with concern (Article 56)

(2) Number of lead proceedings (Article 56)

(3) Number of procedures according to chap. VII GDPR (Art. 60 et seq.)

according to Art. 58 Para. 2 a (warnings)

according to Art. 58 Para. 2 b (warnings)

according to Art. 58 Para. 2 c-g and j (instructions and orders)

according to Art. 58 Para. 2 i (fines)

according to Art. 58 Para. 2 h (revocation of certifications)

case numbers

01/01/2020

until

12/31/2020

5,414

(of that

855 charges)

1,983

1,433

(1) 1

(2) 31

(3) 13

(4) 2

(5) 0

(1) 198

(2) 5

(3) 724*

167

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

f. "Formal support for legislative projects"

Here, the total number from parliament/government is lumped together

called for and carried out consultations. this includes

also the participation in public committees and opinions.

dishes.

54

*In the previous year there were 66 procedures.

17.2

Additional explanations on the facts and figures of Part I, Section 17.1

The following illustrations explain and supplement the evaluation

17.1 also in comparison with the previous year and the other

other areas of work in the year under review. Overall, the numbers show a

significant increase compared to the previous year, which was due to entries in the context of

new DS-GVO was shaped. What is striking in 2020 are the values for the

Subject areas credit bureaus and collection agencies, schools/universities

schools, e-communication/Internet, trade/craft, clubs/associations

and employee data protection.

Complaints and Advice

The data protection implementation of the requirements of the Corona Ordinance

ments by those responsible, uncertainties on the part of employers and

employees on home office issues, the public discussion about

business models from credit agencies and products from software manufacturers

were topics that were present for almost the entire year.

The so-called Schrems solved further need for advice and inquiries

II judgment of the ECJ (for details, see also the article, Part I, Item 2.2).

In addition to the written submissions,

the "quick" way of clarification by telephone information sought. The

Concerns of those responsible and those affected - from the public and

non-public area – were urgent if they had to deal with the at short notice

Specifications of the various Corona regulations or the measures

and recommendations from health authorities/RKI and

had to respond to them. This manifested itself in the enormous increase in

Telephone consultations and clarifications that last longer than ten

minutes, but ultimately found no documented precipitation.

In the testing area, the start of the "new" testing activity according to § 29a HSOG

reported to two police headquarters.

The following overview presents the amounts of input (complaints

and consultations) of the reporting year compared to the previous year:

168

Labor Statistics Privacy

areas of expertise

credit bureaus,

collection

school

school, archives

e-Communication

tion, Internet

employee

data protection

video observer

tion

credit industry

trade, hand

work, trade

traffic, geo

data, farmer

shaft

Health,

Care

operational/

Official DPO

municipalities

Choose

police, judiciary,

constitutional

protection

associations

volumes

address trading,

Advertising

housing, rent

social

utility

company

IT security,

IT technology

insurances

broadcasting

see press

religion

communities

data protection

Outside the EU

difficult-

loading

the

Number 2019

loading

ratun-

gene

inputs

total

velvet

difficult-

loading

the

Number 2020

loading

ratun-

gene

923

56

512

199

253

949

182

240

101

16

115

129

57

174

54

50

76

30

46

46

3

19

312

52

131

95

10

58

39

180

219

112

32

77

6

66

63

22

57

17

1

6

942

368

564

330

348

959

240

279

281

235

227

161

134

180

120

113

98

87

63

47

9

1201

191

565

263

317

323

264

238

201

17

137

201

80

169

65

63

91

19

545

53

170

90

15

74

47

86

258

115

73

119

4

59

56

17

3***

91***

52

57

20

11

29

0

3

29

inputs

total

velvet

1220

736

618

433

407

338

338

285

287

275

252

274

199

173

124

119

108

94

81

57

23

40

169

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

areas of expertise

Research,

statistics

Aliens Law

taxation

other

men < 10 (e.g.

chambers

landness,

finance

subtotal

me get hurt

and consultations

BCR procedure

with German

or across Europe

ter leader

tion of the HBDI

reports from

data breaches*

difficult-

loading

the

Number 2019

loading

ratun-

gene

10

3

1

33

1

8th

0

27

inputs

total

velvet

11

difficult-

loading

the

Number 2020

loading

ratun-

gene

10

1

inputs

total

velvet

11

11 See Other See Other See Other

1 See Other See Other See Other

26

60

20

6

4,258

1,610

5,868

4,559

1,959

6,518

17

40

1,453

1433

7,991

9,444

7,338

7,044

14,382

Total

documented

inputs

Plus sum

telephone

consultations

and information

from more than

10 mins**

Total

documented

+ telephone

inputs

* see also article part I, number 15.1, 15.2

** Telephone inquiries that are not reflected in writing will be charged at a flat rate

recorded. They took the form of advice, information, explanations and questions of understanding of the DS-GMO and similar both on general topics and on specific issues, such as e.g. B.

with regard to the so-called Schrems II judgment of the ECJ or to specific data protection law

Implementation of the Corona regulations. Examples of such telephone calls in November,

as a month without any special incidents, counted and extrapolated as an average value.

*** Further IT topics were accompanying a legal inquiry or a data breach

to check the registration and were therefore not counted independently.

17,435

Labor Statistics Privacy

Other miscellaneous tasks

Unaccounted for in the tables above, but no less noteworthy-
valuable tasks and topics that were dealt with in the reporting year
for example:

– Activities of the internal data protection officer at the HBDI

There were 35 requests for information from citizens regarding the
processing of their data at the HBDI and 21 corresponding ones
consultations carried out.

– Regular consultations

With the internally appointed data protection officers from various
public areas (e.g. of ministries, cities and municipalities and
the European data protection supervisory authorities) were exchanged
maintained and z. T. provided regular consulting services.

– Press and public relations

The number of press inquiries increased in 2020 with 153 inquiries
more than tripled compared to 2019 with 49 inquiries.

Numerous publications and assistance were the responsibility
citizens on the homepage (e.g. in the health
area, for clubs and schools) of the HBDI.

– training services

Four trainee lawyers were elected in their elective or
Management stations trained.

– Training and lectures

15 data protection training courses, some lasting several days,

Seminars and training courses in the public and non-public sector

carried out.

– Participation in conferences, working groups and working groups

Consultations and coordination between the supervisory authorities

and in their bodies at state, federal and EU level, but also

overall with contact persons from non-European third countries,

are now essential for successful data protection in Hesse.

The committee work is sometimes very time-consuming, but no longer

bar. In the times of the Corona lock-downs, personal meetings were held

replaced by video conferencing. The Conference of Data Protection and

The Freedom of Information Officer (DSK) therefore met approximately every two months

on current topics. The 2020 results are in Appendix I

printed in extracts, but also in detail on the home page

of the data protection conference www.datenschutzkonferenz.de.

The HBDI is involved in all areas of the DSK working groups.

Also in the sub-working groups used for special topics

are committed, employees of the HBDI. In

numerous EU bodies (e.g. BTLE, CSC, SCG SIS II, SCG Eurodac,

SCG VIS) HBDI was able to bring in its cooperation. In addition,

support services to the EU Commission, e.g. B. through

participation and contributions within the framework of the Schengen evaluation.

Remedial measures and court proceedings (see also contributions Part I

Clause 16.2, 16.3)

remedial actions

(1) Warnings (Art. 58 Para. 2 a GDPR)

(2) Warnings (Art. 58 Para. 2 b GDPR)

(3) Instructions and orders (Art. 58 Para. 2 c-g, j DS-GVO)

(4) Fines (Art. 58 Para. 2 i GDPR)

(5) Revocation of certifications (Art. 58 Para. 2 h GDPR)

In total

court proceedings

Complaints pursuant to Art. 78 Para. 1 GDPR

Complaints pursuant to Art. 78 (2) GDPR

Other

In total

Number

1

31

13

2

0

47

Number

19

2

4

25

Data Breach Notifications

a. Reports according to Art. 33 DS-GVO and § 60 HDSIG (see also article part I no.

15.1, 15.2)

general overview

Ground

– wrong shipment

– Hacker attacks, phishing, malware

– Loss/theft of documents, data carriers, etc.

– Unlawful disclosure/sharing of data

– Impermissible inspection (incorrect setup of access rights, etc.)

– Open e-mail distribution list

Number

494

184

142

107

85

76

172

– Abuse of access rights

– Unauthorized publication

– Incorrect assignment of data

– Disposal that does not comply with data protection regulations

– Unencrypted e-mail transmission

– Other

In total

Labor Statistics Privacy

43

25

21

9

7

240

1,433

most affected areas

Credit industry, credit bureaus, trade and commerce 491 cases

Employee data protection 254 cases

Health sector 230 cases

173

Appendix to I

Appendix to I

Appendix to I

1. Resolutions of the Conference of Independents

Federal and state data protection supervisory authorities

1.1

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

11/25/2020

Information procedures for security authorities and

Design intelligence services in accordance with the constitution

When setting up the manual information procedure for inventory data

of telecommunications customers, the legislature has important constitutional

legal requirements ignored. The previous access rights

of the security authorities are too far-reaching. The data protection supervisory

Federal and state authorities have been working on the for years

Disproportionality of corresponding regulations pointed out.

By resolution of May 27, 2020 - 1 BvR 1873/13 and 1 BvR 2618/13 -

("Inventory data information II"), the Federal Constitutional Court again

constitutional requirements for the design of the manual

Status data information procedure made. The court affirmed that

both the transmission of data by telecommunications service providers

as well as retrieval by authorized bodies, each with a proportional

gene and standard-clear legal basis. The transmission and

According to the court, retrieval regulations must state the intended use

adequately limit the use of data to specific purposes

cke, factual intervention thresholds and a sufficiently weighty one

Bind the protection of legal interests (principle 1). Includes that for use

to avert danger and the activities of the intelligence services in principle

a concrete danger in individual cases and an initial suspicion for criminal prosecution

must exist. The assignment of dynamic IP addresses must be above

addition to the protection or reinforcement of legal interests of

serve equal weight (4th guiding principle). The transmission regulation of § 113

Telecommunications Act and a number of corresponding ones

technical legal retrieval regulations were in view of this for with the

Basic Law declared incompatible.

The previous regulations remain in place until the new regulation, at the longest

however, until December 31, 2021 depending on the reasons for the decision

further applicable. In the interests of legal certainty, the Conference

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

of the countries (DSK), however, to those responsible for politics, this deadline is not

exhaust, but the manual information procedure as promptly as possible

to be constitutionally compliant.

The DSK also considers it necessary that federal and state legislators

in the course of the implementation of the decision not only directly from the

adjust the regulations affected by the decision, but all comparable

available regulations, the basis for the transmission and retrieval of

personal data may be, in the light of the decision of the

review the Federal Constitutional Court and, if necessary,

shape shape. This applies in particular to regulations of the police and

Constitutional protection laws of the countries, the provision of information about

Link data only to the fulfillment of the tasks of the authorized body.

Such schemes come with the risk of unlimited uses of

Connected to data and therefore disproportionate (cf. BVerfG, above-mentioned decision

of 27 May 2020, paragraphs 154, 197). Data queries may no longer be due

such vague legal bases.

1.2

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

11/25/2020

Website operators need legal certainty

Federal legislature must comply with European legal obligations

Finally fulfill the "ePrivacy Directive".

The legislator is obliged to the EU directive on the European

Electronic Communications Code of December 11, 2018 (RL

2018/1972/EU) by December 20, 2020.

The conference of the independent federal data protection supervisory authorities

and of the countries (DSK) calls on the legislator to finally introduce regulations

enacted to fully comply with the ePrivacy Directive1 and in accordance with the

implement the General Data Protection Regulation (GDPR).

In the past, the DSK has repeatedly pointed out that

that the legislature does not or not Art. 5 Para. 3 ePrivacy Directive

properly implemented.2 The judgment of the Federal Court of Justice (BGH)

1 Directive 2002/58/EC as last amended by Directive 2009/136/EU

2 See circular resolution of the federal and state data protection officers

from February 5, 2015, available at: https://www.datenschutzkonferenzonline.de/media/

en/20150205_en_Resolution_Cookies.pdf

Appendix to I

of May 28, 2020 (I ZR 7/16 - "Planet49") strengthened according to opinion

the DSK the long-standing urgent need for action.

As early as April 2018, the DSK stated in the position determination "On application

of the TMG for non-public bodies from May 25, 2018" the status

punkt represented that the data protection regulations of the Telemedia Act

are no longer applicable in addition to the GDPR. A detailed justification

on this legal opinion was published by the DSK in the guidance for

Telemedia providers published in March 2019.3

The BGH had to decide a dispute in the Planet49 proceedings in which the

sued companies personal data about usage behavior

from consumers using cookies to create pseudonymised usage profiles

processed and used for personalized advertising. after the word-

according to § 15 paragraph 3 Telemedia Act (TMG) would be such a procedure

only permissible if the persons concerned are informed accordingly

and have not objected (so-called objection solution).

With a view to Art. 5 Para. 3 ePrivacy Directive, the BGH sets § 15 Para. 3 TMG

to the effect that already in the absence of effective consent

such a contradiction can be seen, which is why an active consent

is required. Based on this interpretation of § 15 paragraph 3

TMG he applies this regulation in addition to the DSGVO. Ultimately the

BGH followed the preliminary ruling of the European Court of Justice and

confirms the basic requirement of effective consent for

the setting of cookies.

Even the fact that the DSK and the BGH in a very practice-relevant

legal question agree in the result that a processing,

as presented to the courts for decision, requires consent,

however, differ in the derivation of this result

Represented views illustrates the extent of the legal ambiguity.

With the decision, the demarcation of the regulatory areas between

ePrivacy Directive, GDPR and the data protection regulations of the TMG German

much more difficult. The BGH expressly states that the ePrivacy Directive

and DSGVO pursue different protection directions. The regulations in

§§ 12 to 15 TMG expressly link to the term processing

personal data. This matter is at European level

3 Position determination of the DSK from April 26, 2018 "On the applicability of the TMG for

non-public bodies from May 25, 2018", available at: https://www.datenschutz-

konferenz-online.de/application notes.html), guidance for providers of

Telemedia (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.

pdf).

179

largely conclusively regulated by the General Data Protection Regulation.

Art. 5 para. 3 ePrivacy Directive, on the other hand, also has information without

Personal reference to the subject of the regulation. It therefore remains open whether § 15

Para. 3 TMG - contrary to the wording - even then an implementation of the

Art. 5 para. 3 ePrivacy Directive should represent if the information that

stored or accessed on a participant's device

will have no personal reference.

§ 15 para. 3 TMG refers expressly and exclusively to the

Creation of pseudonymous usage profiles for advertising purposes

market research or for needs-based design of the telemedia. The

Storage of information or access to information that already exists

are stored in the end device of a participant or user, however

also for other purposes and is not limited to § 15 Abs. 3 TMG

mentioned purposes.

Finally, Art. 5 Para. 3 ePrivacy Directive requires in principle without

taking specific purposes into account. Only in Art. 5 para.

3 sentence 2 ePrivacy Directive there are exceptions to this principle.

This rule-exception principle is not reflected in the TMG.

Website operators and other actors who use their services e.g. in relation to

"Cookies" have to be designed in a legally compliant manner, need legal clarity. The

The legislature is therefore called upon to eliminate existing legal uncertainties

immediately through clear legislation that conforms to European law

remove.

1.3

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

11/25/2020

To protect confidential communications with a secure

End-to-end encryption - Proposals of the Council of

stop the European Union

The conference of the independent federal data protection supervisory authorities

and of the countries (data protection conference) occurs demands of the governments

of the Member States of the European Union, security authorities

and secret services to open up the possibility of accessing encrypted content

access communication. In response to recent terrorist attacks

these authorities and services access to the encrypted communication

tion are made possible. This also includes messenger services in particular

like WhatsApp, Threema or Signal. According to the draft resolution "Si-

180

Appendix to I

Security through encryption and security despite encryption" of the

Council of the European Union (No. 12143/1/20 of November 6, 2020)

should appropriate opportunities in cooperation with the providers

be developed by online services.

Secure and trustworthy encryption is an essential prerequisite

requirement for resilient digitization in business and administration

tion. Companies must be able to protect themselves against industrial espionage.

However, a weakening of the encryption process could be European
put companies at a disadvantage in the global market. Citizens
must ensure that digital administrative services are used securely and with integrity
can trust and need protection from extensive surveillance
investigation and data misuse. The goals of the Online Access Act,
to offer administrative services electronically via administrative portals,
would be thwarted if users of these portals took advantage of the
confidentiality of electronic communications could not be assured.
Encryption is also a key means of data transmission
to third countries according to the recommendations for additional measures for
Transmission tools to ensure the EU level of protection of the
European Data Protection Board in response to the "Schrems
II" judgment of the European Court of Justice.
If the proposals of the Council of the European Union were implemented,
undermine secure end-to-end encryption and necessary
Trust is destroyed without the desired goal, the investigative
opportunities of security authorities to improve, sustainably and effectively
is reached. Backdoors in encryption procedures provide security
and effectiveness of these entirely in question. The excavation of encryption
solutions would inevitably lead to evasion
Evasion techniques are used by both criminals and terrorists
as well as technically experienced citizens could operate.
At the same time, the use of more effective end-to-end encryption
practically impossible for technically less experienced citizens
made.
In 1999, for good reason, the Federal Government committed itself to the

German crypto policy guidelines on the use of cryptographic methods

known. In Europe, the confidentiality of communications is protected by the

individual right to respect for communication protected in Art. 7 GRCh.

