THE HESSIAN COMMISSIONER

FOR PRIVACY

AND FREEDOM OF INFORMATION

LT Drs. 7/1495 BC 3/29/1972 ú LT-Drs. 7/3137 BC 29.3.1973 ú LT-Drs.

LT Drs. 7/1495 BC 3/29/1972 ú LT-Drs. 7/3137 BC 29.3.1973 ú LT-Drs.

7/5146 BC April 1, 1974 ú LT-Drs. 8/438 BC 3/26/1975 ú LT-Drs. 8/2475 BC

7/5146 BC April 1, 1974 ú LT-Drs. 8/438 BC 3/26/1975 ú LT-Drs. 8/2475 BC

30.3.1976 ú LT-Drs. 8/3962 BC 11.3.1977 ú LT-Drs. 9/67 BC 12/18/1978 u

30.3.1976 ú LT-Drs. 8/3962 BC 11.3.1977 ú LT-Drs. 9/67 BC 12/18/1978 u

LT Drs. 9/2740 BC 06.2.1980 ú LT-Drs. 9/4032 BC 12/23/1980 ú LT-Drs.

LT Drs. 9/2740 BC 06.2.1980 ú LT-Drs. 9/4032 BC 12/23/1980 ú LT-Drs.

9/5873 BC 15.1.1982 ú LT-Drs. 10/166 BC 12.1.1983 ú LT-Drs. 11/473 BC

9/5873 BC 15.1.1982 ú LT-Drs. 10/166 BC 12.1.1983 ú LT-Drs. 11/473 BC

19.1.1984 ú LT-Drs. 11/3215 ú 14.2.1985 ú LT-Drs. 11/5232 BC 1/24/1986

19.1.1984 ú LT-Drs. 11/3215 ú 14.2.1985 ú LT-Drs. 11/5232 BC 1/24/1986

ú LT-Drs. 12/21 BC 18.2.1987 ú LT-Drs. 12/1742 BC 26.2.1988 ú LT-Drs.

ú LT-Drs. 12/21 BC 18.2.1987 ú LT-Drs. 12/1742 BC 26.2.1988 ú LT-Drs.

12/4040 BC 2.2.1989 ú LT-Drs. 12/6126 BC 13.2.1990 ú LT-Drs. 12/7951 BC

12/4040 BC 2.2.1989 ú LT-Drs. 12/6126 BC 13.2.1990 ú LT-Drs. 12/7951 BC

11.2.1991 ú LT-Drs. 13/1756 BC 4.3.1992 ú LT-Drs. 13/3887 BC 2/23/1993

11.2.1991 ú LT-Drs. 13/1756 BC 4.3.1992 ú LT-Drs. 13/3887 BC 2/23/1993

ú LT-Drs. 13/5813 BC 11.2.1994 ú LT-Drs. 14/412 BC 21.2.1995 ú LT-Drs.

ú LT-Drs. 13/5813 BC 11.2.1994 ú LT-Drs. 14/412 BC 21.2.1995 ú LT-Drs.

14/1418 BC 22.2.1996 ú LT-Drs. 14/2701 BC 24.2.1997 ú LT-Drs. 14/3697

14/1418 BC 22.2.1996 ú LT-Drs. 14/2701 BC 24.2.1997 ú LT-Drs. 14/3697

v. 5.3.1998 ú LT-Drs. 15/23 BC 8.4.1999 ú LT-Drs. 15/1101 BC 3/28/2000 u

v. 5.3.1998 ú LT-Drs. 15/23 BC 8.4.1999 ú LT-Drs. 15/1101 BC 3/28/2000 u

LT Drs. 15/2500 BC 2.4.2001 ú LT-Drs. 15/3705 BC 6.3.2002 ú LT-Drs.

LT Drs. 15/2500 BC 2.4.2001 ú LT-Drs. 15/3705 BC 6.3.2002 ú LT-Drs.

15/4790 BC 17.3.2003 ú LT-Drs. 16/2352 BC April 24, 2004 ú LT-Drs. 16/3746

15/4790 BC 17.3.2003 ú LT-Drs. 16/2352 BC April 24, 2004 ú LT-Drs. 16/3746

v. 7.3.2005 ú LT-Drs. 16/5359 BC 6.3.2006 ú LT-Drs. 16/6929 BC 2/21/2007

v. 7.3.2005 ú LT-Drs. 16/5359 BC 6.3.2006 ú LT-Drs. 16/6929 BC 2/21/2007

ú LT-Drs. 16/8377 BC 19.2.2008 ú LT-Drs. 18/106 BC 27.2.2009 ú LT-Drs.

ú LT-Drs. 16/8377 BC 19.2.2008 ú LT-Drs. 18/106 BC 27.2.2009 ú LT-Drs.

18/2027 BC 9.3.2010 ú 18/3847 B.C. 18.3.2011 ú 18/5409 B.C. 20.3.2012 u

18/2027 BC 9.3.2010 ú 18/3847 B.C. 18.3.2011 ú 18/5409 B.C. 20.3.2012 u

18/7202 BC 9.4.2013 ú 19/289 B.C. 3/31/2014 ú 19/2334 B.C. 31.8.2015 ú 19/3510

18/7202 BC 9.4.2013 ú 19/289 B.C. 3/31/2014 ú 19/2334 B.C. 31.8.2015 ú 19/3510

v. 22.6.2016 ú 19/4762 B.C. 30.3.2017 ú 19/6137 B.C. 7.5.2018 ú 20/704 B.C.

v. 22.6.2016 ú 19/4762 B.C. 30.3.2017 ú 19/6137 B.C. 7.5.2018 ú 20/704 B.C.

5/28/2019 ú 20/2607 B.C. 6.4.2020 ú 20/5799 B.C. 27.5.2021 úLT-Drs. 20/8296

5/28/2019 ú 20/2607 B.C. 6.4.2020 ú 20/5799 B.C. 27.5.2021 úLT-Drs. 20/8296

x.x.2021 úú

x.x.2021 úú

50

50

50. Activity report on data protection

4. Freedom of information activity report

Fiftieth activity report

to data protection

and

Fourth activity report

to freedom of information

of

Hessian Commissioner for Data Protection

and freedom of information

professor dr Alexander Rossnagel

submitted as of December 31, 2021

according to Art. 59 of Regulation (EU) No. 2016/679 i. V. m.

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

50th activity report on data protection / 4th 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. Alexander Rossnagel

Gustav-Stresemann-Ring 1, 65189 Wiesbaden

PO Box 31 63, 65021 Wiesbaden

Phone:

E-mail:

Internet:

(06 11) 14 08-0

poststelle@datenschutz.hessen.de

www.datenschutz.hessen.de

Printed matter of the Hessian state parliament 20/8296

Technical and organizational support: Frauke Börner (HBDI)

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

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

Table of contents

Table of contents

core items

core items

core items

1. For data protection in Hesse, there were no difficult

significant violations - in contrast to the development in

Germany or in the world. In Hesse, data protection has been largely

accepted and not fundamentally questioned. Nevertheless, in many

Areas that meet the requirements of the General Data Protection Regulation (GDPR)

GMO) still not sufficiently implemented, lead to complaints,

require the intervention of the data protection supervisory authority and orders

and enforcement actions on a case-by-case basis. The digitization of many

Tasks and activities cause additional

che obligations, entails additional requirements and requires

additional attention (Part I No. 1).

2. For the further development of data protection in Hesse win the

Europeanization with decisions of the European Court of Justice

(ECJ) and the European Data Protection Board (EDPB) (Part I

No. 1 and 5) as well as the juridification of data protection law with a

Significant increase in fines (from 2 in 2020 to 29

in 2021) and involving the courts (Part I, Items 1 and 6)

increasingly important. This requires more influence

European developments through committed participation in work

circles of the EDPB and the expansion of the legal department to deal with the

additional process procedures.

3. The diverse data protection issues in the implementation of the corona protection

measures in many everyday areas of life led to

data protection complaints, inquiries and advice from

Those affected and those responsible for data processing (Part I No. 1

and 2). Additional measures were also required to

management decisions made at the beginning of the pandemic

with the new challenges that are understandable in the situation im

Result but were in breach of data protection, to correct gradually

(Part I Nos. 1 and 4.2).

4. A key focus of oversight activity continued to be the

Handling of complaints, inquiries and advice on exercise

of the rights of those affected and to support those responsible.

Their number has stabilized four years after the DS

GMOs at a very high level, they are becoming more demanding in terms of quality.

Simpler questions, such as information obligations and information

right, go back and telephone consultations with them (of more

than 10 minutes) (from 9,444 to 6,384). On the other hand, more difficult ones took

Edits and with them the documented inputs still

slightly (from 7,991 to 8,404). Large digitization projects, e.g. B.

the implementation of the online access law or the Hessian school

portal, do not appear in the statistics to the same extent as they do

actually employ my authority (Part I, No. 19).

5. Data Breach and Breach Reporting

according to Art. 33 DS-GVO now form a large part of the reactive

activity of my supervisory authority. New forms of cybercrime
such as phishing and ransomware attacks, exploiting security
security vulnerabilities and the publication of personal data
in the Darknet caused new dangers for the persons concerned
and those responsible and led to an increase in reports
(from 1,432 to 2,016) (Part 1 No. 17).
In the administrative authorities of the state and the municipalities
currently designing large and demanding digitization projects,
planned and implemented, which requires intensive participation and critical
work of data protection supervision (Part I, Item 8).
6.
7. The schools and colleges were primarily characterized by strong
Developments towards more digitization of lessons and examinations,
teaching and learning. In addition to the use of video conferencing systems
(Part I No. 4) this concerned e.g. B. equipment rental, learning aids and remote
functions. In the school area, I accompanied the development of Hessian
school portal and advised on the data protection regulations of the
new school law (Part I, Item 9).
8. The digitization of work means that employee relationships
Employers are measuring performance and behavior more and more intensively
of employees can monitor. In this area had to mine
Authority to intervene to correct in several cases (Part I No. 11).
In the field of video surveillance by the police and security
authorities, but even more so by private companies and in the neighboring
relationship, my authority had to repeatedly settle disputes
intervene (Part I, Items 7 and 13).

9.

10. In the private sector I had many complaints

in particular on the rights of data subjects such as the request for information

dictation (Part I No. 14) and for the processing of address data

Credit agencies and debt collection agencies (Part I, Item 15).

11. In the healthcare sector, data protection oversight has been heavily

data processing in the context of the corona pandemic (Part I, Item 2).

But also problems such as maintaining patient confidentiality

X

core items

Transmission of patient data and storage of patient

files had to be solved. (Part I No. 17).

12. Although freedom of information in Hesse is still limited to the

of the administration and a few municipalities and counties, I had

as Freedom of Information Officer many interesting ones in the year under review

To answer questions about freedom of information and to support many

Citizens in enforcing their claims (Part II

Sections 2 and 3). I also took part in legal policy

Further development of the freedom of information (Part II No. 5) and worked in the

Conference of Freedom of Information Officers (IFK) with (Part II Appendix).

13. Complaints and consultations increased slightly (from 111 to 123).

XI

foreword

foreword

foreword

This is the first activity report for which I am responsible and at the same time the

50th of the Hessian Commissioner for Data Protection and Freedom of Information.

The first activity report (state parliament printed matter 7/1495) dates from 29.

March 1972. With him, the first data protection officer in Hesse described,

Willi Birkelbach, the first steps of data protection supervision in the new

scope of data protection. The duties of the data protection officer

were without any precedent at the time because the Hessian Data Protection Act

(HDSG) of October 7, 1970 was the world's first data protection law.

In this respect, there was also no model for such a report. It was

the world's first privacy report.

The report describes a "forward into new territory" of data protection (p. 10f.).

The law only applied to machine data processing in the public sector

Administration of the State of Hesse. It was a reaction to the foundation

the Hessian Center for Data Processing (HZD) and the local authorities

Regional data centers (KGRZ) (p. 8). The Data Protection Act applied to everyone

Data of natural and legal persons collected by data centers and

Public administration authorities were processed. It tracked three

Aims: protection against encroachments on privacy and secrecy, preservation

separation of powers between parliament, government and municipalities

and backing up data and databases (p. 31). The tasks of

According to § 10 HDSG, data protection officers insisted on compliance

of the law and the competent supervisory authority

teach and the effects of machine data processing

on the state separation of powers (p. 11f.). objects of

Investigations and observations included machine rooms and roof

data carrier archives, punched cards and magnetic tapes (pp. 20, 31f.). The integration

of databases and remote data processing were at the time

to recognize the horizon (p. 33f.). The data protection officer was appointed according to § 7 Para. 1 HDSG elected by the state parliament at the suggestion of the state government and was free from instructions according to § 8 HDSG. Him stood to fulfill his Tasks of a technical official and a civil servant of the higher service and a typist available (p. 35).

Remarkable for this first activity report are findings on Task of data protection and data protection supervision, which after the Experience with 49 other activity reports appear timeless: On the one hand comments Birkelbach on the relationship between data protection law and information technology that with an unregulated development of information technology there is a risk

"that the laws no longer determine the development of data processing, but that they are adapted to the status of data processing. Then once the EDP systems are installed at great expense and has changed the work structures accordingly, then there are practical constraints emerged that narrow the scope for decision-making. The subsequent Consideration of the measures necessary for data protection would be included involves a great deal of effort or is no longer feasible" (p. 36).

On the other hand, Birkelbach closes his report with a look into the future the challenges of data protection that still exist today – in a world of artificial intelligence, big data and the global and ubiquitous Data processing – applicable is:

Development does not stand still. New techniques may be tomorrow

open new avenues to progress and the good of man; but she

are also new, unknown dangers for the individual and for the freedom

inherent structure of state and society. These dangers must

be countered in a timely and effective manner. Constant vigilance is necessary

digital Society will also change its structures. New needs and

Opinions will also touch on privacy issues. privacy is

therefore not a one-time task, but a permanent task that is carried out every day

new ones and which need to be reconsidered every day" (p. 36).

The following 48 activity reports of the

Hessian data protection officer. Willi Birkelbach (representative from

June 9, 1971 to June 18, 1975) was also responsible for the second and third

Report. This was followed by the fourth to 19th activity reports, which are attributed to Prof. Dr.

Spiros Simitis (Commissioner from 18 June 1975 to 22 October 1991) re-

go. This was followed by the 20th to 24th activity reports, which Prof. Dr. Winfried

Hassemer (representative from October 22, 1991 to May 30, 1996)

tete, the 25th to 27th activity report, which goes back to Dr. Rainer Hamm (Representative

from May 30, 1996 to June 29, 1999), thereafter the 28th to 31st

Activity report that Prof. Dr. Friedrich von Zezschwitz (representative from

June 29, 1999 to September 30, 2003), and finally the 32

to 49th activity report, which Prof. Dr. Michael Ronellenfitsch (Representative

from October 1, 2003 to February 28, 2021).

The reports of the Hessian data protection officers document

impressive way the history of privacy and data

property rights in Hesse, Germany and Europe. Because data protection in

Hessen has data protection in Germany and in the European Union

influenced and was influenced by the framework conditions

protection developments in Germany and Europe. To

think about the entry into force of the Federal Data Protection Act on 1.

January 1978, to the census judgment of the Federal Constitutional Court of

December 15, 1983, the European Data Protection Directive of October 24

1995, the judgment of the European Court of Justice of March 10, 2010, which the

Independence of data protection supervision demanded, and the date of application

of the General Data Protection Regulation in Germany on May 25, 2018. Hesse

has responded to these developments with five amendments to the Data Protection Act

reacted and additionally adapted several regulations of this law.

Among other things, the reactions to the census verdict by legal

State corrections to improve the protection of fundamental rights and the

Implementation of the data protection directive through improved regulations on

Data protection. Following the judgment of the European Court of Justice, the

Data protection supervision over the public and the non-public area

merged and the data protection supervisory authority as independent

supreme state authority established. In adaptation to the basic data protection

regulation, the Hessian state parliament passed the Hessian data protection and

Freedom of Information Act (HDSIG) of May 3, 2018. The activity reports

of the Hessian Data Protection Authority document all these developments

and its implications for privacy practices and operations

the data protection supervisory authority.

The 50th Activity Report, covering developments in 2021,

describes radically changed relations compared to the first activity report

conditions and many new problem areas and challenges, from

which nobody had any idea 50 years ago - but also

still the fundamental task, individual and societal

Self-determination towards the powers that use data processing,

defend and power imbalances caused by data processing

arise to balance.

However, these tasks have to be fulfilled under completely new circumstances:

The everyday use of globally networked information technology

almost everyone has to have an explosion of personal data

guided. Their information content is so rich that almost every

movement can be recorded and mapped. opinions, values,

Interests, preferences, habits, relationships and movements

appear calculable for almost every person. This amount of information

and new evaluation techniques offer hitherto unimagined possibilities

through data processing the behavior of individuals, social

Predict and influence groups and even states. risks

and restrictions on individual and collective self-determination

are no longer just based on state authorities, but - above all

even - from a private perspective, starting with the nosy neighbor to

to global corporations.

However, the finding from the first activity report still applies:

the dangers to freedom and self-determination are constantly changing,

but that we always counter them in a timely and effective manner

must. “Data protection is therefore not a one-off, but a permanent one

A task that is set anew every day and that applies anew every day

to reconsider." And the data protection-compliant design of the information

technology and the establishment of precautionary and protective measures must

follow, before “constraints have arisen that limit the scope for decision-making

… constrict. Subsequent consideration of data protection

necessary measures would involve a great deal of effort or even

no longer feasible."

The function of the activity report has remained - as in the first activity

The safety report of the Hessian supervisory authority describes and analyzes the

50th activity report of the Hessian data protection officer the current

Practice of data protection in Hesse and the possibilities of supervisory

authority to influence them in favor of fundamental rights and democracy

gain weight.

Prof. Dr. Alexander Rossnagel

XVI

I

First part

50th activity report on data protection

50th activity report on data protection

The Hessian Commissioner for Data Protection and Freedom of Information

New tasks and framework conditions

1. New tasks and general conditions

New tasks and framework conditions

This activity report describes and analyzes data protection

in Hesse in year 4 since the date of application of the basic data protection

regulation on May 25, 2018. Many uncertainties that the new, very

has brought abstract legal frameworks for the practice of data protection,

are overcome. Some issues have now been resolved, others are

still under discussion. In some areas of action arise

first routines. The Europeanization of data protection is progressing

and is increasingly changing the tasks and options for action

data protection supervision.