In addition, for stored communication content, Art. 8 GRCh

guaranteed right to protection of personal data. In Germany will

the protection of fundamental rights when using communication services

the telecommunications secrecy in Art. 10 GG and supplemented by the right to

informational self-determination and the right to confidentiality and

Integrity of information technology systems guaranteed. logically

In 2015, the federal government again approved the use of crypto

graphy in the charter to strengthen trusted communications.

The Data Protection Conference sees no reason for the Council of Europe

European Union deviates from these fundamental rights-preserving positions, especially since

others that massively invade the privacy of users

Powers are also not required. The effective fight against terror

is a legitimate concern, but the security agencies are responsible for the

pursued goals already extensive and very intervention-intensive instruments

available.

The data protection conference has repeatedly advocated the use of more secure and

integrity encryption and trust in the indispensability

worthy and integrity communication possibilities pointed out. She

calls again on the Federal Government and the German EU Council Presidency

the use of state-of-the-art encryption

to promote solutions and to strive to weaken such solutions,

determined to oppose. Secure end-to-end encryption must

become the rule in order to ensure a safe,

trustworthy and honest communication in administration, economy,

to ensure civil society and politics.

1.4

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

09/22/2020

Data protection also needs regional courts in the first instance

With the "draft of a law to make the fine procedure more effective"

(BR-Drs. 107/20 (B)), the Federal Council wants jurisdiction in the first instance

of the regional courts for fines under the General Data Protection Regulation

(GDPR) above 100,000 euros. Even about fines in this

In the future, the district courts will decide the amount.

The aim of making the fine procedure more effective will be combined with the planned one

law cannot be achieved. The bill misjudges in blatant

Point out the particular economic, technical and legal complexity

of GDPR fines. A deletion of the regional court jurisdiction

would also not relieve the district courts, but even more

load than before.

182

Appendix to I

The right to sanctions of the GDPR is - in contrast to what is assumed by the Bundesrat - also included

the sanctioning of conventional German administrative offenses such as

Road traffic fines are in no way comparable. It goes here

not about the prosecution of petty crimes, but about Union-wide

highly relevant procedures to protect the free movement of data and the

privacy of citizens. In doing so, millions of

customer data may be affected. Data protection offenses with a fine

Values over 100,000 euros have a special, economically and technically

complexity and therefore require an appreciation by the

by a collegiate court. They are much more likely to deal with white collar crime

comparable, which are assigned to the regional courts anyway. Not without

The reason why the European legislature has to do with the fine regulations of the

GDPR based on antitrust law. For similarly complex administrative offences

in cartel matters in Germany it is even a responsibility of the

given to higher regional courts. This rating also comes in that far

clear wording of Section 41 (2) sentence 1 of the Federal Data Protection Act

(BDSG) expressing a corresponding application of the regulations

about the criminal proceedings and thus also about the occupation of the criminal chambers

as so-called large fine chambers according to § 76 GVG.

The conference of the independent federal data protection supervisory authorities

and the countries (data protection conference) therefore calls for the retention of the

regional court jurisdiction for GDPR fines of over 100,000 euros

and warns against a deletion of the regulation and its consequences.

1.5

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

09/22/2020

Creating digital sovereignty in public administration –

Better protect personal data

The term “digital sovereignty” is used in different ways in the public debate.

which uses meanings. According to the definition of the center of excellence

In a comprehensive sense, public IT1 is digital sovereignty

Sum of all abilities and possibilities of individuals and institutions,

their roles in the digital world independently, self-determined and secure

to be able to exercise.

1 Public IT Competence Center (ed.), Gabriele Goldacker, Digital Sovereignty,

available at https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver-

%C3%A4nit%C3%A4t

The role of public administration is to comply with the law

of state tasks. From the point of view of those responsible in the public

Administration means digital sovereignty in particular, independently

to be able to divorce, as set out in Art. 1 General Data Protection Regulation (GDPR

GVO) formulated goals in accordance with the in Art. 5 DS-GVO

Principles for the processing of personal data, such as legal

moderation, transparency, purpose limitation and security of processing,

are to be implemented. According to the conference, this requires the independent

gigantic data protection supervisory authorities of the federal and state governments (data

protection conference) Freedom of choice and full control of those responsible

about the means and procedures used in digital processing

of personal data, if necessary with the involvement of the

respective processor.

However, the digital sovereignty of public administration is after a

for the Federal Government Commissioner for Information Technology

conducted "Strategic Market Analysis"2 impaired, "since the business

public administration with external, mostly private IT

offer significant dependencies. After that, these result

Dependencies from the technical nature of the IT landscape

the strongly software-oriented processes, from the fact that

the employees have become accustomed to the software used,

contract clauses as well as from the existing market conditions". They bring

Loss of control and limited availability, confidentiality and

integrity of the processed personal data. Also before

against this background, the IT planning council has set itself the goal of

Sovereignty of public administration in their roles as users,

to continuously strengthen manufacturers and clients of digital technologies.

The data protection conference shares the assessment of the IT planning council that

the digital sovereignty of public administration is impaired, and

sees their guarantee as a priority field of action. from her

view are data protection regulations for large software providers that

Diversification recommended in the "Strategic Market Analysis".

Use of alternative software products and the use of open source

Software particularly promising options for action. through the

Use of open source software can ensure the independence of the public

Management of market-dominating software providers permanently secure

2 PwC Strategy & (Germany) GmbH, Strategic market analysis to reduce

Individual software vendor dependencies, available at https://www.cio.

bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.

pdf?__blob=publicationFile

be asked. Specifically, the data protection conference calls for the federal, state and municipalities to only use hardware and software in the long term

– giving those responsible exclusive and complete control about the information technology they use, in particular in that access and changes only after prior information and approval of those responsible in individual cases,

– in which all available safety functions for responsi- literal are transparent and

- the use of the hardware and software as well as access to personal related data without unauthorized persons being aware of it and without inadmissible user profiles being able to be created.

In the short term, strengthening digital sovereignty requires public Administration in federal, state and local authorities to comply with the data protection legal requirements in particular:

1. Improved options for assessing data protection law Products and services - both in the selection and in the ongoing operation:

– Certifications allow those responsible for testing and control facilitate if they do not independently form a valid picture of the complex functioning of information technology.

– The ministerial level should be made responsible for providing guidelines to do for public administration.

– In addition, authorities should cooperate more closely in order to Being able to provide expertise yourself.

2. Consideration of the goals and criteria of digital sovereignty

the allocation and procurement of hardware, software, information and

Communication technology and IT services:

– For the allocation and procurement of hardware, software, information

tion and communication technology as well as IT services should be

Consistent with European public procurement law tender criteria

are designed to be preferred in awarding such providers

to be able to choose which ones enable digital sovereignty.

3. Use of open standards by product developers so that the

Those responsible will also actually be able to offer providers

and to switch products if they are unfamiliar with their products and services

the data protection requirements not (any longer) or only insufficiently

can implement:

– The use of open standards can be limited by their inherent

Transparency help to ensure verifiability and a

to facilitate control. This affects system software and in particular

Data formats, but also databases and application software that

set up on software platforms. There are also open standards

suitable for avoiding undesired lock-in effects. In particular

can do this via the establishment of federal/state/municipal

cross-national development networks and distributes expenses

economies of scale are lifted. Therefore, those responsible should

Prefer use of products and services that are open

use defaults.

4. Publication of the source code and specifications publicly fi-

nanced digital developments:

– If software or hardware standards with financial participation

are developed by the public sector, these should be standard

be published in such a way that they can be understood.

– By default, these should be designed in such a way that a public

further development is possible (open source licenses).

5. Ways to control access to data, configuration

of systems and the design of processes:

– Those responsible must have actual control options

dispose, in particular, to fulfill their obligations under Art. 25 DS-GVO

to be able to Data protection through technology design and data

Protection-friendly default settings must be an elementary part of

Services and products related to the

processing of personal data. Responsible should

only procure and use products and services that

observe these principles. Organizations with distributed responsibility

(e.g. municipalities, federal states or service providers involved

such as corporations) must also be used for centrally procured or operated

Components such as hardware, software and services that

be able to make relevant settings in order to ensure a legally compliant

to ensure the operation of the procedures. For centrally provided

Applications, for example in one currently being discussed in the IT planning council

"Management Cloud", it is a necessary requirement that the

respective data protection regulations of those responsible for

Operation and configuration can be implemented individually. The

must be taken into account in the design.

The data protection conference believes that strengthening the digital

Sovereignty of great strategic importance for public administration

has and must be pushed forward together and continuously. She

calls on the federal, state and local governments to act in the resolution

listed criteria for strengthening the digital sovereignty of public

public administration in the areas of IT procurement as well as system and

Process development to be taken into account.

1.6

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

01.09.2020

Patient Data Protection Act: Without improvements to the

Data protection for the insured violates European law!

On July 3, 2020, the German Bundestag approved the patient data protection

Act (PDSG) contrary to the independent data protection supervisory

the criticism voiced by federal and state authorities. The

Criticism is directed in particular at the only roughly granular design

Access management, authentication for the electronic patient file

(EPA) and the agent solution for policyholders who do not have an appropriate

end device.

The PDSG is to be finally discussed in the Bundesrat on September 18, 2020

become.

Central legal regulations are in contradiction to elementary pro-

compliance with the EU General Data Protection Regulation (GDPR). contrary to

current draft, the insured must already at the time of

EPA will have full sovereignty over their data on January 1, 2021

receive. This also corresponds to the PDSG formulated by the legislature itself

the patient's sovereignty over the insured

EPA in principle to uphold without restrictions and the use of

Design EPA for all insured persons in accordance with data protection.

The bill does not achieve these goals. At the start of the EPA

will all users in relation to the service providers

like (doctors, etc.) stored in the electronic patient file

forced to an "all or nothing" as there will be no control in 2021

at the document level for this data. It means that

those to whom the insured grant access to their data, all there

information contained can be viewed, even if this is in the concrete

treatment situation is not required.

Only a year after the start of the EPA, i. H. from January 1, 2022

only insured persons who have suitable devices for accessing their EMR

(smartphone, tablet, etc.) independently use a document-specific

Carry out control and assignment of rights in relation to these documents.

All other insured persons who do not have suitable end devices or

for security reasons to protect their sensitive health data

do not want to use (i.e. so-called non-frontend users).

not exercise these rights beyond the key date of January 1, 2022. From the
January 1, 2022, the PDSG allows non-frontend users to do so
only a representative solution. After that, this can be done by means of a representative
and exercise their rights on their mobile device. In case of substitution
However, the insured would have to give their representative full access
access their health data.
Another point of criticism is the authentication process for the EPA
and the "guarantee of the necessary high level of data protection law
protection levels". Since the data in question is health data
and therefore highly sensitive personal information
According to the requirements of the GDPR, the authentication is as high as possible
Ensure state-of-the-art security. This applies in particular
special for authentication methods without using the electronic
health card. If alternative authentication methods are used
that do not meet this high standard is a violation of
the GDPR.
In its statement on the PDSG of May 15, 2020, the Federal Council
(BR-Drs. 164/1/20, see number 21. to Article 1 number 31 [§§ 334 ff. SGB
V-E9]) the Federal Government to considerable concerns with regard to the
DSGVO conformity of the PDSG pointed out. His criticism relates to
Essentially due to the fine-grained access
management and the resulting restriction of data sovereignty
rity of the insured. He called on the federal government to
Ren legislative procedures, in particular the proposed regulation on
Offer and to set up the EPA (§ 342 SGB V) comprehensively regarding
review data protection concerns.

Also in the light of this, the independent data protection supervisory

authorities of the federal and state governments to the Bundesrat on the occasion of its for

18 September 2020, the Mediation Committee

to call to make necessary data protection improvements to the PDSG

still to be achieved in the legislative process.

188

Appendix to I

1.7

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

08/26/2020

Implement register modernization in accordance with the constitution!

With the law introducing an identification number in the public

Administration (contained in the Register Modernization Act - RegMoG) plans

the federal government is modernizing the administration

Register. For this purpose, among other things an identification number (ID no.) for natural persons

Persons as a cross-register classification feature in all for the

federal register relevant to the implementation of the Online Access Act

countries are introduced.

The tax identification number should be used as a general classification feature

mer (tax ID), prior to their progressively expanded use, the

data protection officers of the federal and state governments several times

had warned. The now planned extended use of the tax ID

as a uniform personal identifier completely separates from its original

original purpose for purely tax matters, although

this is the only reason why it can so far be regarded as constitutional.

The conference of the independent federal data protection supervisory authorities
and the countries (data protection conference) already pointed out in their resolution
from 09/12/2019 to point out that the creation of such uniform and
cross-administrative personal identifiers or identifiers (also
in connection with a corresponding infrastructure for data exchange)
entails the risk that personal data is easily disclosed on a large scale
linked and completed to form a comprehensive personality profile
can become.
The Federal Constitutional Court has the introduction of such personal identification
signs have always imposed narrow barriers that are disregarded here.
A look at the scope of application of the planned regulation shows this
Potential for possible misuse.
For example, if there are more than 50 registers, the draft law links the tax ID as
additional order feature. In this way data could be about
the population register with data from the register of insured persons of the health
kassen and the register for supplementary help with subsistence or
compared to the list of debtors and a personality profile
be summarized. The technical ones provided for in the draft law
and organizational safeguards are not sufficient to create such a profile
to prevent effectively. These ensure that only authorized

Authorities transmit the required data end-to-end encrypted.
However, they do not offer sufficient protection against the abusive
merging the data on one person from different

registers, not even in the case of data leaks. In addition, it is closed

reckon that the new ID no. also widespread in economic life

will be found, further increasing the risk of abuse.

The data protection conference, on the other hand, had “sector-specific”

key figures are required, which are data protection-compliant and at the same time practical

net because, on the one hand, they clearly imply a one-sided state comparison

make it more difficult and, on the other hand, clearly identify a natural person.

Although such a model in the Republic of Austria for many years

successfully practiced, the federal government has never seriously

weighed and without convincing justification with the blanket reference

rejected on "legal, technical and organizational complexity".

Even if the corona pandemic shows how necessary it is to accelerate

of digitization, this must not be used as an argument for

constitutionally necessary amendments with reference to the

To let “urgent needs” fall under the table.

The data protection conference therefore points out again that the dem

Draft law underlying architecture contradicts constitutional

legal regulations. She is therefore calling on the federal government to do so

to submit a draft that meets the constitutional requirements

suffices before they can be decided by the Federal Constitutional Court

is obliged to do so.

1.8

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

04/16/2020

Police 2020 - see risks, seize opportunities!

With the police program decided by the conference of interior ministers

In 2020 there is an opportunity to eliminate previous data protection deficits

and to improve data protection in the long term. The police authorities

in the federal and state governments have a first "technical development plan" for

presented the Police 2020 program. This names data protection

as one of the core goals. The conference of independent data protection

Federal and state supervisory authorities expressly welcome this. She

but misses sufficient proposals on how the project protects data protection

wants to strengthen. The conference therefore calls for the goals and milestones of the

Align the program with core data protection requirements

and to involve the data protection supervisory authority in this process.

From the point of view of the data protection authorities, the following goals are the priority

to take a look:

1. Comprehensive inventory

So far, a project analysis has only included questions of technical feasibility.

In particular, it did not use the results of the numerous data protection

legal controls and consultations over the last few years. This

must be made up for in an independent evaluation.

2. Legal guidelines

With the new “data house” in Police 2020, the security authorities are creating

a technical basis for comprehensive computer-aided analyses

personal data. These interfere intensively with fundamental rights and

are therefore to be limited legally and technically. you only on Gene-

ral clauses, the fundamental right to informational self-determination

not fair. The responsible bodies must comply with the law and

constitutionally implied red lines. This is mandatory

needed before budget funds are used on a large scale.

3. Separation of Purpose

If the security authorities process personal data,

always have a specific purpose. This is the core of the

data protection law. Therefore, the new system must be precise between the

various processing purposes task fulfillment, documentation

and separate care. In particular, for a specific task or

Data stored for documentation is not generally included in a data store

transferred or used as an evaluation and research platform.

4. Improving data quality

If the police authorities reorganize the IT structure, they all have to

Take advantage of opportunities: You have to clean up existing databases,

separate necessary data and ensure the quality of the data. This is also valid,

when old data is transferred to the new systems. data protection con-

trolls have shown that this is necessary. Example is the case file

Drug.

5. Privacy Specific Basic Services

The Police 2020 program offers the opportunity to develop new basic technical

to implement data protection functionalities as “basic services”.

Necessary are e.g. B. a “basic service purpose separation”, a “basic service

Data Quality” and a “Basic Supervision and Control Service”.

1.9

Resolution of the Conference of Independents

Federal and state data protection supervisory authorities –

04/03/2020

Data protection principles in dealing with the corona pandemic

The corona pandemic is one of the greatest tests for the

European societies for decades. All member states of the

European Union are currently facing extreme challenges

cope with to ensure the health of their population. offered

In view of the measures already taken, the value of the

Freedom rights can be experienced, including the fundamental right to informational

belongs to self-determination.

In this situation, it is essential for the stability of state and society

bar that the citizens can rely on the fact that

Freedom rights such as the basic right to informational self-determination only

be restricted to the extent and for as long as is absolutely necessary and

is appropriate to effectively protect public health.

Drastic regulations must be reversible and strictly limited in time and

are the responsibility of the legislature and not solely of the executive.

As for the justification of the processing of personal data

In accordance with the European General Data Protection Regulation

particularly in its Article 5, it contains uniform principles throughout Europe

ready to serve as a guide for government action, especially in times of crisis

can serve to effectively combat the corona pandemic

and at the same time deal with them in a way that protects fundamental rights

ensure personal data.

In connection with overcoming the Corona crisis, the conference
the independent data protection supervisory authorities of the federal and state governments
therefore on the following essential legality requirements for
the processing of personal data:

– Times of crisis do not change the fact that the processing of personal
The data obtained must always be based on a legal basis.

This requires, in particular, that the persons pursued with processing
purposes are specified as precisely as possible.

– The planned measures must also be critically assessed for their suitability
be checked to record infections, infected people
treat or prevent new infections. This is how it can be in emergency situations
for example, be a suitable measure to aid organizations
oblige medically trained personnel to attend the health
to report to the competent authorities. However, exist
considerable doubts as to the suitability of measures taken solely with
individual routes of infection with the help of telecommunications traffic data
should understand.

– The planned measures must be necessary. standing too
suitable measures to achieve the purpose are available, which
niger, or – like a previous anonymization – not even in the
human rights intervene, these must be implemented as a matter of priority
become. In addition, the processing of personal data may not
– how the preventive surveillance of the entire population without exception
tion - are disproportionate to the intended legitimate purpose.

It follows that particularly strong freedom-restricting measures

must also be linked to special conditions - for example

to the formal determination of a health emergency, such as may arise after the

Infection protection legislation has already been implemented in some countries.

- For the proportionate design of the processing of sensitive

After all, it belongs to the data that the

Pandemic measures designed to be reversible in the sense

that they can be withdrawn after the end of the crisis

and, if they are then disproportionate, even have to. So are

personal data no longer required for the stated purposes

delete data immediately. In general, all measures should

be limited. This applies in particular to such legal ones

Measures that are particularly relevant to the fundamental rights of those affected

intervene.

– Health data are among the most sensitive data because their

Last but not least, use for the persons concerned special risks

can justify in their social environment. The European

Data protection law therefore requires suitable guarantees to protect the

affected persons. Technical and organizational measures for

Protecting the integrity and confidentiality of health data

are not only required by law, but also necessary in order to

prevent misuse of data and errors in

to counteract the processing. It is also important in terms of

Data protection principle of transparency the data subjects in

to inform them in an understandable way about the processing of their data.

Data protection principles offer sufficient protection, especially in times of crisis

Design options for legally compliant processing of personal

related data. Your observance contributes to the preservation of the

freedom in a democratic society.

194

Appendix to I

2. Selected decisions of the Conference of Independent

Federal and state data protection supervisory authorities

2.1

Decision of the Conference of Independents

Federal and state data protection supervisory authorities –

11/26/2020

Telemetry functions and data protection when using Windows

10 enterprises

At the 98th Conference of Independent Data Protection Authorities of the

Federal and state governments (DSK) developed a test scheme for data protection

decided to use Windows 10 and then published

light.1 This is intended to enable those responsible to check compliance with the

data protection regulations when using Windows 10 are made easier

become. A working group of the DSK, with the participation of LDA Bayern,

BfDI, LfDI Mecklenburg-West Pomerania and LfD Lower Saxony since then

Examination of Windows 10 with regard to the telemetry level security,

which is available in the Enterprise edition.

Regardless of this, a laboratory study by the working group has proved this

In addition to the LfD Bayern as a guest, BSI itself was involved in an extensive

Study (SiSyPHuS study) also with questions of the Windows 10 tele

metric function busy.

Research results of the DSK working group

The working group used the telemetry of Windows 10 in a laboratory study

carried out to determine whether the telemetry data transmission

can be prevented by configuration. Microsoft has

authorities declares that when using the telemetry level Security

no telemetry data2 are transmitted.

It was Windows 10 Enterprise version 1909 in three test scenarios

examined. In all three scenarios, user activities were simulated to

achieve realistic results.

1 https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.

pdf

2 For the term, see the report Windows 10 telemetry test with user interaction (An-

position 1)

1. Application of the "Windows Restricted Traffic Limited Functionality Base-

line", telemetry level "Security", 72 hour test period

2. Application of the "Windows Restricted Traffic Limited Functionality Base"

line", telemetry level "Basic", 30-minute test period

3. No application of the “Windows Restricted Traffic Limited Functionality

Baseline, Security telemetry level, 72 hour test period

The details of the examination can be found in the laboratory report (Annex 1).

become men.

The investigation has confirmed that in the second test scenario, the transmission

development of telemetry data could be determined. In the third scenario

made a connection call to the settings-win.data.microsoft.com endpoint

established. According to Microsoft, this endpoint is used by several

Windows 10 system components, also from the telemetry component,

driven. If the telemetry component uses this endpoint, the

Possibility of downloading configuration data,

caused by the changes in the behavior of the telemetry service

could. Microsoft has responded to this call to the data protection supervisory

authorities based on a laboratory scenario provided by Microsoft

explains and explains this with another system component apart from the

telemetry. Upon verbal request to the data

safety authorities stated that despite a - possibly due to

a software error - unintentional call to the settings-win.data.

microsoft.com endpoint from the telemetry service at a telemetry level

"Security" still no telemetry data transmission would take place.

Research results of the BSI

In an investigation supplementing the laboratory test of the working group,

Windows 10 Enterprise data traffic through the BSI in January 2020

the data transfers to "settings-win.data.microsoft.com".

(see Appendix 2).

A Windows 10 Enterprise system version 1803 with telemetry

level Security and "Windows Restricted Traffic Limited Functionality Baseline"

used. However, it should be noted that the connections to "settings-win.

data.microsoft.com" could not be analyzed in plain text and thus

there is a possibility that Microsoft will exfiltrate data through this channel

or influences the system in an undesired way. Before this

The BSI maintains the background based on a defense-in-depth approach

Strengthening the security of the federal IT systems at the need

a network separation of Windows 10 clients of the federal administration, too

to protect against malicious code.

According to Microsoft, the endpoint "settings-win.data.microsoft.com"

also the configuration of the Windows component “User Experiences

and Telemetry in Connected Mode” updated dynamically.3 Also in

BSI project "SiSyPHuS" is this address several times in connection with

called the dynamic configuration of Windows telemetry.4

As a result of the findings, Microsoft could use the behavior of the

Customize the telemetry service, configure the type and scope of data collection

or execute commands to enrich the data without

the user must agree to this or can control this. Before this

The background is connections to this endpoint after the assessment

classified by the BSI as at least questionable.

Consequences for those responsible

The published test scheme explains that those responsible

Evidence of the legality of any transfers of personal

ner provide data to Microsoft or the transmission of personal

have to prevent data.

To prevent the transmission of personal telemetry data

When using the Enterprise Edition, those responsible have the

metric level security and by means of contractual, technical or

organizational measures (e.g. by filtering internet access

of Windows 10 systems via an appropriate infrastructure)

deliver that demonstrably no transmission of telemetry data to

Microsoft takes place.

In view of any other open questions that e.g. B. by calling the "set

tings-win.data.microsoft.com" data connection or the

also raises the BSI's SiSyPHuS study, such as the fact that the

available investigations based on ongoing developments

software of course only represent a snapshot, the up-to-

previous investigations responsible not conclusively from their

Art. 5 Para. 2 DS-GVO deriving obligation to test and provide evidence for

data protection-compliant use of Windows 10 with regard to transmission

relieved of telemetry data. This is especially true for those responsible

3 https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints

4 https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Work-

package4_Telemetry.pdf

Use Windows 10 in the Pro and Home editions, in which the telemetry

level cannot currently be set to Security. In these cases stay

other measures to prevent any transmissions anyway

to check personal telemetry data or the legality of the

proof of transmission.

Therefore, Windows 10 in all editions offered should have the option

offer to disable telemetry data processing by configuration.

For this and for the laboratory tests of the DSK and the SiSyPHus

The remaining imponderables identified in the BSI study will

Data protection supervisory authorities lead the further discussion with Microsoft.

198

Appendix to I

WWiinnddoowwss 1100 TTeelleemmeettrriiee--PPrrüuffuunngg mmiitt NUuttzzeerriinntteerraakkttiioonn

Responsible implementation

for testing and documentation:

LfD Lower Saxony,

Unit 3 - IT Laboratory

06/17/2020

05/14/2020

Test completion date:

finalization and release

the documentation:

1 Objective of the test

Microsoft states that no telemetry data is transmitted to Microsoft if the

Windows 10 Enterprise operating system and the one provided by Microsoft

"Windows Restricted Traffic Limited Functionality Baseline" (V1903)1 has been installed.

At the end of last year, a telemetry test without user interaction was carried out on Windows 10

Enterprise System (by the Lower Saxony State Commissioner for Data Protection (LfD Nieder-

Saxony) and the Bavarian State Office for Data Protection Supervision (BayLDA)).

This test found that the tele-

metric data can be deactivated when using the Enterprise Version in the checked scenario.2

Since telemetry data may only be transmitted when there is user activity, this aspect should now be included in

are taken into account in the present test.

For this purpose, the data transmissions that occur are logged (Wireshark3 protocols).

It is then examined whether the logs contain connections to the Microsoft

specified endpoints (“Telemetry Connections”).

DDiieessee EEnnddppuunnkkttee wweerrddeenn vvoonn MMiiccrroossooffttt wwiiee ffoollggtt aannggeeggeebbeenn44::

1 Windows Restricted Traffic Limited Functionality Baseline: https://docs.microsoft.com/de-de/windows/pri-

vacy/manage-connections-from-windows-operating-system-components-to-microsoft-services, download link:

https://go.microsoft.com/fwlink/?linkid=828887, downloaded 1/8/2020

2 See the 9th activity report of the BayLDA 2019: https://www.lda.bayern.de/media/baylda_report_09.pdf, page 22

3 https://www.wireshark.org/

4 https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization

THE STATE COMMISSIONER FOR DATA PROTECTION LOWER SAXONY -

WINDOWS 10 ENTERPRISE TELEMETRY TEST WITH SIMULATED USER INTERACTION

199

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

WWiinnddoowwss--VVeerrssiioonn

EEnddppuunnkktt

DDiiaaggnnoosseeddaatteenn:: v10c.vortex-win.data.microsoft.com

Ffuunnkkttiioonnaall:: v20.vortex-win.data.microsoft.com

Windows 10 version 1703 or

higher, with installed cumulative

tive update 2018-09

Windows 10 version 1803 or

higher, without cumulative 2018-

09 update installed

Windows 10 version 1709 or

earlier

MMiiccrroossooffttt DDeeffeennddeerr AAddvvaanncceedd TThhrreeaatt PPrrootteeccttiioonn is country specific; the

prefix changes by country,

e.g.: ddee.vortex-win.data.microsoft.com

EEiinnsstteellllluunnggeenn:: settings-win.data.microsoft.com

DDiiaaggnnoosseeddaatteenn:: v10.events.data.microsoft.com

Ffuunnkkttiioonnaall:: v20.vortex-win.data.microsoft.com

MMiiccrroossooffttt DDeeffeennddeerr AAddvvaanncceedd TThhrreeaatt PPrrootteeccttiioonn is country specific; the

prefix changes by country,

e.g.: ddee.vortex-win.data.microsoft.com

EEiinnsstteellllluunnggeenn:: settings-win.data.microsoft.com

DDiiaaggnnoosseeddaatteenn:: v10.vortex-win.data.microsoft.com

Ffuunnkkttiioonnaall:: v20.vortex-win.data.microsoft.com

MMiiccrroossooffttt DDeeffeennddeerr AAddvvaanncceedd TThhrreeaatt PPrrootteeccttiioonn is country specific; the

prefix changes by country,

e.g.: ddee.vortex-win.data.microsoft.com

EEiinnsstteellllluunnggeenn:: settings-win.data.microsoft.com

Connections to other Microsoft services, such as B. Windows Update Services, Windows

Activation services or certificate services can also be used in the Wireshark protocol.

but do not constitute "telemetry connections" as defined for this test.

It is therefore important to find out whether there are connections in the Wireshark protocol to the in the table

listed Microsoft endpoints.

The test includes three different test scenarios:

Appendix to I

PPrrüüffsszzeennaarriioo 11 ((WWiinnddoowwss RReessttrriicctteedd TTrraaffffiicc LLiimmiitteedd FFuunnccttiioonnaalliittyy

BBaasseelliinnee,, TTeelleemmeettrriieelleevveell == 00))::

•

Installation of the "Windows Restricted Traffic Limited Functionality Baseline". Through this

among other things, the telemetry level of the system is set to "0".

• 72 hours operation of a Windows 10 Enterprise system, with Microsoft installed

"Windows Restricted Traffic Limited Functionality Baseline" (V1903) and various

partially automated user activities (with system-related programs

men, each according to a schedule) within the 72 hours of the test.

• Recording of the network traffic that occurred.

• Evaluation of the Wireshark protocol for the presence of connections to relevant

ten Microsoft endpoints (see above).

PPrrüüffsszzeennaarriioo 22 ((WWiinnddoowwss RReessttrriicctteedd TTrraaffffiicc LLiimmiitteedd FFuunnccttiioonnaalliittyy

BBaasseelliinnee,, TTeelleemmeettrriieelleevveell == 11))::

According to Microsoft, the actual suppression of the telemetry data transfer

setting the telemetry level to "0" is sufficient.

Test scenario 2 is intended to check whether a telemetry level greater than "0"

Find network connections to the endpoints named by Microsoft in the logs

the are.

The telemetry level can be changed with the following registry entries:

• HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection

• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows

\CurrentVersion\Policies\DataCollection

• HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\System

\AllowTelemetry

The parameter "AllowTelemetry" or "Value" found there

(in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default

\System\AllowTelemetry)

represents the intensity of the Microsoft-side telemetry data with the possible values 0-3

transmission:

• 0 = "security" = No telemetry data collection and transmission until

• 3 = "full" = Complete telemetry data collection and transmission

Note: the telemetry level "0" can be used in the Windows Home and Pro versions of

Windows 10 not be set.

THE STATE COMMISSIONER FOR DATA PROTECTION LOWER SAXONY -

WINDOWS 10 ENTERPRISE TELEMETRY TEST WITH SIMULATED USER INTERACTION

201

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

The test setup in test scenario 2 is therefore only in one point (cete-

ris paribus) as follows:

• The parameter value "AllowTelemetry" (or "Value") is entered manually in the available

Available registry variables are set to "1" (= "simple" or "basic").

Duration of the test: 30 minutes.

•

o The shortened running time is justified by the fact that it is to be expected that in tele-

metric level 1 already after a short time connections to the above table

specified endpoints (especially to v10.events.data.microsoft.com)

take place.

o The following user activities on the Windows 10 system are recorded in the 30 test

utes carried out:

▪ Insert any USB stick.

▪ Create a Notepad file.

▪ Saving the file on the USB stick.

▪ Start the browser manually and call up the website www.rki.de with

subsequent call-up of three links on the same website.

▪ Close the browser.

▪ Start of the Invoke User Simulator (automated web browsing).

PPrrüüffsszzeennaarriioo 33 ((SSttaannddaarrdd--WWiinnddoowwss--IInnssttaalllllaattiioonn,, TTeelleemmeettrriieelleevveell

== 00))::

The Microsoft "Windows Restricted Traffic Limited Functionality" installed in test scenarios 1 and 2

nality Baseline" not only prevents telemetry traffic. There will also be many

soft uninstalls the "additional products" that are installed by default. As a result, the network

Connections to Microsoft systems significantly reduced.

In some cases, however, a person responsible would like to use these “additional functionalities”.

It would therefore be relevant for the person responsible to know whether the suppression of the telemetry

Data transmission is only possible by setting the telemetry level to "0", without that

Install “Windows Restricted Traffic Limited Functionality Baseline” and thus others

(possibly required in the corporate environment) to use Microsoft services that are provided by the installa-

tion of the package would not be available.

To check this, the following test is carried out:

Standard installation of Windows 10 Enterprise.

•

• Manually setting the system's telemetry level to "0".

•

• Recording of the network traffic that occurred.

•

72 hours user activities on Windows 10 system, according to schedule.

Evaluation of the Wireshark protocol for the existence of connections to relevant ones

Microsoft endpoints (see above).

Appendix to I

2 Description of the laboratory setup

Graphical representation of the laboratory setup

The following hardware components and configurations are used:

Notebook Lenovo type 20KE-S9020

KKoonnffiigguurraattiioonn::

• Windows 10 Enterprise V1909.