Jurisprudence of the European Court of Justice

Accordingly, the importance of the European Court of Justice increases and

jurisprudence for the further development of data protection law. He has

some important decisions on data protection and interpretation

of the General Data Protection Regulation and existing

disputes resolved. But every decision focuses on its development

the subject of divorce and yet always contains things that point beyond it

Remarks. As a result, the decisions leave many new questions

which is being disputed and the legal uncertainty for those responsible and

effect supervisory authorities. An example is the “Facebook Fan Page Judgment”

of June 5, 2018 (C-210/16), in which the court found that the

Operators of a "fan page" and Facebook share responsibility for

have the processing of the data of persons who visit the "Fanpage".

Since this judgment, every IT cooperation between two bodies has been asked

whether they share joint responsibility for data processing.

A clear demarcation to separate responsibility, accepted by all

or for order processing has not yet been found. This question has

the Hessian data protection supervisory authority in many individual cases. A

Another example is the "Schrems II judgment" of July 16, 2020 (C-311/18). It

is very meritorious that the court has clarified that the international

level of protection for the protection of fundamental rights must not be undermined. dementia

speaking, given the disproportionate surveillance practices

tics of US intelligence agencies and the absence of any

Legal Protection for US Aliens Commission Decision

to reduce the protection of fundamental rights in favor of undisturbed data exchange,

recognized as contrary to Union law and void. Data transfers are permitted in

the USA only if those responsible take additional protective measures

provide protection against access by the US authorities. Many remember this

However, subsequent questions remained unanswered - e.g. B. which

additional protective measures are required for further data exchange

are and how they are given the enormous dependency on IT

Providers from the USA can be implemented (see item 3). This question

affected many efforts to implement the judgment in Hesse such as

with regard to video conferencing systems (see Section 4). A final example is this

Judgment on the Hessian Petitions Committee of July 9, 2020 (C-272/19). In

the court found that the petitions committee in the Hessian

sian state parliament is subject to the General Data Protection Regulation. It has

but very narrowly limited to the classification of the Petitions Committee and

leaving ambiguity with regard to many other important questions,

such as the question of whether the state parliaments in Germany

fall rich of regulation. A legal opinion could answer this question

I have created for the Hessian state parliament, clarify that the

Data processing to support parliamentary activities

of the state parliament, the state parliament factions and the state parliament members

subject to the General Data Protection Regulation (see Section 10).

European cooperation

The framework conditions for the Hessian data protection supervision

increasingly also determined by the European data protection infrastructure,

of which she is a part. The European Data Protection Board (EDPB) has

meanwhile caught on and many issues in cross-border

Individual questions decided as well as many helpful clarifications in the form of

Recommendations, guidelines and opinions given.

Alongside the European Court of Justice, the committee is the instance that

Union-wide determines how the abstract provisions of the General Data Protection

ordinance are to be understood in practice. Anyone who wants to influence

how data protection will be understood and practiced in the future in the Union,

must be actively involved in the work of the EDPB and its working groups

(see item 5).

In order to ensure uniform implementation of data protection in the Union

len, the General Data Protection Regulation sees a narrow cross-border

cooperation between the supervisory authorities in the Member States. Touches a

Supervisory procedures several Member States, the supervisory authorities should join

agree on the necessary measures. If no agreement is reached

the EDPB makes the final decision in the controversial supervisory procedure.

This collaboration mandated by the General Data Protection Regulation

between the supervisory authorities is therefore proving to be difficult

rigorous and complex because it lacks the necessary cultural basis. All

Member States come from different data protection traditions and

have developed different understandings of data protection supervision.

Therefore, the supervisory authorities very often have to

Common understanding of terms, implementation practices and objectives in the

legal implementation to be negotiated. Then there are the language problems

and the cumbersome procedures of collaboration. Overall, the

General Data Protection Regulation a culture change of cooperation in

ahead of all Member States, which it cannot guarantee itself. Here but

in these collaborative processes it is decided who influences

the future understanding of data protection in the European Union,

intensive participation is necessary (see item 5). However, it is often frustrating

reluctant to watch helplessly as the data protection requirements,

agreed upon by all Union supervisors, for the worldwide

operating technology groups for which it would be most important

do not apply because the competent supervisory authority has these against them

not or insufficiently enforced.

Juridification of the supervisory activity

The General Data Protection Regulation has new legal options for

created opportunities for data subjects and the supervisory authorities who

are to be welcomed in principle, but lead to a stronger juridification of the

carry out supervisory activities. On the one hand, according to Art. 77, each data subject has

DS-GVO the right to lodge a complaint with a supervisory authority if you

is of the opinion that the processing of the personal

Genetic data violates the regulation. Is she with the editing

If you do not agree with your complaint, you can contact the

competent administrative court filed a lawsuit against the legally binding
Submit a decision by the supervisory authority. Both rights strengthen the fundamental
legal protection, because they help individual legal enforcement and
strengthen visual self-determination against powerful data processors
can. The complaints are also a helpful tool for the supervisory authorities
to gain insights into data protection practices. On the other hand
Art. 58 of the General Data Protection Regulation has to the supervisory authorities
stronger powers to enforce data protection in practice.
You can issue orders to non-public responsible persons
data processing and in the event of a violation of data protection regulations
impose heavy fines. Both the new rights of the affected
n persons as well as the greater depth of intervention of the new powers of the
Supervision of the fundamental rights of companies lead to a
increasing number of court cases. The prospect that their

acts are increasingly subject to judicial review,
characterizes their tasks and character in an ever stronger way
their supervisory activities. This becomes more formal and awkward. she will
increasingly shaped by questions of procedural rights, file management,
the burden of proof, the provision of evidence and procedural tactical
ments. Impartial advice and assistance
the responsible persons and the persons concerned, who very quickly
Opponents can become more difficult.
The number of complaints, which has been increasing since 2018, leads to

granting the supervisory authority to the dilemma that the supervisory authority

can only cope with the increasing workload if it means the

uses work rationalization. But this can lead to dissatisfaction with the

people who have lodged a complaint and an increase

of complaints against the supervisory authority. These in turn increase the

workload and jeopardize the regulator's reputation as a fiduciary

the fundamental rights of the data subjects.

Through the juridification of the supervisory activity, the jurisprudence of

increasing importance for data protection at national courts.

However, there are no courts or chambers specializing in data protection

or senates. On the contrary, the individual arbitral tribunals usually decide too seldom

about data protection issues than that they are always included in the special systematics and

methodology of data protection law could be considered. This makes it difficult

consistent jurisprudence in this area. Add to that by

the court decisions at a crucial point again one of national

nal legal concepts come into play. Self

when the federal and state regulators in their conference

(DSK) laboriously found a unified opinion on a legal issue

and also the EDPB are committed to the same view of things throughout Europe

could agree, it is not impossible that a court first

or second instance represents a different legal opinion and the competent

competent supervisory authority is bound by this (see item 6). This makes it difficult

very, to a uniform application of the General Data Protection Regulation

to get into the European Union. Until the Federal Administrative Court

for Germany or the European Court of Justice for the European Union

contribute to a unified view, years can pass

- and then leave the open questions described above.

6

New tasks and framework conditions

cooperation in Germany

Another important framework for exercising supervisory

The task is the increasing need for oversight

to coordinate in Germany. The Hessian supervisory authority is part of the

German data protection supervisory structure. On the one hand, this coordination

necessary because within the Union only in Germany the data protection

supervision is organized on a federal basis and Germany only has one in the EDSA

has voice. The German supervisory authorities must therefore opt for the

Agree on one opinion at a time in the EDPB. On the other hand

is an understanding within Germany necessary on the questions

in which it concerns facts that are not only important for a federal

have land. This is in the non-public area of data processing

the case and in many areas of federal-state cooperation or in the

transnational cooperation. On most privacy issues

a nationwide implementation of data protection law is therefore required.

The supervisory authorities of the federal and state governments work for this

closer together within the framework of the DSK. That always requires more

Votes within the framework of the conference, in the technical working groups

of the conference and in an increasing number of task forces

temporary joint tasks. Third, the supervisory authorities must

who develop common concepts and strategies in order to face each other

to enforce strong data processors. Only if they are together

appear and fight their positions together, they have chances

advance data protection in Germany. The most important

ments therefore fall within the bodies of the DSK. Accordingly, in

The importance of working in these bodies within the framework of supervisory activities

and is thus increasingly changing the work tasks of employees in

the supervisory authority.

In view of the need for increasing cooperation, the DSK has one

Working group "DSK 2.0" founded, which the current cooperation of

independent federal and state data protection supervisory authorities

including the working methods of the DSK and, if necessary,

should develop proposals for a redesign. In addition to their semi-annual

In addition to the two-day conferences, the DSK now holds around four

one-day interim conferences. She also has a weekly

chen Jour fixe set up to mutually in everyday questions

to inform and vote.

corona pandemic

External influences also shaped supervisory activities in the reporting period –

above all the corona pandemic. On the one hand, it forced them to maintain

of the ability of the supervisory authority to work in a supervisory capacity

pandemic mode. The employees mainly worked in the home office

and strict hygiene conditions prevailed in the office. You could

significantly fewer on-site external oversight activities

more dependent on and using telephone contacts and video conferences

more written procedures. On the other hand, the pandemic generated

Measures to combat them and which are always changing rapidly -

the legal regulations for new supervisory tasks. examples were

the data processing in the organization of vaccination appointments, in the context

of testing procedures, in contact tracing, in maintenance

the functions of day-care centres, schools and universities and the

Processing of disease and immunity status data in work

circumstances (see item 2).