Workgroup installation without connection to a domain.

• All Microsoft updates available at the time of the test are installed.

• Microsoft “Windows Restricted Traffic Limited Functionality Baseline” (V1903)

•

•

will be installed (test scenario 1 and 2).

Command line: ipconfig /flushdns is run before running each check scenario

executed.

Beyond that, no further changes will be made to Windows 10

Enterprise system made.

• The system is restarted before each test.

Notebook Fujitsu type E734 with operating system Debian 10

KKoonnffiigguurraattiioonn::

• Use of the integrated ETH NW interface as a connection to the Fritz!Box.

•

IP address (192.168.178.x range) is sent from the Fritz!Box to the de-

bian notebook distributed.

An additionally connected USB network card serves as a network interface

go to the Windows 10 Enterprise Notebook.

•

• The Debian notebook acts as a router by using the LINUX service dns-

masq for the Windows 10 Enterprise test notebook.

• DHCP router service runs on Debian Notebook and assigns IP (in the address range

192.168.250.x) to the Windows 10 Enterprise Notebook.

Fritz!Box 7590

• Serves as a network router for the Debian Notebook with V-DSL connection to

Internet.

• The DNS cache of the Fritz!Box is emptied before each test scenario.

3 Description of the test procedure

The test simulates 72 hours of operation of the Windows 10 Enterprise notebook.

At different time intervals (which are recorded in a table to the minute),

manual activities on the Windows 10 Enterprise Notebook with different software

components as well as browser activities controlled by a script in order to

to simulate the activities.

A subcomponent of an automatically running PowerShell script is used for this.

The script called "Invoke-UserSimulator" was created to automate the simulation of

processes running on the PC. It is freely available via Github5.

Only the web browsing function of the script is used in this test.

The following user actions are performed:

Automated web browsing

The GitHub tool "Invoke-UserSimulator" automatically starts the browser and "clicks" scripted

controls automatically at certain, fixed intervals, randomly based on predetermined links

(i.e. also entered in the script) websites in order to then (again randomly controlled)

ert) to continue browsing.

In order to carry out the number of IP address requests to be expected in the Wireshark evaluation protocol

not to increase the automated web browsing unnecessarily (and thus the evaluation of the wire

shark protocol more difficult), only one website was selected for the test and

automatically "surfed" by the tool.

The following website was selected and used for automated browsing because this

Website does not connect to other host addresses (IP addresses) when started:

https://www.rki.de.

During the course of the test, the (random) call-up of further websites must also be

are calculated, which can be reached from the source website.

5 https://github.com/ubeeri/Invoke-UserSimulator

THE STATE COMMISSIONER FOR DATA PROTECTION LOWER SAXONY -

WINDOWS 10 ENTERPRISE TELEMETRY TEST WITH SIMULATED USER INTERACTION

204

Appendix to I

Manually performed activities on the test system during the 72 hours

Testing

In addition to automated web browsing, after a predetermined (and for

subsequent facilitation of the evaluation recorded in an Excel table) schedule over 72 hours

the following activities were carried out manually on the system:

• Create, save, modify and copy Notepad file.

•

•

• Copy and replace files multiple times from and to a connected USB stick.

Control Panel → Event Viewer "System" Randomly select and view events.

Create, save, modify and copy Paint file (drawing).

HHiinnwweeiiss::

No third-party products or parts of the Microsoft Office package were intentionally installed

and used for the simulation, since further telemetry traffic to the software

manufacturer can be assumed.

4 Evaluation of the Wireshark logs

The recorded Wireshark log of the test scenario is searched using plain text

("character string") for the presence of the strings

•

•

•

•

v10c (.vortex-win.data.microsoft.com)

v10. (events.data.microsoft.com)

v20 (.vortex-win.data.microsoft.com)

settings-win.data.microsoft.com

searched.

According to Microsoft, the expected contact with the endpoints is determined by DNS queries.

be marked (which are only resolved outside of the laboratory system or the Internet),

because Microsoft is constantly changing the IP addresses behind these connections.

In the Wireshark protocol, it is therefore only possible to find the above addresses (in plain text)

decisive.

5 test result

Test scenario 1

In the test period of 72 hours, with regular user activity on the system

(incl. web browsing) no connections to the addresses mentioned in chapter 4 were found

become.

A transmission of telemetry data did not take place in this scenario.

Test scenario 2

In the test period of only 30 minutes, with regular user activity on the system

system (incl. web browsing) already have connections to v10.events.data.microsoft.com and connections

Connections to settings-win.data.microsoft.com can be found. These connections could

even be detected in an additional 30 minutes test without any user activity

the.

A transmission of telemetry data thus took place as expected.

Test scenario 3

In the test period of 72 hours, with user activity, on the system (including web

Browsing) only connections to settings-win.data.microsoft.com are detected.

A transmission of telemetry data, in particular diagnostic data transmitted to v10

th, has therefore not taken place.

6 Conclusion

These tests could not refute Microsoft's statements that in

no telemetry data is transmitted with the configuration described above. From here

however, the conclusion cannot be drawn that telemetry data transmission is fundamentally

additionally does not take place. Therefore, those responsible are always obliged to check whether the

set of Windows 10 also in your individual system and processing situation

legally permissible.

Special attention should be paid to connections to settings-win.data.microsoft.com,

since there is a possibility that configuration data will be downloaded via this connection

that may cause changes in the behavior of the telemetry service.

The State Commissioner for Data Protection Lower Saxony

Prinzenstrasse 5

30159 Hanover

Telephone 0511 120-4500

fax

0511 120-4599

Email poststelle@lfd.niedersachsen.de

Page 8 of 8

THE STATE COMMISSIONER FOR DATA PROTECTION LOWER SAXONY -

WINDOWS 10 ENTERPRISE TELEMETRY TEST WITH SIMULATED USER INTERACTION

206

Appendix to I

Federal Office for Security in Information Technology

PO Box 20 03 63, 53133 Bonn

Distributor:

Federal Commissioner for Data Protection and Freedom of Information

Unit 23

Bavarian State Office for Data Protection Supervision

Head of Cyber Security and Technical Data Protection

The State Commissioner for Data Protection Lower Saxony

Unit 3

Subject: Windows 10 Enterprise traffic scan

Reference: Windows 10 exam at BayLDA on December 10th/11th, 2019

Business reference: TK 12 – 240 05 00

Date:

page 1 of 10

01/28/2020

Ladies and Gentlemen

Robert Krause

Federal Office for Security in

of information technology

Godesberger Allee 185-189

53175 Bonn

POSTAL ADDRESS

P.O. Box 20 03 63

53133 Bonn

TELEPHONE +49 228 99 9582 5697

FAX +49 228 9910 9582 5697

referat-tk12@bsi.bund.de

https://www.bsi.bund.de

the German federal and state data protection supervisory authorities are dealing with the

Question whether and under what configuration options the operating system Windows 10 from

Responsible in Germany can be used. Particular attention is paid to this

on the so-called telemetry data that Windows 10 automatically transmits to Microsoft.

On December 10/11, 2019, the Bavarian State Office for Data Protection Supervision held a discussion on this topic

a meeting of representatives of the authorities with Microsoft for a technical exchange took place

which the BSI also took part from an IT security perspective. The aim was to make a statement

to find out whether Windows 10 Enterprise can be operated in compliance with data protection regulations. in one

Test setup should also be proven that no unwanted data,

in particular no telemetry data, are no longer transmitted to Microsoft.

The result was that no data was sent to Microsoft in the observed period

were transferred, where there is a particular data protection or IT risk

to go out. Due to the fact that in the experimental setup there was no user interaction and more

technical framework conditions (e.g. domain membership and updates) are reproduced

could be made, the interest was expressed to shed light on these partial aspects again.

The BSI did this in its own test setup with a view to IT security aspects

explained below and the results presented.

experimental setup

Over an investigation period of 72 hours, the following systems were tested in virtual

machines operated:

• Routers (Debian 10)

 Use as a router, DHCP server, DNS server

 Using tcpdump to record network traffic

 Use for live display of data connections

• Windows 10 Server 2019

 Use as a domain controller, DNS server, WSUS server

 Deploying Group Policy to use a WSUS server

 Provision of updates for Windows 10 SAC 1803

• Windows 10 Enterprise (SAC 1803)

 Use as a workstation

 Application of the Windows Restricted Traffic Limited Functionality Baseline1 for

Windows 10 SAC 1803

 Domain Member

 Obtaining updates from the domain's WSUS server

 Using Fiddler and procmon for local system monitoring

 Deactivation of the certificate pinning by setting the key

"SkipMicrosoftRootCertCheck" in HKLM/SOFTWARE/Microsoft/Windows/

CurrentVersion/Diagnostics/DiagTrack/TestHooks on DWORD 0x1

 Simulation of user and system behavior

• Regular check for updates and their installation

• Regular reboots

•

•

System load and crash simulation (via Sysinternal Suite)

Starting and using programs (without Internet functions), e.g. Wordpad,

Notepad, Powershell, system commands

• De- and installation of additional programs, reconfiguration of the settings via

GUI

1

https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-

components-to-microsoft-services

208

Appendix to I

Page 3 of 10

The network diagram looks like this:

209

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

Page 4 of 10

Result

In the entire study period, 2741 packets (1,919,128 bytes) passed the network via the

router out to the internet. The following end points are addressed in detail

been:

These will now be considered separately.

50.56.19.116 – fiddler2.com – 1.6MB / 1931 packages

This IP was retrieved each time the "Fiddler2" application was started and is used for the

Checking and getting updates. It is a connection that

is not attributable to Microsoft Windows and can therefore be ignored in this investigation

remain.

23.210.254.117 – store-images.s-microsoft.com – 27KB / 119 packages

Connections to the image archive of the Microsoft Store are closed throughout the period

register.

More specifically, it involves downloading images, including from the application

Office Sway, which is a presentation web application. reason for that is

presumably, the application as a shortcut in the dynamic Windows start menu

to be able to offer.

210

Appendix to I

In addition to the image data, the following information is transmitted as part of the data connection

been.

This connection is unexpected because all connections were assumed to be

to the Microsoft Store by applying the Windows Restricted Traffic Limited Functionality

Baseline are suppressed or disabled.

Nevertheless, the transmitted data does not give rise to any risk or disclosure

to see more trustworthy information.

52.155.217.156 - displaycatalog.mp.microsoft.com - 126 KB / 123 packages

In connection with checking for updates, connections to the

Domain "displaycatalog.mp.microsoft.com" which is the basis for the previously

mentioned retrieval of the image data from "store-images.s-microsoft.com".

211

The header data of the connection is as follows:

In response, the client received information about products offered by Microsoft; For this

Office Sway in JSON encoded form.

Among other things, the links to the icons called up in the image archive of the Microsoft Store are also included

find.

212

Appendix to I

Even if this connection is undesirable and i.R. of Windows Restricted Traffic Limited

Functionality Baseline should not occur due to the little data available from the client

itself sends and the content of the received data does not pose a threat.

.microsoft.com

23.210.253.93 - crl

– 2 KB / 12 packages

This is a connection to the Certificate Revocation List (CRL) at Microsoft,

to check if certificates have been suspended or revoked. This connection could

be observed only once during the investigation period, namely after the initial start of the

Application "procmon". This program is signed with a certificate to the real time

to prove. In this context, Windows has apparently contacted the CRL.

The screenshot below shows the properties of the connection.

Here, too, the transmitted data do not give rise to any risk or disclosure

to see more trustworthy information.

213

2.22.119.98 / 2.22.119.33 / 2.22.89.31 / 2.22.94.250 / 2.19.241.220

*.deploy.static.akameitechnologies.com - 45 KB / 212 packages

These IP addresses and domains are a Content Delivery Network (CDN)

by Akamei, which is used to deliver and accelerate online applications. This

Endpoints represent aliases corresponding to other endpoints already analyzed here.

2.22.119.98 → crl.microsoft.com

2.22.119.33 → crl.microsoft.com

2.22.94.250 → store-images.microsoft.com

2.22.89.31 → store-images.microsoft.com

2.19.241.220 → store-images.microsoft.com

40.74.35.71 - settings-win.data.microsoft.com - 124 KB / 344 packages

This connection is regularly checked by the system - prior to checking for Windows

Updates - made.

What was striking about this connection was that initially it was only on the router and not in the local

Proxy could be observed. The proxy server configured via GUI / Fiddler in Windows

was not used. Rather, it was necessary to carry out further configuration via the

execute the command "netsh winhttp set proxy".

Subsequently, the establishment of the connection could be observed in Fiddler, the

However, the connection itself no longer transmitted any user data, which indicates the use of

indicates certificate pinning by Microsoft.

There were no further attempts to access the unencrypted data traffic

undertaken. No statement can therefore be made about the content of this connection.

According to Microsoft, apps would use these endpoints to manage their configuration

update dynamically. For example, the Windows component "User Experiences and

Connected Mode Telemetry and Windows Insider Program affected.

In the BSI project "SiSyPHuS"3, this domain is also used several times in connection with the

dynamic configuration of Windows telemetry. As a result of the findings

Microsoft could use this to adjust the behavior of the telemetry service, the type and scope of the

Configure data collection or execute data enrichment commands without

2

3

https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints

https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf

214

Appendix to I

Page 9 of 10

that the user must agree to this or can control this. Against this background

Connections to this endpoint should at least be classified as questionable.

Upon request, this was confirmed verbally in a conversation with Microsoft on December 10th/11th, 2019 in Ansbach

that the data transmitted in these connections after application of the Windows

Restricted Traffic Limited Functionality Baseline (and thus the telemetry level "Security") of

the Windows telemetry component would no longer be used and retrieving

solely have technical causes in the implementation.

What this data connection actually transmits and whether it is security or

configurations relevant to data protection can be made to the system, in the absence of

Traffic insight, not rated.

Evaluation

Within the scope of this investigation, there were no indications that Windows 10

Enterprise with Windows Restricted Traffic Limited Functionality Baseline configuration

has transferred data to Microsoft originating from h.S. a risk or disclosure

represent trustworthy information. In particular, no transmission of

Telemetry data to Microsoft are observed.

However, it should be noted that the connections to "settings-win.data.microsoft.com" are not

could be analyzed in plain text and therefore there is the possibility that Microsoft via

exfiltrates data from this channel or influences the system in an undesired way.

Furthermore, this investigation provides only a snapshot for an explicit version

of Windows 10 Enterprise in this patch level and a special configuration

further updates and changes to the system by Microsoft or user configurations

this behavior can change. Regularly updating and checking the

Investigation results is therefore required.

Despite the knowledge gained, the BSI's recommendation that Windows 10 be implemented as part of a

mains separation to operate maintained. The reason for this is, on the one hand, the possibility that

the detected system behavior at any time through updates or configuration changes of the

manufacturer can change. In particular, the non-assessability of the dynamic

Configuration of the telemetry involved connection to "settings-win.data.microsoft.com" shows,

that no reliable, final statement is possible and further data communication

can occur. On the other hand, with the network separation of a system, the principle “Defence

in depth”. So not only possibly occurring, undesired

Data transfers from applications on the system prevented, but also effective

the exfiltration of data e.g. by malware can be prevented.

However, application of the Windows Restricted Traffic Limited Functionality Baseline

for Windows 10 Enterprise a significantly reduced amount of data going to the Internet

be transmitted. A similar configuration option for Windows 10 Pro/Home

would be desirable.

However, in accordance with the designation of the guideline, there is a reduced

functionality to be noted. For example, as part of the investigation

no more applications can be started that are related to the Windows Store. The

Effects on the practicability of this guideline will be based on the test results

however, rated as rather low.

On behalf

dr wobbly

216

Appendix to I

2.2

Decision of the Conference of Independents

Federal and state data protection supervisory authorities –

09/22/2020

Application of the GDPR to data processing by parliaments

On the occasion of the judgment of the ECJ of July 9, 2020 (C-272/19), the

conclusion of the data protection conference on September 5, 2018 “Application

of the GDPR in the area of parliaments, parliamentary groups, members of parliament and

Political Parties” suspended pending reformulation of a decision.

2.3

Decision of the Conference of Independents

Federal and state data protection supervisory authorities –

09/10/2020

Use of thermal imaging cameras or electronic ones

Temperature recording in the context of the corona pandemic

I. STARTING POINT

Since a SARS-CoV-2 infection is sometimes associated with a specifically increased body temperature of the infected person, electrical

ronic devices for temperature measurement as a means of access control

previously used in publicly accessible rooms or workplaces.

A non-contact temperature measurement is usually carried out by infrared

measurement and is either using a clinical thermometer or a

Thermal camera / infrared thermal imaging camera1. In the now

envisaged scenarios for access to airports, shops, authorities,

workplaces, etc., the use of thermal imaging cameras in

taken into account, since no temperature can be

temperature can be measured for larger groups. You can only for

the measurement of individuals sequentially, such as B. in isolation

lock, are used, with a single fever measurement

using a thermometer without logging depending on the application scenario

Applicability of the General Data Protection Regulation (EU) 2016/679 (GDPR)

can be in question. retail companies and government agencies

1 If in the following only the use of thermal imaging cameras or the electronic

Temperature measurement is discussed, the explanations relate in principle

always on both types of processing.

already comparable heat measurements to gain access to their

regulate business premises.

SCOPE OF THE DECISION

The resolution concerns the use of thermal imaging cameras or

tronic temperature recording for control or on the occasion of

Access to airports, shops, government offices and workplaces in the

context of the corona pandemic. facilities in the field of

health care including nursing can be special

subject to action.

II. SUMMARY

For electronic measurement of body temperature for general regulation

access to airports, shops, authorities and workplaces

Art. 6 Para. 1 Subparagraph 1 Letter e, Art. 9 Para. V. m. § 3

BDSG and comparable regulations in the state data protection laws

(performance of a task in the public interest) or

Article 6 paragraph 1 subparagraph 1 letter f, Article 9 paragraph 2 GDPR (pursuit of a

legitimate interest) as a legal basis. Also

is the measurement as an operational measure of occupational safety or for

Assessment of ability to work based on Art. 88 GDPR i. V. m. § 26 para.

3 BDSG (or the personal data protection law of the respective country) or

§ 22 paragraph 1 no. 1 letter b BDSG i. In conjunction with Art. 9 (2) GDPR in principle

conceivable. However, it is missing i. i.e. R. the suitability and necessity of the

Measurement. Because an increased body temperature cannot necessarily

be considered symptomatic of SARS-CoV-2 infection and

many infected people have no symptoms and therefore no increased temperature

temperature up. In addition, milder measures such as B. Compliance with

Hygiene and distance regulations and the event-related survey

of employees by the employer conceivable.

III. PRIVACY ASSESSMENT

The electronic measurement of body temperature falls - at least typically -

wise – within the scope of the General Data Protection Regulation

(EU) 2016/679 (GDPR).

Measuring a person's body temperature constitutes a processing

personal data within the meaning of Art. 4 No. 1 and No. 2 DSGVO.

Does a responsible person have body temperature measurements taken on persons

take, this regularly affects personal data.

218

Appendix to I

Although the temperature measurements themselves do not yet record a clearly identical

tifying information such as the names and addresses of the persons who

pass the corresponding measuring device. Typically, however, the

affected person can be otherwise identified, for example by personal

nal, which makes the measurements and possibly records, by the

Use of video cameras or time recording devices. other

res could apply at most if an automated temperature measurement

takes place, which is completely without logging and without anything else

The values are assigned to specific or identifiable persons.

In connection with the corona pandemic, such a measurement would

however, fail to achieve their preventive purpose.

As a rule, they are carried out using an automated temperature measurement

The data generated is personal data within the meaning of Art. 4 No. 1

GDPR. Especially supports the storage of infrared camera recordings

a subsequent personal identification of data subjects. Becomes

thermal imaging even with conventional video surveillance

linked, is generally excluded from a personal reference to the image recordings

(cf. BVerwG, judgment of March 27th, 2019, Az. 6 C 2/18, paragraph 43 of the

justification for the decision).

The application of the General Data Protection Regulation is based on Art. 2 Para. 1

GDPR continues to require either automated processing

or non-automated processing of personal data takes place,

that are or are to be stored in a file system.

Example: The acquisition of body temperature using a thermal imaging

camera systems is an automated processing of personal data

Data within the meaning of Art. 4 No. 2 DSGVO - regardless of whether the

recordings are saved or whether live monitoring is carried out (cf.

BVerwG, judgment of March 27, 2019, a. a. O., Paragraph 43 of the Decision

Reason).

Based on the described operating conditions of the electronic

cal temperature detection are based on the following explanations

the applicability of the General Data Protection Regulation. She

however, do not refer to such temperature measurements, for

which the scope of the General Data Protection Regulation

is not open by way of example.

219

Since the electronic temperature measurement is aimed at people

identify those who are infected with SARS-CoV-2, it is a

processing of health data within the meaning of Art. 4 No. 15 GDPR. So far

such processing of personal health data takes place,

it is strictly forbidden according to Art. 9 Para. 1 GDPR. This basic

The additional prohibition on processing does not apply if the processing

fulfills an exception of Art. 9 Para. 2 DSGVO.

Therefore, in the following, depending on the application, the

legal bases are examined in more detail, starting with the general ones

Processing Powers.

In addition to the basic processing ban and the exceptions

Article 9 GDPR stipulates that processing

personal data according to Art. 5 Para. 1 Letter a, Art. 6 Para. 1

Subparagraph 1 GDPR is only lawful if it refers to at least one

Legal basis within the meaning of Art. 6 Para. 1 GDPR

can. This is usually not the case with electronic temperature measurement

given. The following considerations should be noted in this regard:

– Consent within the meaning of Article 6 Paragraph 1 Subparagraph 1 Letter a GDPR

can only be effectively granted if the requirements of Art. 4

No. 11, Art. 7 DSGVO are fulfilled (for details see data protection con-

ferenz, Brief Paper No. 20, Consent according to the GDPR; European

Data Protection Committee, WP 259 rev. 01: Guidance in relation to the

approval according to regulation EU 2016/679). In addition, it should be noted that

the heat measurement just to detect a possible illness

serves; therefore, the data subject has given their express consent

to explain (cf. Art. 9 para. 2 letter a DSGVO).

In connection with the objective of access regulation using

Thermal imaging measurements will be based on consent as the basis for processing

from a practical point of view, because it is the voluntary

the declaration of consent is missing. In addition, the effectiveness of

consent often also fail because transparent information

mation of the person concerned before carrying out the measurement process

seems doubtful in practice.

Example: Numerous employment relationships are strong of one

Imbalance between employees and their employer

employer (Recital 43 GDPR). In front of this background

For this reason, employees hardly ever get a job established by their manager

can refuse access control if they are asked to go to their

want long. Other exceptions may apply if employers

or employers, for example with the help of company or service agreements

the framework conditions for the voluntariness of a declaration of consent

set by employees.

Example: Access control for government or court buildings

typically cannot be based on consent if the

affected persons a statutory state benefit

want to claim or even to official or judicial

request access to the respective building. Because so far

the voluntariness of consent is always doubtful and can

are regularly not proven to those responsible (cf. Art. 7 Para. 1,

Recital 43 GDPR).

Example: Regarding access to a company's business premises

is the obtaining of a here according to Art. 9 para. 2 letter a GDPR

the legally required express consent of the customer

out of the question for pragmatic reasons. In addition, the

Voluntariness also depends on the circumstances of the individual case, with the
legal assessment of Art. 7 Para. 4 GDPR must be observed.2 As far as
access to the business premises depends on the consent to the temperature measurement
sung is linked, can therefore not be assumed to be voluntary
to be run out.

- Also Art. 6 Para. 1 Subparagraph 1 Letter b GDPR separates as legal
basis as a rule. In the case of access controls, the temperature
tower measurement not to fulfill an existing contractual relationship
between the parties.

– The contract is most likely to be used as the basis for processing in the case of employees
employment relationships in the non-public sector and in collective bargaining
public sector employees. In this respect, Art. 9
Para. 2 letter b GDPR under the conditions specified there
etc. an exception to the processing ban of Art. 9 Para. 1 GDPR
before, as far as the person responsible or the person concerned from
must comply with the obligation under labor law. Regarding the
electronic temperature measurement for employees comes at best
considering that with her the employer or employer from the
Occupational health and safety law wants to fulfill the following obligations.

2 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, para. 14

However, such contractual authority to measure temperature can
go no further than a legal obligation on the part of the controller
within the meaning of Article 6 Paragraph 1 Subparagraph 1 Letter c GDPR.

– In some cases, when measuring the temperature, companies refer to

it is necessary to fulfill a legal obligation within the meaning of Art. 6

Paragraph 1 subparagraph 1 letter c GDPR. This provision provides

itself does not constitute a legal basis for processing, but sets in accordance with

Article 6 paragraph 2, paragraph 3 subparagraph 1 GDPR a legal basis in the area

specific EU law or the law of a Member State. The

The obligation standardized in this provision must relate directly to the

processing of personal data. Just the fact

that a person responsible in order to fulfill any legal obligation

being able to process personal data is sufficient

not enough (cf. e.g. LSG Hessen, decision of 29.01.2020,

Az. L 4 SO 154/19 B, paragraph 13 of the reasons for the decision).

Such a legal obligation for companies to

Tower measurement is not expressly provided for in German law. In

Employment relationships are subject to Section 3 (1) of the Occupational Health and Safety Act

the employer in general to take the necessary measures of the

Occupational health and safety "to be taken taking into account the circumstances which

affect the safety and health of employees at work".

Furthermore, according to Section 618 of the Civil Code, the employer is

additionally obliged to take measures to protect life and health

to seize on its employees. From these general legal

However, specifications for occupational health protection can be precisely

not a concrete legal obligation within the meaning of Article 6 (1) subparagraph 1

letter c GDPR, access to the company premises with the help of

to regulate an electronic temperature measurement.

Also taking into account the April 16, 2020 by the Federal Ministry

Ministry for Labor and Social Affairs published "Occupational Safety Standard

SARS-CoV-2" or the other area and industry-specific

Occupational health and safety standards result in nothing else. Regardless of,

that temperature measurements are considered as an operational measure

should be pulled (II. No. 13 of the occupational safety standard SARS

CoV-2: “particularly fever, cough and shortness of breath … signs of a

Infection with the corona virus (can be). There is one in operation for this purpose

to provide for contactless fever measurement if possible."), do not justify any

legal obligation of the employer or principal within the meaning of

Article 6 paragraph 1 subparagraph 1 letter c GDPR, by means of temperature measurement

to process personal data. Because the occupational safety

dars SARS-CoV-2 are not a legal sentence from which a legal

Obligation follows, but a kind of guideline of the public administration

for occupational safety.

There is currently no specific legal obligation

for persons responsible within the meaning of Article 6 Paragraph 1 Subparagraph 1 Letter

c GDPR to carry out electronic fever measurements.

– Article 6 paragraph 1 subparagraph 1 letter d GDPR permits the processing

personal data when it is required for vital purposes

Interests of the data subject or another natural person

protect son. When processing personal data in the room

related health data through electronic temperature measurement

However, pursuant to Art. 9 (2) (c) GDPR, the data subject must

Person for physical or legal reasons be unable to their

To give consent to the processing, so that this legal basis

cannot be used.

– On the other hand, in individual cases it is possible that the temperature measurement

solution for the perception of a public interest

Task that has been assigned to the person responsible is required.

Article 6 paragraph 1 subparagraph 1 letter e GDPR itself does not constitute any

authorization to work, but according to Art. 6 Para. 2 and 3 Subparagraph 1

DSGVO a legal basis. Such processing basis

can in principle also consist of a general clause; in particular

EU law does not require it, as is the case with processing for

Fulfillment of a legal obligation, specifically the purpose of processing

contain. According to Article 6 Paragraph 3 Subparagraph 2 GDPR, it is sufficient if the

Purpose of processing is necessary to fulfill a task,

which is in the public interest or in the exercise of public authority

he follows. This presupposes, after all, that such a task is legal

of the Member State is described in such a clear and specific way that it

a permissible processing purpose can be derived with legal certainty.

In particular, the statutory rules of responsibility and tasks

not be undermined by processing rules that are too vague.

It follows that the processing for reasons of public inter-

esses in the field of public health pursuant to Art. 9 Para. 2 Book

stabe i GDPR, § 22 para. 1 no. 1 letter c Federal Data Protection Act

(BDSG) no general authorization of authorities for processing

based on health data. These regulations relate to

rem wording and the history of its origin to the public

health care and health administration.

However, if the temperature measurement is used for general access

to buildings of public administration, is lacking

area-specific regulations, recourse to the data protection law

General clauses in § 3 BDSG and comparable regulations in

the national data protection laws. would be the starting point

insofar as the task of every public body to

ßen - that also means for visitors and employees

to ensure the safest possible service operation. Additionally must

a processing authority with regard to Art. 9 Para. 2 DS-

GMO specially protected health data are available (e.g., insofar as

applicable, Section 22 Paragraph 1 No. 1 Letter d BDSG). It is regular

the principle of necessity to be taken into account, based on which to

check whether the fever measurement is actually necessary and expedient

is to achieve the purpose. For checking the necessity

To create concepts that describe the intended measures and the associated

the purposes pursued in a conclusive and comprehensible manner. Additionally

the authorities have the special rules to protect sensitive

data to consider. The suitability and necessity of an electronic

niche fever measurement, however, there are considerable doubts; this

are explained below in connection with the comments on Art. 6

Paragraph 1 subparagraph 1 letter f GDPR discussed in more detail.

The control of access to public sales areas of companies

on the other hand, Article 6 Paragraph 1 Subparagraph 1 cannot be taken as a rule

Letter e GDPR in connection with the respective member state

support norm of authority. companies and other non-public

Responsible persons can only invoke this provision if they

a processing authority in the public interest or as an exercise

is "transferred" to public authority. You must instead of an authority

take action, which requires some kind of state transfer

required act. In other words, individuals can

do not declare yourself to be the guardian of a public interest. For this reason

the performance of a public task within the meaning of Art.

6 paragraph 1 subparagraph 1 letter e GDPR for non-public responsible

currently used as a reason for processing (cf. BVerwG, judgment of

03/27/2019, a. a. O., paragraph 46 of the decision).

– For companies and other non-public bodies, however, stands

Article 6 paragraph 1 subparagraph 1 letter f GDPR available, which - shortened

expressed - processing on the basis of an interest

weighing is permitted if it is used to protect legitimate interests

is necessary and does not outweigh the interests of the data subject

gen. Public sector officials can register under

do not base their task fulfillment on this processing basis,

See Article 6 Paragraph 1 Subparagraph 2 GDPR.

224

Appendix to I

In connection with the electronic fever measurement is again

to note that as processing of personal health

data can only be admissible if an exception to the basic

Processing is prohibited according to Art. 9 Para. 2 GDPR. Such

However, exceptions are only conceivable in exceptional cases.

The processing basis of Article 6 Paragraph 1 Subparagraph 1 Letter f

According to established case law, the GDPR requires three test steps

(cf. inter alia ECJ, judgment of 04.05.2017, Az. C-13/16, paragraph 28 of the

reasons for divorce):

First, the processing must be based on a legitimate interest that

by the controller or by the person(s).

is perceived by third parties, secondly, the processing of personal

personal data for the realization of the legitimate interest

be necessary and thirdly, the interests, fundamental rights and

Fundamental freedoms of the data subject not the processing interest

of the person responsible prevail.

A legitimate processing interest is to be affirmed in the present case,

as far as the survey associated with the electronic fever measurement

of data to ward off threats to the workforce or the

other customers and thus also the maintenance of the business

should serve operationally.

The necessity of the measure, on the other hand, is regularly not too

affirm. As far as the publication of the data protection conference "Data

protection law information on the processing of personal

nal data by employers and employers in connection with

of the corona pandemic" in this respect for determining the necessity

generalizable indicates that - taking into account the

principle of proportionality - the "collection and processing of personal

sun-related data (including health data) of guests

and visitors could be legitimate, in particular to determine whether

they are infected themselves or in contact with someone who has been proven to be infected

Person stood or was in a place defined by the RKI as

area classified as a risk area", this is limited

to the permitted data processing in the immediate context of using

health hazards associated with the pandemic. before this

The background to this are surveys and further measures

not generally ruled out, but is an element of the offense

the necessity in the specific processing context

observe.

When checking the necessity, it should be noted that an increased physical

temperature is not necessarily symptomatic of a SARS-CoV-2

infection can be viewed. It can also be

other causes, such as colds, metabolic and vascular diseases

effects, rheumatism, inflammatory processes. In addition, wise

According to the Robert Koch Institute (RKI), only about 41 percent of the

Infected have a disease course with fever; in the up to 14 days

The infected persons do not yet have a comprehensive incubation period

Symptoms appear or remain complete throughout the course of infection

dig symptom-free, but are potential carriers due to the viral load

(cf. https://www.rki.de/DE/Content/InfAZ/N/Neuartigs_Coronavirus/Profile.

html#doc13776792bodyText2, status: 06/12/2020).

Notwithstanding that fever is generally symptomatic of a

SARS-CoV-2 infection can be a temperature measurement with the

Aim of protecting employees, customers or visitors

a predominant number of symptom-free carriers of infection at most as

conditionally suitable. The RKI therefore advises in its epidemic

miological Bulletin 20/2020 from May 14th, 2020 from the use

corresponding devices at airports, since no added value is seen

(https://www.rki.de/DE/Content/Infekt/EpidBull/Archiv/2020/Quellen/20_20.

pdf?__blob=publicationFile).

In this context, the test is therefore of particular importance

ment whether milder, less intrusive measures to achieve

of the purpose pursued, the protection of employees and customers who

serve as it were to achieve the purpose. given

which are the usual measures in retail, such as the

Limiting the number of customers, attaching information signs

Rules of conduct and access restrictions, ensuring the

Compliance with minimum distances, the request to wear one

face masks, the installation of partitions in the checkout area and

at sales counters and the implementation of hygiene requirements

to call. Such a package of measures also promises

in view of the greater risk of virus exposure due to no

established symptom-free infected a more sustainable protection of

Customers and employees as an intrusive camera-assisted

collection of health data.