Finally, in the reporting period, the supervisory authority was faced with the task of

the exceptions to data protection regulations and the temporary ones

Toleration of conditions that do not comply with data protection regulations, which they had at the beginning of the

Corona pandemic and during the first lockdown in spring 2020

to cope with the emergency situation at the time, back to the

adapt to data protection requirements. To this end, she has

for example when using video conferencing systems – together with

searched for those responsible for constructive corrections and those for

necessary time for the conversion (see item 4).

Supervisory activity in individual areas

The main outcome of oversight activity in 2021 is that for the

Data protection in Hesse no serious violations were found

- in complete contrast to the development in Germany or in the world. There

technical, economic and political developments can be observed,

which are increasingly endangering the personal rights of the persons concerned.

For Hesse, on the other hand, it should be noted that data protection in the reporting period

accepted and not fundamentally questioned.

Nevertheless, in many areas the requirements of the General Data Protection

regulation is still not sufficiently implemented, leading to complaints,

require the intervention of the data protection supervisory authority as well as orders and

enforcement actions on a case-by-case basis. The digitization of many tasks

and activities creates additional obligations for those responsible

additional requirements and requires additional attention.

8th

New tasks and framework conditions

Large companies and administrations can cope with this to some extent.

This can be small and medium-sized businesses or communities but easily

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

not lead to a reduction in data protection. Therefore strives

my authority again and again together with those responsible

to find privacy-friendly solutions that also protect privacy in small

and medium-sized companies as well as in small communities.

Between the developments in data processing in the field of security

security and criminal prosecution authorities as well as the protection of the constitution and

the requirements of data protection exists because of the controversy

Tasks always a tense relationship, but only in the reporting period

in individual cases has led to demands from the data protection supervisory authority

the authorities concerned have complied (see item 7).

In the administrative authorities of the state and the municipalities,

time designed and planned large and demanding digitization projects

and implemented. These are for administration in a digitized world

indispensable, but create challenges for the in many places

Protection of personal rights and self-determination of citizens

and citizens. It is therefore necessary for the data protection supervisory authority to contact

involved in these digitization projects and with constructive advice for

contributes to compliance with data protection requirements (see Section 8).

Schools and universities were particularly affected in the reporting period

through strong developments towards more digitization of teaching and examinations

activities, teaching and learning. In addition to the use of video conferencing systems

(see item 4) this concerned e.g. B. equipment rentals, learning aids and remote examinations,

for which supervisory notices were required but also welcomed.

In the school sector, the supervisory authority accompanied the developments of the

Hessian school portal and advised the Ministry of Education with regard to the

data protection regulations of the new school law (item 9).

The digitization of work means that in employment relationships

monitors the performance and behavior of employees more and more intensively

can be. It is important here that these possibilities are only used in different

proportionate scope and in compliance with the personal rights of the

affected employees are used. In that regard, my

authority to intervene to correct this in several cases (see item 11).

On the Internet, the use of cookies is often necessary to enable users

to recognize them and offer them the services they want. Still

more often, however, they are used to track the surfing behavior of users,

to create profiles about you and to record your interests, preferences, habits

to recognize behaviors and relationships and – in particular

for advertising measures - to influence. For the self-determination of

To protect users, this is largely only permissible if they are in the

have consented to the use of cookies. To this end tried almost

every Internet provider in the form of "cookie banners" such consent

to catch up Due to the constant confrontation with such "cookie banners"

is a sensible measure to protect self-determination

just annoying in everyday life. To this end, the telecommunications telemedia

Data Protection Act (TTDSG) on December 1, 2021 new regulations

created (see item 12).

The topic of video surveillance remains a "long-running issue" for data protection

watch. Due to advances in video technology and an increasing

Video surveillance by the police takes away the need for precaution and protection

and security agencies, but even more so by private companies

and in the neighborhood relationship to. This compels the data protection supervisory authority

again and again to notices and correction orders issued by authorities

accepted, but sometimes passed through to private

must be set (see item 13).

There were many complaints in the private sector, e.g. B.

with questions of the rights of data subjects, in particular with the

entitlement to the future (see Section 14), the processing of address data

Credit agencies and collection agencies (see Section 15) and queries from

Vehicle owner data to enforce contractual penalties

(see para. 16), which the employees of my authorities had to pursue.

In healthcare, data protection oversight was heavily impacted by data

processing in the context of the corona pandemic (see item 2). But also

Problems such as maintaining patient confidentiality and transmission

of patient data and the storage of patient files

be resolved. (see item 17).

Of particular note is the increase in cybercrime, which is also

has an impact on data protection. Criminals get targeted

through phishing and other forms of social engineering

IT systems of those responsible. In other cases they use known

vulnerabilities that have become apparent in certain software systems and are penetrating

through these into IT systems. Their malware spreads to everyone

Share the systems and extract – sometimes very large amounts of – data.

To blackmail those responsible, they download encryption software

after, encrypt (all) data and provide the keys to decrypt

against large sums of money. In other cases, they publish at

Those responsible withdraw data from the Darknet and threaten with more

Releases when no ransom is paid. These increasing

New tasks and framework conditions

Forms of cybercrime require stronger preventive measures,

quick reactions to known vulnerabilities and the

repeated information for all employees about the possibilities of attack as well as

the measures to avoid them (see paragraph 18).

Data protection during the corona pandemic

2. Data protection during the corona pandemic

Data protection during the corona pandemic

In the reporting period, too, data protection supervision was heavily dependent on the

effects of the corona pandemic. For one, brought the fight

the processing of personal data required by the pandemic many new ones

Challenges for data protection. These were both from always

again new regulations adapted to the respective pandemic situation

as well as by many reactions of the addressees of these regulations,

which led to constantly new forms and contents of data processing.

On the other hand, the work of my authority was also made more difficult by the fact that

its employees carry out their supervisory activities mainly from

home office had to provide.

2.1

Was data protection an obstacle in the fight against the pandemic?

Despite claims to the contrary, data protection during the reporting period

not an obstacle to fighting the corona pandemic, but one

effective support because he is responsible for the trust in the state corona

Politics and the individual measures taken by government agencies are an important

suspension was.

In many editorials, talk shows and political speeches, online posts and

Reader comments claim that data protection has the effective combat

of the pandemic. Therefore, data protection must be cut back

become. This opinion is even held in scientific circles.

These claims can even be found in the Federal Government's Ethics Council.

Its chairwoman, Prof. Dr. Alena Buyx, announces the privacy

is the only fundamental right that has not held back in the pandemic

must. With less data protection would be in the fight against the pandemic

been able to achieve better results (https://www.zdf.de/nachrichten/

digital/coronavirus-warnapp-datenschutz--kritik-100.html). The former

Minister of State for Culture and current Deputy Chair of the Ethics Council

Prof. Dr. Julian Nida-Rümelin has this idea with the claim

taken to the extreme: Germany has strict data protection in the

Corona crisis paid for with 70,000 deaths. From this assertion derives

he rejects the political demand for stricter restrictions on data protection

(Zeit-Online 03/26/2021).

These claims complicate privacy, but don't hold anyone up

fact check. In fact, the opposite is true: data protection has evolved

shown to be very flexible in relation to the requirements of fighting the pandemic

and is even an important prerequisite for combating the

Corona virus succeeds.

Data protection law is very flexible when it comes to health risks

and expressly permits data processing to combat the pandemic.

The data processing required for this is in accordance with Article 6 Paragraph 1 Subparagraph 1 lit

DS-GVO expressly permitted if it is necessary to "vital

interests". Mentions as an example of such an interest

the DS-GVO in recital 46 expressly the "monitoring of

epidemics". Data protection law therefore permits all data processing

necessary to fight the pandemic. If vaccination, testing and

Contact tracing didn't work as expected, so this isn't it

the fault of data protection law.

Data protection has not caused any deaths, nor is it in the Corona crisis

as the only fundamental right to remain unrestricted. Rather, they have

Data protection supervisory authorities have great flexibility in this special situation

shown to save lives. Data protection is therefore the management of the

not against the Corona crisis. Rather, he supports them: in a western way

Democracy like in Germany can only successfully fight the pandemic

be when the citizens trust the institutions of the state.

A key trust factor is data protection. only when they experience

that their fundamental rights, one of which is data protection, are in good hands

are and can be maintained even in the case of drastic measures

they develop the necessary trust.

What was the relationship between data protection and the fight against pandemics in the

reference period actually? In the first lockdown in spring 2020, many

Those responsible grabbed the next best digital opportunity to

to maintain social and professional life despite the distance requirement.

Privacy was not the priority. The data protection supervisory

many of the video conferencing systems used could not

approve, but have tolerated them to this day or have not objected to them, for example

about the education of the children in the schools, the offer of courses

events in universities, holding meetings

in companies and authorities as well as the offer of events in the

To continue to enable cultural activities even during the pandemic (see Section 4).

The handling of the usually hasty relocation of work was similar

to the home office and enabling mobile working. In many

cases, the conditions at home did not meet the requirements

to the secure handling of personal data, nor were the

technical and organizational procedures for connecting home offices

to the data processing systems of companies and authorities

State-of-the-art requirements. Of blatant exceptions

Apart from the monitoring of employees (see Section 10.2), these

Circumstances at least not complained at first.