As a result, a need for electronic

Fever measurement as an instrument for access control to public

chen sales and traffic areas, especially in the area of

Basic services as well as for areas whose use is for daily

are indispensable for life (e.g. train stations, airports, buildings of

administrative authorities) cannot be affirmed.

226

Appendix to I

When measuring fever as an operational measure of the work

protection, it should be noted that their legal admissibility due to the

Specification clause of Art. 88 GDPR based on § 26 BDSG

judge is. For employees in the public sector of the countries

the personal data protection law of the respective country applies; on

however, this will not be discussed further below. With regard

the necessity must be taken into account that the person responsible as

Employer or employer the determination of an increased body temperature

temperature can combine with subsequent investigations, what the

Suitability of the measure slightly increased. Nonetheless, with regard to

the need to consider that symptom-free cases of infection

cannot be detected by electronic temperature measurement

can. Apart from that, there would be – depending on the question and on a case-by-case basis

- as a milder measure, the possibility of health

Impaired ability to work to ask if this is because of

Nature of the activity to be performed or the conditions of its performance

is an essential and crucial professional requirement.

According to this, the question of the state of health of a

nes employees permitted if the employment is unreasonable

making potential downtime or limitations of activity

exist or are to be expected. Furthermore, may generally after

Presence of contagious diseases asked colleagues

or could endanger customers.

If, despite the above concerns, the necessity is affirmed

as well as the non-predominance of the interests worthy of protection

affected persons, it must be checked whether the basic processing

Prohibition of Art. 9 Para. 1 GDPR does not prevent fever measurement.

According to the hints already given, in this respect comes present

an exception to the processing ban only according to Art. 9 Para. 2

Letter h GDPR in connection with Section 22 Paragraph 1 No. 1 Letter b or

26 Para. 3 BDSG into consideration. After that, processing is personal

withdrawn health data is not prohibited when used for assessment

of ability to work is required. The documentation should

key principles, including purpose limitation, data minimization

and memory limitation, follow. In addition, the fulfillment of the requirements specified in Art. 9

Paragraph 3 DSGVO, § 22 paragraph 1 number 1 letter b) BDSG mentioned

Conditions and guarantees provided. In other words, one should

Electronic fever measurement only by a company medical service

be made. This should be given to the employer or employer

if necessary, inform which employees have access to the company premises

has been denied.

227

In the field of occupational health protection, the

Participation rights of interest groups must be observed.

The permissible use of electronic temperature measuring devices depends

finally, overall, from the fulfillment of further data protection regulations

specifications, e.g. B. are the regulations on the register of processing

activities, for data protection impact assessment and for information

Art. 12 ff. GDPR (signage) to be observed.

The person responsible must also ensure that the specifications

of data protection through technology design from Art. 25 GDPR and

of data security according to Art. 32 GDPR. Here can

For example, the following aspects play a role:

– Suitable body parts for measurement: A meaningful recording

a complete thermal image of a person is hardly possible, since e.g. B.

clothing can alter infrared radiation. Usually will

therefore measured at the forehead or the inner corners of the eyes. There are

This means that special cameras are required that automatically detect these areas

and can target.

– Measurement accuracy: Classic non-contact forehead thermometers often have

larger deviations. Therefore, depending on the context of use,

Systems are used that have a significantly higher measurement accuracy

have than conventional contactless clinical thermometers for home use

offer.

– Falsification of the measurement: In addition, it must be taken into account that

in addition to other illnesses, physical activity (sports, haste),

Ambient conditions etc. to measurement differences or deviations

can contribute.

– Absolute / relative measurement: There is both the approach, one

to define a threshold value from which the thermal imaging camera detects positively,

as well as the measurement and alerting compared to the surrounding ones

perform people. In the first case, the

Difficulty determining the relevant fever threshold

to the extent that body temperature fluctuates throughout the day and also

can be different in children and adults.

– Error rate: Due to the technical difficulties of the measurement

can it also be independent of the problem that infected people have not yet

show ne symptoms to "false positive" as well as "false negative"

Results come, for example, depending on the determination of the

threshold values and the installation situation.

228

Appendix to I

– Resolution, image accuracy: Many thermal imaging cameras offer a very

high resolution, so that the question arises as to which additional

information can thus be seen, especially if a real image of the

facial is captured in high resolution (detection of other diseases,

biometric identification etc.).

– Automatic measurement / human operator: Because of the effort

for the measurement it can be assumed that this is not fully automated

can take place, but at least monitored by human personnel

must become. In addition, in the case of a positive detection, as a rule

human intervention required to filter out the affected person

and take further action.

2.4

Decision of the Conference of Independents

Federal and state data protection supervisory authorities –

05/12/2020

Regarding preliminary objections to StreetView and comparable services

For publishing street views, including partial

Images of house facades and private property areas

adjoin the public street space, can be used within the framework of street

View and similar services Art. 6 Para. 1 Subparagraph 1 lit. f GDPR as

legal basis to consider. Only the personal

Genetic data are published that are mandatory for the achievement of the purpose

required are; so are characteristics that identify a person

enable, in particular faces and license plates, to be unrecognizable

make. This already results from Art. 5 Para. 1 lit. c DS-GVO (principle

of data minimization). In addition, the provider before the start of the recordings

inform the public in an appropriate manner.

As part of the balancing of interests, a request from data subjects

to obliterate personal data.

This request can be made at least from the time the

Recordings are perceived through the service and also includes

Images of house facades and private property areas. kind

21 GDPR remains unaffected.

The request for redacting according to Art. 17 Para. 1 DS-GVO and

the objection according to Art. 21 DS-GVO must be both online and

can be submitted by post.

These rights must be expressly referred to.

Federal and state data protection supervisory authorities –

05/12/2020

Notes on the use of Google Analytics in the non-public Area

Google Analytics is one of the most widely used tools for website operators about (user). With the help of this tool, comprehensive statistical Carry out evaluations of website usage. For this reason there is a great need for advice regarding the use of Google Analytics.

Against the background of the new Legal framework with the validity of the DS-GVO the use of Google Analytics newly rated. Older views of the data protection supervisory authorities Communicated before May 25, 2018, taking into account the legal situation were considered obsolete.1

The following is by no means a final assessment.

The following explanations are a supplement to the orientation guide for providers of telemedia2 and only affect the most common ones Questions when using Google Analytics. The following tours do not constitute a recommendation for the use of Google Analytics, but only describe the minimum requirements under data protection law s which are currently mandatory for site operators to comply with Need to become.

The views of the data protection supervisory authorities are under the Subject to a future – possibly different – interpretation by the European Data Protection Board and case law of the ECJ.

The statements apply in the event that the user of Google Ana-

lytics uses the default settings currently3 recommended by Google. For

in the event that the user of Google Analytics from the recommended

Settings differs and/or additional functions are used (e.g.

Google Analytics 360) or Google the processing or the contractual

fundamentals changes, will be based on the German data protection supervisory

1 This applies in particular to the publication of the Hamburg Commissioner for Data

data protection and freedom of information, "Notes for website operators based in Hamburg,

who use Google Analytics".

2 Available at: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.

pdf

3 Status: 03/11/2020

Appendix to I

Authorities published versions of the guidance for providers

referred by telemedia.

I. Personal data

When using Google Analytics, personal data is always collected

the user processes.

In the Google Analytics Help Center4, Google explains that usage data is not

"personally identifiable information". This view does not stand

only contrary to the definition of the term "personal data"

in Art. 4 No. 1 of the GDPR, but is also misleading, since Google in

Further executes the following:

"Please note that data that Google does not consider personally identifiable

re classifies information as personal within the framework of the DS-GVO

data may apply."

The data protection supervisory authorities therefore expressly point out that
that the data processed with Google Analytics (usage
data and other device-specific data that a specific user
can be assigned) to personal data i. s.d. GDPR
acts.

II. Relationship between Google Analytics users and Google

Google has the processing processes of Google Analytics on an ongoing basis
adjusted. This has meant that Google Analytics is no longer just
is a tool for statistical analysis (reach measurement), but that
offers the user a large number of additional functions with which the
user can pursue different purposes.

In the opinion of the data protection supervisory authorities, the processing in
No order processing in connection with Google Analytics
Art. 28 GDPR. According to Art. 4 No. 7, Art. 28 Para. 10 DS-GVO, the
responsible to determine the purposes and means of processing themselves.
From this follows the obligation of the processor to process the data exclusively
to process on the instructions of the person responsible (Art. 29 DS-GVO). At the
The website operator does not determine the use of Google Analytics alone
about the purposes and means of data processing. Rather, these will
partly specified exclusively by Google, so that Google in this respect
himself is responsible and contractually accepted by the site operator. The

4 Available at the URL: https://support.google.com/analytics/answer/7686480 [status:
09/27/2019].

Processing when using Google Analytics provides a uniform

Facts of life, in which the various aspects of processing

only make sense as a whole. As a result, those involved

within a processing activity not their role as processor

and/or person responsible can change.

Although Google continues to offer a contract for order processing,

but additionally in the "Google Measurement Controller-Controller Data Pro-

tection Terms"5 clear that for certain processing processes Google and

the user (website operator) are separately responsible. In addition

Google's terms of use6 make it clear that Google uses the data for its own

Purposes, in particular also for the purpose of providing his web analytics

analysis and tracking service. According to article 28 paragraph 10 GDPR

Google is no longer a processor.

Taking into account the current case law of the ECJ, Google

and the Google Analytics user together for data processing

responsible, so that the requirements of Art. 26 DS-GVO must be observed

are.

III. legal basis

As a rule, the use of Google Analytics cannot be based on Art. 6 Para. 1

lit. b DS-GVO are supported, since the use of Google Analytics is not

is required to fulfill the contract between the website operator and the user.

The use of Google Analytics is also generally not permitted under Art. 6

Paragraph 1 lit. f GDPR lawful. In view of the specific data processing

steps when using Google Analytics outweigh the interests

Fundamental rights and freedoms of users regularly protect the interests of

website operator. In particular, the user does not reasonably calculate

so that his personal data with the aim of creating

personal advertising and linking to those from others

related personal data to third parties

given and comprehensively evaluated.7 This goes far beyond that

5 The "Google Measurement Controller-Controller Data Protection Terms", available at:

https://support.google.com/analytics/answer/9012600, version of November 4, 2019,

Clause 4 applies, among other things in the event that Google products and services in the settings for

Data sharing is enabled.

6 Available at: https://marketingplatform.google.com/about/analytics/terms/de/, version

dated June 17, 2019, Nos. 6, 7.

7 Google privacy policy at: https://policies.google.com/privacy, version

effective October 15, 2019, under the heading "Measurement of Performance."

beyond what is permitted under Art. 6 (1) lit. f GDPR.8 The

In this respect, the situation deviates considerably from the case of a statistical function

your own website or by means of order processing.

In the contractual regulations, Google obliges the user of

Google Analytics, under certain conditions for the use of the

Service to obtain consent from visitors to the website.9 The

Data protection supervisory authorities expressly point out that it is

the lawful use of Google Analytics does not affect the contractual

Agreements between Google and the user matter. The right-

moderation is governed solely by the law.

The result is a lawful use of Google Analytics as a rule

only on the basis of an effective consent of the website visitor acc.

Art. 6 (1) lit. a, Art. 7 GDPR possible.

IV. Measures

If website operators do not use alternative and data-saving tools

dodge to measure range, but continue to use Google Analytics

use, the following measures in particular must be implemented:

1) Obtaining informed, voluntary, active and prior consent

ligation of the users

A consent is only effective if the requirements according to Art. 4 No. 11,

Art. 7 GDPR and, if applicable, Art. 8 GDPR are fulfilled. This means in particular:

– Website operators must ensure that the consent is specific

Processing activity through the integration of Google Analytics and

associated transmissions of usage behavior to Google

LLC recorded.

– The consent must clearly state that the

Data processing is essentially carried out by Google, the data is not

are anonymous, which data is processed and that Google accepts them

8 More detailed explanations in the "Orientation aid for providers of telemedia".

9 See “Terms of Use”, available at: https://marketingplatform.google.com/

about/analytics/terms/de/, version dated June 17, 2019; “Policy Requirements for

Google Analytics Advertising Features”, available at: https://support.google.com/analytics/

answer/2700409, version 16 December 2016; “User Consent Policy

in the EU”, available at: https://www.google.com/about/company/user-consentpolicy.html,

undated, last accessed 23 January 2020.

any own purposes such as profiling and with others

Linked to data such as any Google accounts. A mere hint

such as B. "This site uses cookies to improve your browsing experience"

sern" or "uses cookies for web analysis and advertising measures"

is not sufficient but misleading because of the associated

Processing is not made transparent.

– Users must actively consent, i. H. approval must not be assumed

and preset without user intervention. An opt-out procedure

is not sufficient, rather the user must, through active action (e.g. clicking

of a button) to express their consent. Google must

are expressly listed as recipients of the data. before an active

ven consent of the user may not collect any data or elements

downloaded from Google websites. Even the mere use of one

Website (or an app) does not constitute effective consent.

– Consent is only voluntary if the data subject chooses

opportunities and a free choice. You must give consent as well

can refuse without suffering any disadvantages. The coupling

a contractual service to the consent to a for the

Data processing that is not required for the performance of the contract can be carried out in accordance with

Art. 7 para. 4 DS-GVO means that the consent is not voluntary

and is therefore ineffective.

To meet the requirements for effective consent on websites or in

To implement apps, the following design guidelines must be observed:

– Clear, not misleading headline – mere “shows of respect”

regarding privacy are not sufficient. It is recommended to

documents in which the scope of the decision is discussed,

such as "Data processing of your user data by Google".

– Links must be clearly and unambiguously described –

essential elements/contents in particular of a data protection declaration

must not be obscured by links.

– The object of the consent must be made clear:

Users of Google Analytics must make it clear for which

Purpose Google Analytics is used that the usage data from

Google LLC are processed, this data is stored in the USA

both Google and state authorities have access to them

have data, this data with other data of the user such as

such as search history, personal accounts, usage data

other devices and any other data that Google has about that user

exist, be linked.

234

Appendix to I

– Access to the imprint and the data protection declaration is permitted

cannot be prevented or restricted.

2) Technical requirements for the implementation of the withdrawal of consent

ligation

When using Google Analytics, a simple and always

accessible mechanism (e.g. button) to revoke the once dated

be implemented with the consent given by the user. The same goes for apps that

ask for consent at the beginning of use. Also here must in the

settings an easily accessible possibility for an effective revocation

of consent.

Once a user has given his consent and he revokes it

a later date, it must be ensured that after the revocation

the Google Analytics script is not loaded or executed.

Google provides a browser add-on to disable Google Analytics

available. It is not permitted to restrict the user solely to this

to refer to the add-on, as this is not a sufficient possibility of revocation

represents. According to Art. 7 Para. 3 S. 4 DS-GVO the revocation is as easy as

to design the granting of consent. That available from Google

The add-on provided does not meet these requirements because the user

Downloading more programs is forced. Incidentally

speaks the AddOn due to the variety of browsers and operating systems

neither the state of the art nor is it suitable for data processing

to prevent in apps.

3) Transparency

According to Art. 13 DS-GVO, users must enter the data protection

comprehensive provisions on the processing of personal data

informed within the framework of Google Analytics. Regarding the requirements

this information obligation is based on the guideline on transparency10 of the

European Data Protection Board and the guidance

for providers of telemedia.

10 Available at: https://www.datenschutzkonferenz-online.de/media/wp/20180411_wp260_

rev01.docx

4) IP address truncation

In addition to the above Measures should users of Google Analytics

cause the shortening of the IP addresses through appropriate settings

senior This is on every website with a Google Analytics integration

add the "_anonymizeIp()" function to the tracking code. Further

Details can be found in the technical instructions from Google,

available at: https://developers.google.com/analytics/devguides/collection/

gtagjs/ip-anonymization.

The shortening of the IP address represents an additional measure in accordance with Art.

25 Para. 1 DS-GVO to protect users, but it does not lead to

that the complete data processing takes place anonymously. When deployed

Google Analytics collects further usage data in addition to the IP address

ten collected, which are to be evaluated as personal data, such as e.g. B.

Identifiers of each user, which is also a link

for example with an existing Google account. From the-

For this reason, the scope of the GDPR is opened in any case,

so that users of Google Analytics are also obliged to

The requirements of the GDPR must be observed if they reduce the IP

addresses have prompted. The data protection declaration states that

whether the shortening of the IP addresses is required to be indicated accordingly.

Otherwise, the statements in the orientation guide for providers apply

from telemedia.

2.6

Decision of the Conference of Independents

Federal and state data protection supervisory authorities –

04/15/2020

To the consent documents of the medical informatics initiative

of the Federal Ministry of Education and Research

From the point of view of the conference of independent federal data protection authorities

and the federal states are against the nationwide use of the consent

documents of the medical informatics initiative in version 1.6b, existing

from patient information and a declaration of consent as well as the

associated manual in version 0.9b no concerns under the

Condition that in the consent documents to the processing

genetic data from biomaterials and in particular the associated

the risk of traceability is explicitly pointed out, the preservation

the right of withdrawal at any time despite the transfer of ownership

Biomaterials is expressed more clearly and patients on the opportunity

be advised to register with an e-mail distribution list that

in good time before the start of new research projects based on the data

of the medical informatics initiative. Also in the handout

to delete the passage in which it is pointed out that in future the

Data transmission to third countries should be permitted.

In order to implement these requirements in patient information,

beaten:

– Insert under 3.2 in the first paragraph after sentence 2: “In biomaterials can

Your genetic material may be contained in the form of genetic data. In this respect are

in particular the risks for genetic data described under 1.4

observe. This also includes an increased risk of traceability

your person based on this data.”

– Insert under 3.3 in the first paragraph after sentence 2: “Your right to have the

It remains to determine the processing of your personal data yourself

unaffected by the transfer of ownership. Despite transfer of ownership

you can revoke your consent to data processing at any time

(see point 6) and request the destruction of your biomaterials.”

- In addition, in the consent and in the patient information

at a suitable point for the possibility of registering with one

e-mail distribution list, which will be informed in good time before the start of new

research projects based on data from the medical informatics initiative

informed.

In addition, in the declaration of consent in the box under 3.3 as

second sentence should be included: "My right to object to the processing of my

personal data to be extracted from the biomaterial

determine remains unaffected by the transfer of ownership (see point 3.3

the patient information)."

As an editorial correction, it is also recommended that in the consent

explanation under 1.1 on the keyword of the coding also on point 1.3 of the

refer to patient information as the coding is described there.

237

Appendix to I

3. Selected guidance from the Conference of

independent federal data protection supervisory authorities

and the countries

3.1

Orientation guide of the working group “Technical and

organizational data protection issues” – March 13, 2020

Measures to protect personal data at

Submission by email11

1. Objective

This orientation guide shows which requirements are to be met by the

Procedures for sending and receiving e-mail messages

by controllers, their processors and public email services

Provider12 are to be fulfilled on the transport route. address these requirements

in accordance with the requirements of Art. 5 (1) lit. f, 25 and 32 (1) GDPR.

The guidance takes the state of the art to publication

point in time as a starting point for specifying the requirements.

Controllers and processors13 are required by law to reduce the risks

resulting from their processing of personal data, sufficient

to reduce. You must do so by nature, scope, circumstances and purposes

their processing as well as the different probability of occurrence and

seriousness of the risks to the rights and freedoms of natural persons

consider. This guidance only addresses the risks

those with a breach of confidentiality and integrity of personal

data are connected. It assumes that those responsible or their

Processors will assess what damages result from a breach of

confidentiality and integrity can result.

The orientation aid is based on typical processing situations. She

determines the typical implementation based on the state of the art

mentation costs and their relation to the risks of transmission

personal data by e-mail requirements for the measures,

the responsible persons and processors for sufficient reduction

11 The guidance was developed by the Conference of Independent Data Protection Supervisors

supervisory authorities of the federal and state governments decided against Bavaria's vote.

12 Service providers who provide their own or third-party e-mail services for public use

hold.

13 processors exclusively with regard to their obligations under Art. 32 DS-GVO.

of risks to take. The controllers and processors

are obliged to explain the specifics of their processing, including in particular

separate the scope, circumstances and purposes of the intended

to take into account transmission processes that may occur in deviating

claims can result. In doing so, they must take into account that

This guide only considers risks that

arise on the transport route. Risks faced by data at rest as already

received e-mails are suspended or through further processing

such as B. automatic forwarding arise, are in this orientation

ment assistance is not considered and may take further action or another

make it necessary to weight the measures listed below.

Cannot meet the requirements for secure transmission by e-mail

are met, another communication channel must be selected.14

2. Scope and Principles

The legally required protection of personal data in the course of the

The transmission of e-mail messages extends to both personal

ment-related content as well as the circumstances of the communication, insofar as

can be derived from the latter information about natural persons.15

Beyond the scope of this guidance, this protection must

be supplemented by measures to protect the systems involved and

to minimize, limit storage and earmark the on these

Servers processed traffic data.

This guide focuses on protecting the confidentiality of personal

related content of the e-mail messages only insofar as these are not

in advance (e.g. application-specific) according to the state of the art

encrypted in such a way that only the recipient can decrypt them.

Both end-to-end encryption and transport encryption

reduce risks for confidentiality for their respective application

quality of the transmitted messages. Therefore, those responsible must both

Consider procedures when considering the necessary measures.

14 For communication with affected natural persons (e.g. with customers), a

Communication channel consist in the provision of a web portal.

15 Information about the circumstances of the communication can be processed in various

processing processes involved in sending and receiving e-mail messages

connected (from retrieving information from DNS to logging the

communication on different devices). This guide only addresses the issue

the protection of the information contained in the headers of an e-mail message during

the transport of the message.

240

Appendix to I

The most thorough protection of the confidentiality of the content data is provided by

End-to-end encryption achieved for what is currently the Internet standard

S/MIME (RFC 5751) and OpenPGP (RFC 4880) i. i.e. R. in connection with

PGP/MIME (RFC 3156) are available. end-to-end closures-

lung not only protects the transport route, but also data at rest. At

End-to-end encryption allows unencrypted processing

Content data on specially protected network segments or on such parts

of the network are restricted, exclusively for use by authorized persons

(such as a human resources department or a medical officer) are provided.

The use of transport encryption offers basic protection and

represents a minimum measure to meet the legal requirements.

In processing situations with normal risks, this is already done

the transport encryption achieves a sufficient risk reduction.

Transport encryption passively reduces the probability of success

Interception measures by third parties on the transport route to a minor extent.

In order to be able to withstand third parties who actively intervene in network traffic,

it must be carried out in a qualified manner and through measures to

cryptographic protection of the recipients' information about the

Receipt of the messages authorized devices are flanked.

A description of the requirements for the simple and for the qualified

mandatory transport encryption and end-to-end encryption

Encryption and signing of e-mail messages is described in Section 5

laid down.

3. The use of email service providers

3.1 Basic technical requirements for the provision of

email services

To protect the confidentiality and integrity of the processed personal

data must be public e-mail service provider's requirements

the TR 03108-1 of the Federal Office for Security in Information Technology

(BSI) comply.

This means that they are obligated to comply with the

linie laid down requirements for a protected reception of

Creating messages and sending messages related to

the application of cryptographic algorithms and the verification of the

Authenticity and authorization of the remote station under the given

Conditions on the recipient side best possible with proportionate

must achieve protection that can be achieved by means of means.

241

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

3.2 Due diligence when using email service providers

Controllers using public email service providers

must be satisfied that the providers have sufficient guarantees

for compliance with the requirements of the GDPR and in particular the

mentioned Technical Guideline. This also includes the safe

Connection of own systems and end devices to the service provider.

In addition, those responsible must carefully assess the risks

zens associated with breaching the confidentiality and integrity of email messages

directed, which they send or receive in a targeted manner. In from-

The following risks may depend on these risks

additional requirements arise, the fulfillment of which they issue instructions

to the service provider (e.g. by making suitable configuration

settings, insofar as such are offered by the service provider)

have to enforce.

4. Case Groups

4.1 Targeted receipt of personal data in the content

of email messages

Persons responsible who specifically receive personal data by e-mail

men, e.g. B. by explicitly agreeing to exchange personal data

Data by e-mail or the request on the homepage, personal

The ones described below have the right to transmit data by e-mail

to fulfill obligations.

4.1.1 Obligations for normal risks16

Protection of confidentiality and integrity of personal data

in the transmission of e-mail messages requires that sender and

receivers work together. The responsibility for the individual

the transmitter is responsible for the averaging process. However, who specifically personal

accepting data by e-mail is obliged to meet the requirements for

secure receipt of e-mail messages via an encrypted

create channel. This means that the receiving server has at least the

Establishment of TLS connections (directly via SMTPS or after receiving a

STARTTLS command via SMTP) and only

16 For the classification of risks, see brief paper no. 18 of the independent data protection

federal and state authorities “Risk to the rights and freedoms of natural

Persons”, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/

publications/short papers/DSK_KPNr_18_Risiko.pdf.

may use the algorithms listed in BSI TR 02102-2. Around

to facilitate the establishment of encrypted connections, the person responsible should

literal for encryption and authentication as broad as possible

Offer a spectrum of qualified algorithms.

To ensure the authenticity and integrity of received email messages

to check, those responsible should check and sign DKIM signatures

Mark or at ned messages that fail validation

corresponding definition of the sender via a DMARC entry in the

DNS, reject.

4.1.2 High Risk Obligations

If a person responsible receives data specifically by e-mail, where

the breach of confidentiality poses a high risk to rights and freedoms

of the natural persons concerned, then he must have both qualitative

fied transport encryption (see below No. 5.2) as well as the receipt of

Enable end-to-end encrypted messages.

If a person responsible receives data specifically by e-mail, where

the breach of integrity poses a high risk to the rights and freedoms of

represents natural persons concerned, then he must have existing (PGP

or S/MIME) signatures qualified check (see below no. 5.4).

4.2 Sending Email Messages

4.2.1 Ordinary Risk Obligations

All those responsible for sending e-mail messages containing personal data

send, in which a breach of confidentiality (of the content or circumstances

de of communication, insofar as they relate to natural persons)

represents a risk to the rights and freedoms of natural persons,

should be based on TR 03108-1 and must have a mandatory

Ensure transport encryption.

4.2.2 Sending High Risk Email Messages

Those responsible for sending e-mail messages where a break

the confidentiality of personal data in the content of the message

a high risk to the rights and freedoms of individuals

represents, an end-to-end encryption and a

carry out qualified transport encryption. To what extent either on the

End-to-end encryption or the fulfillment of individual requirements

to this (see chapter end-to-end encryption) or to the qualified one

243

The Hessian Commissioner for Data Protection and Freedom of Information

49. Activity report on data protection

Transport encryption (e.g. DANE or DNSSEC) can be dispensed with

depends on the existing risks, the specific design of the

Transmission route and any compensating measures taken.

4.2.3 Sending e-mail messages with content to be kept secret

high risks

Persons responsible for keeping communications confidential on the basis of Section 203 of the Criminal Code

communication content must have the information under 4.2.1 or 4.2.2

ensure the requirements listed above through encryption,

that only bodies can perform a decryption to which the contents

of the news may be revealed.

5. Encryption and signature process requirements

5.1 Mandatory Transport Encryption

An obligatory transport encryption should ensure an unencrypted

Rare transmission of messages can be excluded. she can over

the SMTPS protocol or by calling the STARTTLS SMTP command and

the subsequent structure of an encrypted with the TLS protocol

Communication channel can be realized, with the requirements of TR

02102-2 of the Federal Office for Information Security (BSI).

are fulfilled.

In the latter method (STARTTLS), the obligatory

Transport encryption through appropriate configuration of the sending

MTA (Mail Transfer Agent) can be reached; the corresponding configuration

tion settings are called (En)Forced TLS, Mandatory TLS or similar.

If the remote station does not support TLS, the connection will be established

canceled. Some MTAs allow domain-specific or re-

gel-based specification of this behavior.

5.2 Qualified Transport Encryption

Transport encryption achieves a under the following conditions

adequate protection against active attacks by third parties who are able

are to manipulate the network traffic on the transmission path:

1. The cryptographic algorithms and protocols used are compliant

the state of the art: They meet the requirements of the technical

Guideline BSI TR-02102-2 and guarantee Perfect Forward Secrecy.

2. The designation of the mail servers authorized to receive and their

IP addresses were signed by DNSSEC on the recipient side. The SI-

Signatures of the DNS entries are checked on the sender side. Alternatively

the name of the mail server authorized to receive can also be used

verified through communication with the recipient.

3. The receiving server is encrypted in the course of building the

Connection authenticated either based on a certificate or using a

public or secret key sent over another channel

agreed between sender and receiver.

4. If the authentication is certificate-based, the recipient carries out the

Authenticity of the certificate to a trusted root certificate

or a trust anchor published via DANE.

Compliance with these requirements must be demonstrated.

5.3 End-to-End Encryption

Through end-to-end encryption using the S/MIME and

With OpenPGP it is possible to thoroughly examine the contents of an e-mail message

to protect against unauthorized access. This protection extends

not only on the actual transport route, but also on

the intermediate storage and processing on the basis of the transmission

participating servers. In order to achieve this effectiveness, the following

to comply with the requirements:

1. The person responsible must access the public keys of the recipients

compliance with sufficient safety parameters (in particular one

sufficient key length) check them by verifying the

Authenticate certificates or authentications before each dispatch or

Check signature verification for validity and manage reliably.

2. The verification of the authenticity of a key can be carried out regularly

by verifying a certificate from a trusted certificate

service provider (S/MIME) or authentication of other trusted

and demonstrably reliable third party (OpenPGP). It's over

strongly advised that the release of a key

on an OpenPGP key server no indication of the authenticity of this

key is. Checking the fingerprint of an OpenPGP key

is sufficient for checking the authenticity of a key,

provided the fingerprint with a secure cryptographic hash function

(see BSI TR-02102) and the authenticity of the comparison value, e.g. B.

through direct communication with the recipient through another

channel has been checked.

3. The authenticity of a provided via Web Key Directory (WKD).

public key is equivalent to the authenticity of the provided

providing web server. The requirements apply to the review

to verifying the authenticity of the receiving mail server

accordingly.

4. This requirement can also be made retrospectively with regard to keys

are filled, which were initially exchanged opportunistically (e.g.

via autocrypt). For this purpose, a verification of the authenticity via a

another channel required.

5. Checking the validity of an S/MIME key before its

Deployment is to be carried out by retrieving validity information from the certi-

fikat service provider (retrieval of CRL via http, OCSP). The

Checking the validity of an OpenPGP key is only possible

if the owner has announced where he can obtain revocation certificates, if any

intended to publish. This can e.g. B. an OpenPGP key

selserver or the website of the key owner. Unless it's on

such a possibility of retrieval is lacking, there must be guarantees that

that all users of a key are informed immediately if

this its validity - in particular due to a compromise

of the associated private key – loses.

Anyone who encrypts messages end-to-end should note that Perfect

End-to-end encryption alone does not provide forward secrecy

is such that a compromise of a recipient's private key

all messages with the associated public key are compromised

have been encrypted. email messages intercepted by third parties,

can be kept by them and upon disclosure of the private key

one of the receivers to be decrypted at a later time.

5.4 Signature

A signature with the S/MIME and OpenPGP procedures makes it possible

the integrity of the content of an e-mail message against unauthorized persons

protect impairment. This protection does not only extend

on the actual transport route, but also on the intermediate storage

tion and processing on the servers involved in the transmission. Around

To achieve this effectiveness, the following requirements must be met:

Senders must use their own signature keys with sufficient security

s parameters and store the private keys securely and

use, and they must, to the extent that no direct comparison of the keys between

Sender and receiver takes place, the corresponding public

Certify keys from reliable and trusted third parties

and make them available to your communication partners. recomm.

catchers should depend on the authenticity and integrity risks

those in chap. end-to-end encryption listed measures

the verification and management of the keys of the transmitters in

apply accordingly.

Appendix to I

3. Activity Report on Freedom of Information

The Hessian Commissioner for Data Protection and Freedom of Information

II

Second part

3. Activity Report on Freedom of Information

introduction

1. Introduction Freedom of Information

introduction

Freedom of information is only gradually gaining ground. The number of

claims made for information are still limited. Also have the

Municipalities from the possibility of their own freedom of information regulations

create, hardly used. On this development I have as

Chairman of the Freedom of Information Conference carefully in the year under review

made and saw in it a confirmation of the Hessian model, which

Data protection and freedom of information bracketed and in a meaningful

context. This also proved itself in connection with the

Corona pandemic, which showed that the quantity of information is not

what matters is their content and quality.

251

Freedom of information towards the LvV and police authorities

2. Inappropriate disclaimer of freedom of information

the State Office for the Protection of the Constitution and opposite

police authorities

Freedom of information towards the LvV and police authorities

It is both for reasons of freedom of information and with a view to

Tasks of the police authorities and the State Office for Constitutional

protection inappropriate, freedom of information claims against them

to exclude positions entirely. As far as the performance of the tasks

of these bodies is not affected, freedom of information is imperative

to ensure.

Last year 2020 I chaired the conferences of the information

Federal and State Commissioner for Freedom of Information (IFK). A thing

of the discussions was the access to information in the federal and state governments

the protection of the constitution and the police. Unfortunately it turned out that

Hessen is not "in front" in this respect, but rather "behind".

This is due to the fact that Hesse has given these authorities any information

excludes freedom of action, § 81 Para. 2 No. 1 HDSIG by applying the

Hessian freedom of information regulations on these authorities

legally negated.

§ 81 HDSIG

(...)

(2) The provisions of Part Four do not apply to

1. the police authorities and the State Office for the Protection of the Constitution

(...)

Tasks of the Office for the Protection of the Constitution and the Police

The Offices for the Protection of the Constitution have the task of providing information about

anti-constitutional efforts against the free democratic

basic order, against the existence or security of the federal government or a

country or an unlawful impairment of the official

have the goal of collecting and

evaluate. Further areas of responsibility are in particular counter-espionage,

i.e. the fight against security-endangering or secret service activities

ties of other states, as well as the observation of groups by

Germany from e.g. Islamist and other extremist activities in the

Support abroad and thus endanger Germany's foreign interests.