Another example of a restriction of data protection is the

compulsion, e.g. B. in restaurants, shops and events its con-

having to store clock data. This deep intervention in the informational

self-determination, that all citizens have a state

follow-up of stays and visits to these places and meeting with

other people have to put up with is for contact tracing through

necessary for the health authorities and was made constructive by data protection

accompanied (see Sections 2.2 and 2.3). The same applies to the apps used for con-

clock tracking were used instead of paper lists. Also theirs

Risks to fundamental rights have been identified by the data protection supervisory authorities

accepted. Despite many shortcomings, this digitization step was

Data protection supported and continuously improved (see Section 2.2). Also the

Data processing in vaccination appointment management is the responsibility of data protection supervision

not blocked despite deficits.

Another example of backing down on privacy versus

the necessities of fighting the pandemic was data processing

to protect the workplace. The collection of to monitor the

Worker immunity data required by 3G rule in the workplace

by their employers or employers was a deep intervention in the

employee data protection (see Section 2.6). Nevertheless, the regulators

the emergence of these regulations and their implementation in the workplace

constructively supported.

In the coronavirus protection regulations of the countries, the rights of

affected persons completely suspended in order to apply the con-

not to impede clock tracking. The people concerned could

thereby e.g. B. do not request information about the processing of their data,
do not enforce any correction of incorrect data and no deletion
request more necessary data. Only when I was constructive in Hesse
pointed out that this limitation for contact tracing
superfluous, it was included in the next version of the coronavirus protection
ordinances repealed (see Section 2.5).
The objective of the Corona-Warn-App does not come from data protection,
but the desire of health policy, in addition to the existing funds
to establish an additional anonymous instrument for the health authorities,
fight infections. Data protection considerations only came into play afterwards
game when it came to how to do this. France, Australia
and Norway have chosen a solution that centralizes the data of those infected

stores - with the result that these attempts at the lack of trust
of potential users have failed. France now has its
App overtakes and uses it like the German app. In Germany he has
decentralized approach that does not reveal the infected person's identification data,
generates trust. He did at least until the end of the reporting period
led to about 40 million people using the app and over
1.7 million infected approx. 10 million contact persons warned and with it
have prevented millions of further infections (https://www.bundesregierung.
de/breg-de/suche/cwa-40-mio-downloads-1994916).
The data protection supervisory authorities have also approved the further expansion of the
Features of the app supported.

The experience with data protection in the pandemic shows: A re-
tightening of data protection law is not necessary. On the contrary – the
Limiting the fundamental right to data protection would be counterproductive. In
of the crisis, data protection has flexibility and protection at the same time
proven. It is the basis for the trust of those affected and the
condition to motivate them to participate.
After the reporting period, the second year of the pandemic, rou-
tine in the fight against the corona virus and the first
spontaneous reactions and remedial measures in dealing with the new ones
Challenges could be reconsidered, it was necessary
to adapt the solutions found to the data protection regulations
and restore lawful conditions. Also the data protection had
suffered long enough from the corona pandemic.

2.2 Data protection requirements for contact tracing

Already in the course of the previous reporting period (see 49.
ity report, Section 11.6) was the corona-related contact recording
focus of my work. The data protection issues in the reporting period
to work on was particularly difficult because the regulations for contact
tracking were repeatedly adapted to the pandemic.
For this reason, too, I received various inquiries and complaints
on the subject of contact tracing.

I. Frequent change of legal bases

The regulations on contact data collection were throughout the year
subject to frequent changes, which often only apply for a short period of time. The

Data protection during the corona pandemic

Application in practice was therefore particularly important for the obligated

special challenge.

After areas not serving the basic needs of the population

of economic life in the winter months was shut down due to corona

hairdressers were initially allowed to reopen from March 1, 2021.

In addition to compliance with various hygiene measures, the operators

and operators according to § 6 paragraph 3 of the Corona contact and operating

Restriction Ordinance (CoKoBeV, valid from March 1, 2021, GVBl. p. 142)

obliged to record the contact details of customers.

From March 8, 2021, retail outlets in the

Within the framework of a fixed appointment and in compliance with various

Open hygiene rules ("Click and Meet"). Here, too, according to § 3a para. 1

S. 2 No. 22 CoKoBeV (valid from March 8, 2021, GVBl. S. 142) the contact

customer data is recorded. The regulation was correct

those for hairdressers. The only exceptions were

the points of sale serving the basic needs of the population

§ 3a paragraph 1 sentence 2 no. 1-21 CoKoBeV (food retail, pharmacies,

drugstores, etc.). In the case of mixed goods stores, according to § 3a para. 1 sentence 3 CoKoBeV

the focus in the range is crucial.

From April 26, 2021, the relevant legal basis was at the

Retail stores depending on the level of incidence. The

Hessian regulations of the CoKoBeV only applied up to an incidence

from 100 infected people to 100,000 inhabitants. If a county or a

county-level city had an incidence of 100 for three consecutive days

exceeded, according to § 28b IfSG from the day after next

the nationwide regulations of the Infection Protection Act (IfSG,

BGBl. I p. 802).

The Hessian regulation on the collection of contact details in retail

was then repealed on May 17, 2021 (CoKoBeV, valid from May 17

2021, GVBl. p. 254). Contact data collection in retail was now-

more only from an incidence of 100 according to the Infection Protection Act

regulated. With an incidence of up to 150, according to § 28b para. 1 sentence 1 no. 4 IfSG

all shops for individual customers after prior appointment booking

open for a fixed limited period, provided the contact details

of the customers were collected.

Also from May 17, 2021, restaurants, cafés or similar were allowed to open. again one

Offer on-site consumption (initially only for outdoor gastronomy). Included

had to the contact details of the guests are also recorded. the rule

4 para. 1 sentence 3 no. 3 CoKoBeV largely corresponded to that

for hairdressers and retailers.

The contact data was collected from June 25, 2021 as part of the

lifting of the CoKoBeV and the enactment of the ordinance for the protection of

population against infection with the corona virus SARS-CoV 2 (corona virus

Protection Ordinance - CoSchuV - Valid from June 25, 2021, GVBl. p. 282)

newly regulated. While the contact data collection so far in the respective

Standard for the corresponding industry was regulated, this was now

"Before the bracket" and in § 4 CoSchuV in the first part (general

regulations). In Part Two (Special Provisions) was for

individual areas (restaurants, cultural establishments, etc.) on the contact data collection

according to § 4 CoSchuV. § 4 CoSchuV itself referred again

to the federal regulation of § 28a para. 4 IfSG (Federal Law Gazette I p. 370) and supplemented

these by a few stipulations.

From June 25, 2021, the CoSchuV initially obliged various companies

operators and event organizers for the

clock data acquisition:

– Trade fairs and cultural events (theatre, opera, cinema and concerts)

according to § 16 CoSchuV,

- Fitness studios and similar facilities according to § 18 paragraph 2 CoSchuV,

Casinos, amusement arcades and similar establishments according to Section 18 (4).

CoSchuV, restaurants, canteens,

– Hotels, ice cream parlors, ice cream parlors and other businesses in the offer of the

Consumption on site according to § 22 CoSchuV,

– overnight accommodation according to § 23 CoSchuV,

- Dance halls, discotheques, clubs and similar facilities according to § 24

CoSchuV,

– Service companies in the field of body care (hairdressers and

similar) according to § 25 CoSchuV as well as prostitution sites and the like

Facilities according to § 26 CoSchuV.

After the information obligation of Art. 13 DS-GVO and the data subjects

Rights of Art. 15, 18 and 20 DS-GVO according to § 4 No. 3 CoSchuV (or according to

the respective regulation of the CoKoBeV) since the beginning of the corona pandemic

were excluded, this exclusion was due to my intervention

deleted from August 19, 2021 (CoSchuV, GVBl. p. 386) (see Section 2.5).

Since then, the rights of those affected have been part of the contact data collection

applicable without restriction.

Since September 16, 2021 (CoSchuV, GVBl. p. 571) were large parts

of the formerly obligated parties are excluded from contact data collection

(especially restaurants, hairdressers, fitness studios and cultural institutions).

However, dance halls, discotheques, clubs and

Similar facilities according to § 24 CoSchuV as well as prostitution sites and

similar facilities according to § 26 CoSchuV. According to § 27 paragraph 2 CoSchuV

the local competent authorities were also given the power to

according to §§ 28 and 28a IfSG also beyond the CoSchuV

arrange measures. Thus, since then at the municipal level

also a contact data collection for other facilities (restaurants,

hairdressers, etc.) can be arranged.

The CoSchuV was re-enacted on November 25, 2021 (GVBl. p. 742). The

Regulations on the collection of contact data were only editorial

Changes, but the content remained unchanged.

On December 16, 2021, Section 4 CoSchuV was supplemented by sentence 2.

Thereafter, contact data collection was not required if the person

whose data would be recorded in the Corona warning app of the Robert

QR code registration included with the Koch Institute.

The following legal situation applied at the end of the reporting period: The recording

The contact data is based on Article 6 Paragraph 1 Subparagraph 1 lit. c GDPR i. V. m.

§ 4 CoSchuV and the respective provision of the CoSchuV (e.g. § 24 CoSchuV

for discotheques).

Current information on the current regulations for contact data

I have always made the version available on my website.

II. Contact Information Collection Requirements

If the corresponding standard of the CoSchuV does not record contact data

provided (more) for the respective company or event, no

ne contact details are collected. Due to the multiple changes in the

Regulation during the reporting period and related

Due to legal uncertainty, this requirement was not consistently complied with (see

Section 2.3).