The authorities for the protection of the constitution are thus active in domestic reconnaissance.

The offices for the protection of the constitution are an important part of the executive branch

in our free democratic constitutional state, just like the police,

which, in particular, in accordance with the police law for security and

is responsible for the prosecution of criminal offenses under the Code of Criminal Procedure.

Have a privileged position compared to the rest of the administration

these authorities with a view to freedom of information and the associated

the transparency of a democratically founded administrative organization

but not according to our constitution.

Appropriate limitations on access to information

A regulation in the Hessian freedom of information law would be appropriate,

excludes the information for the case constellations in which the

Notification of adverse effects on the performance of the duties of the

State Office for the Protection of the Constitution or the police.

Such a regulation would become part of the Hessian freedom of information law

also insert consistently. Because that is what is already in force in particular

Right that access to information does not exist when the disclosure

of information adverse effects on matters of external or

public security, § 82 No. 2 b) HDSIG. The correlation with the

Tasks of the Office for the Protection of the Constitution and the police are evident here.

§ 82 HDSIG

There is no right to access information...

(...)

2. for information the disclosure of which may have adverse effects on

(...)

b) matters of external or public security

(...)

In addition, there is another alternative legislative option,

to soften the absolute exclusion of information access in favor of a

differentiated and thus also in the matter balanced regulation:

Based on the regulatory concept to be recognized in Section 81 (1) HDSIG

tion, the core functions of the places mentioned there from information access

could also exclude access to information about the core functions

excluded from the police and the protection of the constitution, but for the general public

Administration area of these bodies will be opened. For example, could

254

Freedom of information towards the LvV and police authorities

then information about renting the building or fleet costs

be applied for successfully.

The Hessian state parliament/the Hessian state government should therefore

in the sense of a concise Hessian freedom of information right

tion access to the State Office for the Protection of the Constitution and

the police authorities in favor of a differentiated regulation instead of one

absolute information access exclusion more information freedom friendly

design.

255

Access to information regarding insurance supervision

3. Access to information regarding insurance supervision

Access to information regarding insurance supervision

A right to information access to the Hessian Minis-

terium for social affairs and integration in its function as supervisory authority

for the Unfallkasse Hessen does not exist if the disclosure of the

Information adverse effects on this supervisory task of the

ministry can have.

The Hessian Ministry for Social Affairs and Integration reported to me about

a citizen's freedom of information request submitted to the Minister

terium had submitted and the area of responsibility of the ministry

as the supervisory authority for the Hesse accident insurance fund. Imagine the

Question whether the Ministry in this case as an insurance regulator

with a view to the Hessian freedom of information law, § 82

No. 2 c) HDSIG.

Legal Assessment

The thematization of the Ministry, whether it is in terms of the accident insurance

Hessen is to be classified as an insurance supervisory authority, had its

Reason in the determination of the Hessian freedom of information law that

in such a case there is no right to access information if

the emergence of adverse effects on the supervisory tasks

can have, § 82 No. 2. c) HDSIG.

§ 82 HDSIG

There is no right to access information

(...)

2. for information the disclosure of which may have adverse effects on

(...)

c) the control, enforcement or supervisory tasks of the financial, regulatory, savings banks,

insurance and competition regulators

(...)

The term insurance supervisory authority is not defined in more detail in the HDSIG,

and also in the explanatory memorandum to the bill there is reference to this term

no further information (cf. Landtag-Drucks. 19/5728 p. 151 on § 82).

After all, the savings bank supervision is explicitly mentioned in the justification

(loc. cit.), taking into account the regulatory text of § 82 No. 2 c)

HDSIG it is finally clear that in the official legal text behind "Sparkas-

sen” the separator was obviously forgotten. Just because of

(correctly meant) naming of the savings bank supervision in the regulation

With regard to savings banks as institutions under public law, it makes sense

that accordingly with insurance companies in this supervisory context

Public insurance companies, i.e. Hessian corporations

of public law are meant. An example here would be the

Unfallkasse Hessen as a statutory accident insurance institution within the meaning of

Social Code VII. Consequently, the Hessian Ministry for

Social affairs and integration with the term insurance supervisory authority in

§ 82 No. 2 c) HDSIG meant in the present context.

From the wording of the term "insurance

insurance supervision” should also consider the private insurance industry,

but it is precisely this insurance supervision that is not the responsibility of the state authorities

assigned, as is the case, for example, with the data protection supervisory

issue of the European General Data Protection Regulation in connection with the

Federal Data Protection Act is the case. Rather, this insurance

supervision by the Federal Financial Supervisory Authority (BaFin).

based on the Insurance Supervision Act (VAG).

So this shows that the issue of insurance supervision in the private sector

anyway a federal matter and not a state matter.

Against this overall background, it only makes sense to

Security supervision in the Hessian freedom of information law the Hessian

State supervision of the Hessian public insurance sector

understand. That's why I have the Ministry of Social Affairs and Integration

also confirmed in its opinion that in its function as supervisory

authority via the Unfallkasse Hessen an insurance supervisory authority

within the meaning of the Hessian freedom of information law.

258

Municipal freedom of information statutes without HDSIG

4. Municipal freedom of information statutes do not apply

of the HDSIG

Municipal freedom of information statutes without HDSIG

As far as municipalities decide to use municipal freedom of information

introduce statutes without the Hessian Freedom of Information Act as

The Hessian Freedom of Information Officer is not to be referred to

affected by its legal jurisdiction.

In early 2020, the civil rights group dieDatenschutz

Zer Rhein Main” states that they are based on a proposal from the alliance

"Freedom of information for Bavaria" a model draft for a municipal

have drawn up a freedom of information statute, with which they

munen in Hesse, especially in the Rhine-Main region,

to promote freedom of information at the municipal level.

In this regard, the civil rights group asked me to share their

comment on the draft design. This “model statute presented to me

Freedom of information for cities and communities in Hesse" is known as "Transpa-

statute on freedom of information for the city/municipality” and

contains eleven individual paragraphs. It is therefore a statutory

concept that is outside of the regulations of the Hessian data protection and

Freedom of Information Act lies.

Legal position of the Hessian freedom of information officer

I have informed the civil rights group that I have contacted their satellite

draft. This has the following background, which I

explained to the civil rights group.

The Hessian legislator regulates in § 81 para. 1 No. 7 HDSIG that the

regulations on access to information also apply to local authorities,

as far as the application of the information freedom regulations

of the law (fourth part, §§ 80 ff. HDSIG) by statute expressly

is determined.

§ 81 HDSIG

(1) In accordance with Article 2, Paragraphs 1 to 3, the provisions on the access to information

go for too

(...)

7. the authorities and other public bodies of the communities and districts as well

their associations regardless of their legal form, as far as the application of the fourth

Partly expressly determined by the articles of association.

3. Activity Report on Freedom of Information

Apart from this main municipal regulation, there are still in the HDSIG

a supplementary provision in § 88 para. 2 HDSIG, which stipulates that in this

In this case, i.e. the express application provision by the articles of association,

the costs are also charged in accordance with the statutes. In § 88 paragraph 2

HDSIG is in the official legal text as a result of an editorial error

not, as would be correct, referred to Section 81 Paragraph 1 No. 7 HDSIG, but

erroneously on "§ 81 sentence 1 No. 6". This error results from the fact that in

Draft law (LT-Drucks. 19/5728) the municipal statute reservation

aptly the validity of the Hessian freedom of information law originally

in § 81 paragraph 1 No. 6 was provided and in the later change in

Legislative procedure for No. 7, the cost provision in Section 88 (2) HDSIG

has not been correctively updated from #6 to #7.

For the way, by express statute provision, the Hessian

introduce freedom of information rights at the municipal level

some municipalities have now decided (e.g. the districts of Marburg-

Biedenkopf, Darmstadt-Dieburg, Groß-Gerau and the cities of Kassel and

Neu-Isenburg), even if the vast majority of municipalities apparently do so

prefers to answer citizen inquiries without being bound by the legal requirements in the

To be processed within the meaning of §§ 80 ff. HDSIG.

The Hessian Freedom of Information Officer is responsible for

regulated in more detail by a special standard, namely § 89 HDSIG, and this re-

success implicitly determines the responsibility only for those municipalities that are

Within the meaning of Section 81 Paragraph 1 No. 7, the Hessian freedom of information law, i.e

the fourth part of the HDSIG, integrated into the municipal legal area

have.

§ 89 HDSIG

(1) Anyone who sees his rights violated according to the fourth part can do so without prejudice

other legal remedies, the Hessian Freedom of Information Officer or the

Call the Hessian freedom of information officer.

(...)

(3) (…)

If the Hessian Freedom of Information Officer detects violations of the

th of the fourth part, he or she can demand their correction within a reasonable period of time.

(...)

260

Municipal freedom of information statutes without HDSIG

With a view to these legal requirements, I have the concern of

Civil rights group, outside of Part Four of the HDSIG a self

to appreciate the draft municipal statutes that have been produced, not complied with.

261

WLAN structure of public places

5. Information access regarding the WLAN structure more public

Place

WLAN structure of public places

Access to information regarding the WLAN structure of public authorities

is supported by the Hessian Commissioner for Freedom of Information. In

In this matter, there was cooperation with the Federal Network Agency.

A citizen complained to me that he went to the universities

of the State of Hesse regarding their WLAN structure Freedom of Information

submitted applications, but either did not answer them at all

or rejected with reference to safety concerns

had been.

The information access request was worded as follows:

“Are the WLAN systems (e.g. that provide Eduroam) the

University set so that these z. B. by a rogue access point

Containment function other WiFi signals using Deauth/Deasso

interference packets?

If so, why and what settings are there?

If not why?

Cooperation with the Federal Network Agency

The content of this information access request was reason for me in the

thing to contact the Federal Network Agency and with this the

opportunity to discuss. The freedom of information request concerns the issue

whether a particular technique used under the general assignments of the

WLAN frequencies in accordance with Section 55 (2) of the Telecommunications Act (TKG)

is expressly assessed as inadmissible by the Federal Network Agency,

is used.

Since only a detailed disclosure of the freedom of information request

could touch on security-relevant aspects, I have the one concerned

Universities suggested that the complainant (where applicable)

to inform that the use of the WLAN networks exclusively within the framework

the specifications of the currently published general allocations.

So the answer might look like this:

"Emissions that intentionally interfere with certain WiFi usages or

prevent, such as B. Transmission of radio signals and/or data packets,

Logging out or influencing the WiFi connections of others

The Hessian Commissioner for Data Protection and Freedom of Information

3. Activity Report on Freedom of Information

Targeting users against their will is not permitted and will not

not used at the university.”

The complainant came back after some time and shared

with, his complaints were settled, his freedom of information requests

have now been informed.

264

Labor Statistics Freedom of Information

6. Labor Statistics Freedom of Information

Labor Statistics Freedom of Information

There was a slight increase in complaints compared to the previous year

and consultations.

IFG

complaints

consultations

2019

61

42

2020

64

47

265

ANNEX to II

Appendix to II

In 2020, the Conference of Freedom of Information Officers

ments of the federal and state governments (IFK) no resolutions, resolutions

or materials taken.

subject index

reference

I 4.1

I 17.1, I 17.2

I 2.2

I 11.7

I 2.1

I 2.1

I 8.5

4.2

I 7.1

I 7.1

I 3.2

I 7.2

I 5.1, I 8.2, I 8.6

I 8.7

subject index

The Hessian Commissioner for Data Protection and Freedom of Information

49th activity report on data protection / 3rd activity report on freedom of information

subject index

factual

Remedial Powers

remedial actions

adequacy decision

continuous monitoring

service provider

- representative

– external

Digital sovereignty

digitalization

distance rules

Third country/states

EDSA

e-mail

– accounts

– addresses

– Service Provider

– infrastructure

– communication

- News

- P.O. Box

– providers

– Servers

– distributor

e-Privacy Policy

One mailbox strategy

consent

I 9.3

I 3.4, I 6.1, I 8.7

I 3.4

I 3.4, I 12.3, I 13.1

Appendix I 1.5

Appendix I 1.1

I 10.1

I 2.2, I 16.2, Appendix I 2.6

I 2.1, I 2.2

I 5.3

I 5.3, I 13.2

Appendix I 2.6

I 14.1

I 14.1

Appendix I 3.1

I 5.3

I 14.1

I 14.1

I 8.2, Appendix I 2.6

I 13.1, Appendix I 1.2

I 3.3

I 3.2, I 7.1, I 7.2, I 7.3, I 8.5, I 10.1,

I 11.1, I 11.4, I 12.3, I 13.2, Appendix

I 1.2, Annex I 2.3, Annex I 2.5,

Appendix I 2.6

I 11.3, Appendix I 2.3

I 13.1

I 3.2

I 11.6, I 12.2

I 12.2, Appendix I 2.3

I 2.1

I 9.1

I 6.2

I 6.2

I 7.3

I 16.3

I 2.1

I 2.1

I 6.1

I 8.5

I 10.1

I 11.3

camera dummy

license plate recognition

number plate control

day care centers

litigation

coherence method

cooperation procedure

configuration error

contact details

contact restrictions

bank statements

274

subject index

health insurance

customer data

I 7.2

I 11.6, Appendix I 1.4

teachers

log data

Payroll

deletion

LUSD

I 5.3

I 6.1

I 11.5

I 3.2, I 11.2, I 12.3

I 8.6

I 8.6

measles protection

Measures, preventive police I 4.2

obligation to report

reporting procedure

employees

– former

members

Mobile ticketing system

mouth and nose

– -Coverage

- -Protection

I 8.2

I 5.1

I 15.1, I 15.2

I 15.2

I 8.4

I 8.7

I 10.2, I 11.2

I 6.1

intelligence services

tracking

user

– -accounts

- -groups

– -profiles

Appendix I 1.1

I 13.2

I 6.1

I 13.1

I 13.1

property protection

prohibition of disclosure

One shop stop

Online Appointment

open source software

administrative offences

Organ-

- -recipient

– -donor

Pandemic

parking duration recording

parking garages

parking ticket

parliaments

patient

- -file

- -data

personnel file data

identity card

personality

– -information

– -profile

- -right

ID number

mistaken identity

plausibility check

Police 2020

Privacy Shield

276

I 9.1

I 8.5

I 2.1

I 3.1

I 5.2, Appendix I 1.5

I 16.1

I 8.5

I 8.5

I 8.1, I 8.2

I 6.2

I 6.2

I 6.2

Appendix I 2.2

I 8.2, Annex I 1.6

I 8.2, I 8.4, I 8.7, Appendix I 1.6

I 5.3

I 11.6

Appendix I 2.6

Appendix I 1.7

I 7.1, I 9.3

Appendix I 1.7

I 12.3

I 15.2

Appendix I 1.8

I 2.2

subject index

private autonomy

Private devices

forecast

inspection requirements

pseudonyms

I 12.3

I 5.3

I 15.2

4.2

I 11.6

accountability

legal remedy

legal purchase

Registry modernization

I 7.1

I 16.3

I 11.1

Appendix I 1.7

restaurant operator

RFID time attendance system

risk assessment

I 3.1

I 7.1

I 11.3

I 7.2

Appendix I 1.3

I 4.1

I 14.1

I 3.2

I 4.1

I 5.1

I 3.2

I 5.3

I 2.2

I 14.2

Appendix I 1.7

I 3.4

Appendix I 2.4

I 9.3

Appendix I 1.2, Appendix I 2.5

I 13.1

Appendix I 2.1

Appendix I 2.3

I 13.1

I 10.1

I 2.1

I 14.1, Appendix I 3.1

redactions

confidentiality

security

– -authorities

- -examination

security of processing

meeting minutes

Social networks

State Education Board

city council meetings

master record

Standard Privacy Clauses

Standard Privacy Model

Tax Identification Number

road post

street view

storage duration

telemedia

- -services

telemetry

temperature detection

tracking

training operation

transfer tool

transport encryption

278

inaction

club members

I 10.1

I 7.1

II 2

I 7.1, I 10.1, I 10.2

I 7.1

II 2

Appendix I 1.3

I 14.1, Appendix I 3.1

I 16.2

I 16.1, I 16.2

I 9.1, I 9.3, I 16.3

I 6.2

I 5.2

I 5.2

I 8.1, Annex I 2.3

I 6.1

I 13.1

I 13.1

Appendix I 1.2

I 13.1

I 13.1, I 13.2, Appendix I 1.2

I 7.1, I 12.3, Appendix I 2.3,

Appendix I 2.5

Appendix I 2.1

49th activity report on data protection / 3rd activity report on freedom of information

time tracking system

Central post office

access

– -control

- -steering

accesses

Access Permissions

access management

access

– control

- Regulation

– fuse

earmarking

Two-factor authentication

I 7.1

I 3.3

I 11.4, I 15.2

I 3.1

I 8.2, I 8.4, I 9.3

Appendix I 1.1

Appendix I 1.6

I 11.4

Appendix I 2.3

I 8.7

I 8.5, I 16.1

I 5.3

280