The contact details were surname, first name, address and telephone number

or collect email address. Other data (e.g. a signature)

were not allowed to be raised. Sometimes the signature was

declarations of consent or similar required. Since the contact data collection however

is legally standardized, such "consent" could not be obtained. also is

the production of copies of identity cards or negative evidence

(Proof of vaccination, proof of recovery or proof of test, cf. § 3 CoSchuV)

inadmissible. These contain significantly more personal data (in the case of

Negative evidence also health data within the meaning of Art. 9 DS-GVO)

than may be levied by law (see Section 2.3). The contact details were

according to § 4 S. 1 No. 1 CoSchuV to be given completely and truthfully.

Obviously false information (pseudonyms, "funny names") did not meet

the requirements of the CoSchuV.

In the reporting period, it happened again and again that contact details for other

whose purposes have been used (e.g. advertising or other

communication with the recorded). Since the contact details according to § 28a para. 4

S. 3 IfSG may not be used for any purpose other than them

upon request to the bodies responsible for collecting the data

however, such use is unlawful.

The lack of collection of contact data as well as untrue or incomplete

According to § 30 CoSchuV i. V. m. § 73 Abs. 1a Nr. 24 IfSG a

An administrative offense punishable by a fine of up to

can be fined up to 25,000 euros.

The collection and processing of contact data should be carried out in accordance with Section 4 Sentence 1 No. 2

CoSchuV in electronic form if possible (e.g. using a QR

codes or an app). In addition to the electronic form, however, there is also a

to offer another type of detection. If the contact details are on paper

were recorded, it was important to ensure that the contact details were not made public

accessible and visible to other people. The contact

were to be recorded manually by the staff or by the guests, customers

dinners, customers, participants on individual sheets

to enter. Because of violations of these obligations, it also came

repeatedly to complaints during the reporting period (see Section 2.3).

When collecting the contact data, those responsible had already

special to inform (e.g. by means of a clearly visible notice

on site and on the entry forms) that the contact data is recorded

for the purpose of tracking and interrupting chains of infection

the corona virus SARS-CoV-2 on the basis of Article 6 Paragraph 1 Subparagraph 1

lit. c GDPR i. V. m. § 4 CoSchuV and the respective provision of the CoSchuV

(e.g. § 24 CoSchuV for discotheques).

According to Section 28a Paragraph 4 Sentence 2 IfSG, those responsible had to ensure that

knowledge of the recorded data by unauthorized persons is excluded

is. In some cases that came to my knowledge, this requirement was not met

consistently complied with (see Section 2.3). Those responsible should use the recorded

Data in a locked cupboard, safe or similar if possible

kept at the place of collection. As few as possible should do this

people have access. The mere filing of the registration forms in one

(File) folders were not sufficient if they were not kept securely.

The contact details were according to § 28 paragraph 1 CoSchuV and § 28a paragraph 4 sentence 4

and 5 IfSG upon request only to the health authorities (in urgent cases the

local regulatory authorities). They weren't allowed to go to anyone else

bodies are transmitted - not even to the police or public prosecutor's office.

The contact details were immediately available in accordance with Section 28a Paragraph 4 Sentence 3 IfSG

Four weeks after collection, securely and in compliance with data protection

delete or destroy. Contact details recorded on paper were not allowed

disposed of directly in the paper waste, but had to be filed in a

shredders or paper shredders are destroyed so that third parties do not

could gain knowledge of these. Also with regard to these requirements

several complaints reached me, according to which contact details (clearly)

were kept longer than permitted by law (see Section 2.3).

2.3

Violations of contact tracing rules

Some concrete examples from the practice of the reporting year show the

data protection problems of contact tracing that have arisen. Me

received many complaints that the publicly available interpretation of the

leading contact lists as content. In addition, the improper

Custody and inadmissibly long storage of the contact data was reprimanded.

In these cases, I have taken measures to protect the data protection

prevent legal violations.

On July 5, 2021, I received a complaint against a pedal

boat rental. This had the user for contact tracking

provision of the Luca app. In the event of non-use of the Luca app

copies of the customers' ID cards were made. At the ticket office

the sales hatch was open continuously from left to right, as well

the front door was wide open. Near the sales counter

a commercial copier. Copies of the

ID cards of previous customers. The top copy visibly showed the

front of an identity card. The ticket office was not

hend occupied, so that the copies neither from unauthorized disclosure nor before

loss were protected. Although the operator of the pedal boat rental tried

and responsible for the data processing of his at that time

point according to the statutory obligation to record contact data

§ 4 CoSchuV (dated June 22, 2021) i. V. m. § 28a Abs. 4 IfSG.

However, it was questionable whether there was a legal basis in the present case

for the production of ID card copies. According to Art. 6 DS-GVO, the

Processing is only lawful if at least one of the reasons listed in Art. 6 Para. 1

Subsection 1 lit. a - f DS-GVO is fulfilled. The CoSchuV

ordered the collection of name, address and

phone number or email address. Accordingly, Article 6 Paragraph 1 Subparagraph 1
lit. c GDPR relevant. The CoSchuV represents a legal obligation
which the person responsible must fulfill.
On the identity card, however, in addition to body size
ß and eye color also the place of birth and the identity card number
specified. Due to the large number of those noted on the identity card
personal data there is a high risk of misuse. This
Personal data is not recorded by the CoSchuV. There
none of the other facts of Art. 6 DS-GVO are relevant either,
lacks a legal basis. Consequently, the preparation of
ID card copies not permitted.
Even if there is a legal basis for data processing
would, recording by means of ID card copies would still be inappropriate
been casual, as this violates the principle of "data minimization"
according to Art. 5 Para. 1 lit. c GDPR would be violated. After this, per-
Personal data "adequate and relevant for the purpose and on
be limited to what is necessary for the purposes of the processing".
This central principle of the GDPR means a generally qualitative one
and quantitative limitation of the processing of personal data.
The word "minimization" also indicates the greatest possible extent
limitation. The production of ID card copies does not constitute a
economical processing of personal data and is fundamental
to be considered inadmissible. There are exceptions to this principle,
such as Section 8 Paragraph 2 of the Money Laundering Act or Section 95 Paragraph 4 Clause 3
Telecommunications Act a. F. clarify. In the present case
however, this is no such exception.

The open storage of ID card copies also represents a

Violation of § 28a Para. 4 S. 2 IfSG, after those responsible

have to ensure that the recorded data is acknowledged by

unauthorized is excluded.

As a result, the person responsible was first instructed by me to

to refrain from making copies of ID cards. He then got over

I explained the legal framework. Should therefore the

Customers do not provide their contact information in electronic form (e.g. by means of a

QR codes or an app) recorded, so was another

type of capture to offer. The contact details could be handwritten

are recorded by the staff or the guests, customers or

Participants could fill out individual sheets

be presented. In addition, the person responsible was instructed to

Contact details in a locked cupboard, safe or similar

keep safe depository.

On July 21, 2021, I received a complaint against a re-

restaurant operation. The complaint was made by the district committee

of a district in Hesse. The regulatory authority of the local

The district committee carried out compliance checks in catering establishments

the CoSchuV through. The restaurant concerned was found to have

the contact sheets of the guests since October/November 2020

were kept and thus contrary to § 4 CoSchuV i. V. m. § 28a paragraph 4

S. 3 IfSG not deleted after one month or properly disposed of

had been. Upon request, the restaurant operator and Ver-

responsible for storing the contact data since the beginning of the obligation to
contact data collection. He was instructed under the supervision of the
authority to destroy the contact details.
On September 24, 2021, I received a complaint against
set up contact data collection in a thermal bath company. Such
Contact data collection was neither in § 4 CoSchuV nor in § 28a paragraph 4 IfSG
required. Since there was therefore no legal basis
the local authorities, however, according to § 27 para. 2 CoSchuV i. V. m. §§ 28
and 28a IfSG, measures that go beyond the applicable regulation
I asked the thermal baths to comment.
The Respondent could not find any legal basis for this
be mentioned, according to which the contact data was justified
were. In consultation with the local regulatory authority, the contact
Data collection stopped immediately and the data already collected
destroyed.
A number of other cases mainly concerned restaurants. The CoSchuV
of June 22, 2021 in the version valid from September 16, 2021
for restaurants (defined as: "Restaurants in the sense of the Hessian
Site Act of March 28, 2012 (GVBl. p. 50), last amended by
Law of December 15, 2016 (GVBl. p. 294), canteens, hotels, ice cream parlors,
Ice cream parlors and other businesses") no longer records contact details. In
the earlier versions was a contact data collection in § 22 CoSchuV
standardized. Due to the lack of legal bases reached me
multiple submissions, one going beyond September 16, 2021
had the content of collecting contact data. Also here were from me
Measures taken to stop further recording. The data

were then sent for destruction. With one of these entries

became another in addition to the registration without a legal basis

violation detected. The guests of the restaurant were asked to

Enter data into a form on a provided laptop. here

could in the individual input fields via auto-completion the

Data of all customers who had registered there in the past,

be retrieved. Here, too, the restaurant operator was instructed

to stop the collection of contact data, to delete existing data and

in the event of a renewed obligation to record contact data, this data protection

to perform compliantly.

Another focus of my supervisory work was leadership

from open lists. For example, I received one on July 5, 2021

Complaint directed against a hairdressing salon. This one was after

of the CoSchuV from June 25, 2021 to July 21, 2021

Service company according to § 25 Abs. 2 CoSchuV for the collection of

contact details required. The hair salon came up with contact data collection

after, however, provided a public and therefore for everyone to record

available list. This behavior was also part of the

complaint addressed to me. Publicly visible lists, the contact details

contained, according to Art. 5 Para. 1 lit. f GDPR a data protection

breach of law. For this reason, the Respondent of

instructed me to stop collecting from a public list.

2.4

Data collection from travel returnees by day-care centers

After the end of the holiday season, daycare centers were not allowed to provide any information about this
Stay in SARS-CoV-2 risk areas and possibly subsequent
ongoing quarantine and COVID symptoms and test results
query to check the returnees. A legal basis for
these data collections were not available. The day-care centers are for such queries
not responsible. However, you can contact the parents by means of information letters
or talking about their legal obligations after entry
inform abroad.

Due to an input, I became aware of a form that some
Kitas should use to query information from "travel returnees".
The provider of these day-care centers provided them with a form before the 2021 summer holidays
lar to query numerous personal data of parents and children
ready. The form contains information about the foreign travel country,
a quarantine and the typical COVID symptoms as well as for the digital
Confirmation of entry and asked for a negative test result. The
Respondents were informed that they would take care of the children after the holidays
is only possible after submitting the completed form.

24

Data protection during the corona pandemic

There was no legal basis for the mandatory collection and
Processing of the data specified in the form by the day care centers. Both
Test results and the COVID symptoms are according to Art. 9
Para. 1 DS-GVO specially protected health data, the processing of which
only under the strict requirements of Art. 9 Para. 2 DS-GVO
is allowed. These conditions were not met.

The day-care centers are not responsible for collecting this sensitive data. For the
Verification of entry registrations and test certificates are those with the
responsible for police control of cross-border traffic
Authorities responsible (§ 7 Para. 2 of the Coronavirus Entry Ordinance). The
Requesting information from travelers returning from risk areas, in particular
Special on COVID symptoms and quarantines is the responsibility
the health authorities.
If necessary, the voluntary disclosure of the data could be
agreement of the persons concerned. As data protection compliant
However, an information letter on the obligations for
Returning travelers and the possibility of an interview offer have proven effective.
I already had this assessment in 2020 in a post on mine
Website published, in which also the comparable reflections on
School area are shown. The website post is under the following
Link available: https://datenschutz.hessen.de/datenschutz/gesundheits-und-
social affairs/healthcare/what-schools-and-day-care-centres.
In the further course I contacted the operator of the day-care centers and
informed that the intended data collection is not permitted.
According to the carrier, the daycare centers are still during the summer holidays
been informed that the corresponding form from data
may not be used for copyright reasons. The forbidden ones
Data collection was thus stopped due to my intervention.

2.5 Publication of vaccination data on social networks

There is a risk that those responsible will violate the provisions of the
violate data protection law if they are related to the Corona

Pandemic information on the health status of their employees in

publish on social networks.

During the reporting period, I received a complaint concerning a

contribution (so-called post) in a regional chat group. had in the post

the management of a company announces that all employees

must be vaccinated against Covid-19. The management named though

none of the employees by name. Because of the regional connection

but without much effort it is possible to draw conclusions about the identity of the

attract employees of the company.

I took the complaint as an opportunity to contact the person responsible

to listen to the process. He took this as an opportunity to write the corresponding post

to delete. To process the vaccination status of the employees concerned

he stated that a time off work for the Covid-19 vaccination

had been granted, so that the employees through the exercise

the time off work would have voluntarily disclosed the vaccination status. The

Employees were informed about the intended mail and

had given their consent to this orally.

With regard to the case described, it must be taken into account that two

data processing operations are to be distinguished from one another: On the one hand

the question of the legality of the collection of vaccination data arises

the employer (querying the vaccination status), on the other hand is the disclosure

the vaccination status of employees in a social network (post of

to evaluate vaccination status).

Inquiring about the vaccination status of employees is one

"Processing of personal data". The terms "personal

Data" and "processing" are defined in Art. 4 No. 1 and 2 DS-GVO.

Art. 4 No. 1 and 2 GDPR

For the purposes of this Regulation, the term means:

1.

"Personal Data" means any information relating to an identified or

identifiable natural person (hereinafter "data subject"); as

a natural person is considered to be identifiable, who directly or indirectly, in particular

particular by association with an identifier such as a name, an identification number,

to location data, to an online identifier or to one or more special

characteristics expressing the physical, physiological, genetic, psychological,

economic, cultural or social identity of this natural person,

can be identified;

"Processing" any carried out with or without the aid of automated procedures

Process or any such series of processes in connection with personal data

Data such as collection, recording, organization, ordering, storage,

the adaptation or modification, the reading, the query, the use, the

Disclosure by transmission, dissemination or any other form of making available

development, matching or association, restriction, deletion or

Destruction;

2.

(...)

The verbal query of the vaccination status is in accordance with Art. 2 Para. 1 DS-GVO

basically outside the scope of the GDPR, since insofar

neither a file-bound nor an automated processing takes place

is. In the employment relationship, however, the regulation of § 26 paragraph 7

BDSG to take into account.

§ 26 paragraph 7 BDSG

(...)

(7) Paragraphs 1 to 6 shall also apply if personal data, including

special categories of personal data processed by employees,

without being stored or intended to be stored in a file system.

The regulation expands the regulations of employee data protection

any form of processing of personal data. Also the oral

Inquiry about the vaccination or convalescence status by the employer

therefore represents processing that meets the requirements of data protection law

must suffice.

It must also be taken into account that information about an in

vaccination against Covid-19 to prevent health

within the meaning of Art. 4 No. 15 GDPR and thus special categories

personal data within the meaning of Art. 9 Para. 1 DS-GVO.

Art. 4 No. 15 GDPR

For the purposes of this Regulation, the term means

(...)

15. “Health Information” personal information relating to physical or

mental health of an individual, including the provision of

Health services, obtain and from which information about their

state of health;

(...)

Art. 9 Para. 1 GDPR

The processing of personal data revealing racial and ethnic

Origin, political opinions, religious or philosophical beliefs or

union membership, as well as the processing of genetic

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

Health data or data on sex life or sexual orientation

natural person is prohibited.

The processing of special categories of personal data is

according to the wording of Art. 9 Para. 1 DS-GVO. Art. 9 Para. 2 GDPR

sees exceptions to this principle in the finally defined

cases of lit. a to j. Article 9 (2) is particularly relevant here

lit. b GDPR i. V. m. § 26 paragraph 3 BDSG.

§ 26 paragraph 3 BDSG

(...)

(3) 1Deviating from Article 9 paragraph 1 of Regulation (EU) 2016/679 is the processing

special categories of personal data within the meaning of Article 9 paragraph 1 of

Regulation (EU) 2016/679 for employment purposes if they

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

social security and social protection law is required and not a reason

to assume that the legitimate interest of the data subject in the

Exclusion of processing prevails. 2Paragraph 2 also applies to the consent of special

categories of personal data; the consent must be expressly given

obtain this data. 3§ 22 paragraph 2 applies accordingly.

The post "all employees are vaccinated against Covid-19" also fulfills the

terms "personal data" and "processing". Although the employer

in the post did not name any employees, it is about

personal data within the meaning of the GDPR. As previously shown, are

personal data any information relating to an identified

or identifiable natural person. Since about the data of

employer was able to identify the employees, it acted

are therefore personal data within the meaning of Art. 4 No. 1 DS-GVO.

The requirements of Art. 4 No. 2 DS-GVO were also met, since under

the term processing also includes the disclosure of personal data

falls. Disclosure is to be understood in such a way that third parties have the opportunity

is procured, the personal data of data subjects

to take notice. The regional group in which the post is published

had around 12,500 at the time the post was published

members.

Employees can only consent to the processing of their vaccination data voluntarily

leagues. If the requirements of § 26 Para. 2 BDSG are observed

Employees consent to the processing of their personal data.

According to Section 26 (3) sentence 2 BDSG, this also applies to the processing of special data

Categories of Personal Data. The requirements for a legal

effective consent to data processing in the employment relationship

are regulated in § 26 Para. 2 BDSG.

28

Data protection during the corona pandemic

§ 26 paragraph 2 BDSG

(2) 1If the personal data of employees is processed on the basis

of consent, for the assessment of the voluntary nature of the consent, in particular

or the dependency of the employed person in the employment relationship

as well as the circumstances under which the consent was given.

2Voluntariness can exist in particular if a legal

or economic advantage is achieved or employers and employees

pursue parallel interests. 3The consent must be in writing or electronically

take place, unless another form is appropriate due to special circumstances.

4The employer has informed the employed person about the purpose of the data processing and

about your right of withdrawal according to Article 7 (3) of Regulation (EU) 2016/679 in text form

to clear up.

The decisive factor for the question of whether the consent was lawful is therefore

that the employees voluntarily participate in the data processing described above

processing procedures (queries and mailing of the vaccination status) have consented.

The existing employment relationship must be taken into account

Relationship of superiority and subordination between employer and employee

gen. If there is a legal or economic advantage for the

According to § 26 paragraph 2 sentence 3 BDSG employees can from the voluntary

consent can be assumed. Since the employees for the

A leave of absence was granted to take the vaccination appointments was from

Obtaining an effective declaration of consent for the collection of the

to assume vaccination status.

However, the publication of the post in the social was different

assess network. Here the person responsible could not be credible

represent that the employees have given their consent to the disclosure of the

special categories of personal data – especially on a voluntary basis

– had granted. Also were with the disclosure – in contrast to the first

Case constellation - no economic or legal advantages for the

connected to employees. The requirements for effective consent

were therefore not available.

Posting employee vaccination records violated the GDPR.

As far as special categories of personal data in a social

network have been posted without any legal basis in mind

of Art. 9 Para. 2 lit. b to j DS-GVO or an effective declaration of consent

9 paragraph 2 lit. a or § 26 paragraph 3 sentence 2 i. 2 Federal Data Protection Act

existed, this violated the principle of legality

Art. 5 (1) lit. a GDPR i. In conjunction with Art. 9 (1) GDPR.

29

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

Art. 5 para. 1 letter a DS-GVO

Personal data must

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

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

good faith, transparency");

(...)

2.6

No exclusion of data subject rights due to coronavirus

protective regulation

Restrictions on the rights and obligations under Articles 12 to 22 of the GDPR

GMOs (rights of the data subject) can only be exercised under Art. 23 GDPR

strict requirements of national law.

It must be a necessary and

take proportionate action. In doing so, the need and

proportionality for each limited data subject right and for each

Category of responsible persons are considered individually. A blanket one

Exclusion of the essential rights of data subjects with regard to a processing

processing is difficult to meet with the requirements of Art. 23

Bring GDPR into line.

According to § 4 No. 3 CoSchuV of June 22, 2021, the applicability of the

Rights of data subjects according to Art. 13 (duty to provide information), 15 (right to information), 18

(Right to restriction of processing) and 20 (Right to data portability-

availability) DS-GVO in the context of contact data collection for tracking

and interruption of infection chains excluded:

§ 4 No. 3. CoSchuV

... the provisions of Articles 13, 15, 18 and 20 of Regulation (EU) 2016/679 of the

European Parliament and Council of April 27, 2016 on the protection of natural

sons in the processing of personal data, on the free movement of data and on

Repeal of Directive 95/46/EC (General Data Protection Regulation) of April 27, 2016

(OJ EU No. L 119 p. 1, No. L 314 p. 72, 2018 No. L 127 p. 2) on the information obligation and

the right to information on personal data does not apply; those of

Those affected by the collection of contact data must be informed of these restrictions.

The Corona contact and operating instructions contained a corresponding regulation.

Restriction Ordinance (CoKoBeV) since spring 2020.

30

Data protection during the corona pandemic

In this regard, I received a number of submissions from citizens who

complained about the exclusion of the rights of data subjects.

According to Art. 23 DS-GVO, the rights and obligations according to Art. 12 to 22

DS-GVO are restricted by the legal provisions of the member states,
provided such a restriction violates the essence of fundamental rights and
respects fundamental freedoms and in a democratic society a necessary
constitutes an agile and proportionate measure that is one of the reasons set out in Art. 23
Paragraph 1 lit. a to j DS-GVO ensures.
Such a legal provision must also comply with Art. 23 Para. 2 GDPR
meet the specific requirements mentioned.
The exclusion of the rights of data subjects was effected by an ordinance
of the country. Restrictions according to Art. 23 DS-GVO can also be
Statutory regulations take place, since according to recital 41 DS-GVO a
"Legislative measure" does not necessarily mean a par-
lamentably adopted legislative act.
A legitimate aim of the restrictions in the form of protection of other
tiger important objectives of general public interest in the field of
public health (Art. 23 Para. 1 lit. e GDPR) could with regard to
be accepted on § 4 No. 3 CoSchuV. After justifying the
The state government served to exclude the rights of those affected by the effective
Pandemic control since the fulfillment of these rights for companies
and companies that were subject to the obligation to collect contact data
represented considerable effort.
The necessity and the proportionality of these restrictions
but I had serious doubts. Against the necessity of the restrictions
ments initially said that the federal legislature had no need for
had seen these limitations, although he had contact tracing
tion in § 28a Abs. 4 IfSG had regulated in detail. Especially before that
Background of the electronic contact data favored by the CoSchuV

ten collection according to § 4 No. 3 CoSchuV was also doubtful whether the

Fulfillment of the rights of data subjects for companies and businesses

Effort meant effort that made the fight against the pandemic noticeably more difficult. In the

Otherwise, the blanket exclusion of the rights of those affected left after his

Wording leaves no room for consideration of the circumstances of the individual case

and special situations.

The necessity and proportionality required by Art. 23 Para. 1 DS-GVO

Eligibility of the restriction must apply to each restricted right of the data subject

and be considered individually for each category of responsible persons.

A correspondingly differentiated regulation contained § 4 No. 3 CoSchuV

However not.

Especially the information obligation according to Art. 13 DS-GVO could be

electronic provision of a corresponding declaration without major

effort are met. Sample documents could be used for this.

For example B. the operator of the Luca App a practicable sample document

for information according to Art. 13 GDPR on the use of the Luca system

available. Various industry associations also provide corresponding information

Sample contact tracing documents ready.

The right to information according to Art. 15 DS-GVO, which is one of the elementary

tarsten represents the rights of those affected, could through the electronic contact data

data collection can be carried out regularly with little effort. When deployed

of the Luca app already has the body that is obliged to collect contact data

no access to the personal data, as these are encrypted.

However, information on the registration data and the visit data can

granted by the operator of the Luca app. Even with the written one

Recording contact data in paper form is information regularly without

further possible, in particular if the data subject provides information about the

visiting time makes. Valid reasons for the general inapplicability

availability of this right were not recognizable.

The necessity and proportionality of the blanket exclusion

ses of the right to restriction of processing (Art. 18 DS-GVO) and

Data portability (Article 20 GDPR) was not evident. The right

data portability was part of the mandatory contact

prosecution according to Art. 20 (1) lit. b GDPR anyway not factual

applicable, since the processing is not based on consent (Art. 6 para. 1

lit. a DS-GVO) or a contract (Art. 6 Para. 1 lit. b DS-GVO), but on

a legal obligation (Article 6 (1) (c) GDPR). One

Consequently, there was no need to exclude this right. The

I therefore did not think that the rights of those affected were excluded in § 4 No. 3 CoSchuV

for necessary and proportionate within the meaning of Art. 23 Para. 1 DS-GVO.

For these reasons, I have appealed to the state government for

a deletion of § 4 No. 3 CoSchuV used. The state government

understood and addressed my concerns. With the revision

of the CoSchuV on August 19, 2021, she has § 4 No. 3 CoSchuV without replacement

painted. The rights of those affected under the GDPR have also been there since then

fully applicable to the collection of contact data in Hesse.

I have a post on this process on my agency's website

published, which can be accessed at the following link: https://

Data protection during the corona pandemic

datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesund-

health/restrictions-of-the-rights-concerned.

33

Digital sovereignty

3. Digital sovereignty

Digital sovereignty

An important task in the reporting period resulted from the

ability, with many data processing systems, international processing

to evaluate personal data and the fundamental rights required

Data protection also for data processing outside the European Union

to ensure. This task was updated by the increased digital

talization as a reaction to the corona pandemic and case law

of the European Court of Justice (ECJ) (Section 3.1). Special meaning

has digital sovereignty when data protection-compliant digitization projects

are to be successfully implemented (Section 3.2). Exemplary culminated

digital sovereignty using the example of video conferences (see item 4).

3.1

Digital sovereignty and data protection

The normative commitment of the European Union, the fundamental right

on the protection of personal data in accordance with Article 8 of the Charter of Fundamental Rights

(GRCh) can only be met if the requirements for digitization

IT systems used in social relationships provide this protection

guarantee and not counteract it. Only if the

obligated person responsible is able to apply this protection in his data

To ensure processing, this fundamental right can be implemented.

Protection of fundamental rights in the transmission of personal data

to third countries

Since 2009, the European Union has guaranteed this in its Charter of Fundamental Rights

in Art. 8 the fundamental right to protection of personal data

every affected person. Since then it has been the task of the European Union

and of all Member States, this fundamental right towards every unjustified

th intervention. This also applies to data processing in

Abroad. Therefore, the GDPR has determined in Art. 3 Para. 2 that

it is applicable - regardless of the place of data processing - if the

Data processing is related to data subjects in

to offer goods or services to the European Union or to them

observe. For the same reason, the GDPR has Art. 44 et seq.

against the fact that data subjects have their fundamental rights protected

lose if their personal data is transferred to a third country, ie a

Country outside the European Union. According to Article 44

S. 2 and Recital 101 S. 3 DS-GVO should namely “that through this

Regulation on the level of protection for natural persons guaranteed throughout the Union

... when transferring personal data from the Union to

Responsible, processors or other recipients in third countries ...

not be undermined".

According to Art. 44 sentence 1 DS-GVO is a transmission of personal data

to a third country is generally only permitted if the

written conditions are met. The first condition

consists according to Art. 45 DS-GVO that the European Commission for
the receiving third country has recognized that there is a comparable data
level of protection prevails as in the European Union. Such recognitions
the European Commission has met for 14 third countries so far – under
other for Argentina, Uruguay, Canada, New Zealand, Japan, South Korea
and Great Britain. A second, alternative condition exists according to Art. 46
DS-GVO is that the transmitting person responsible with the recipient
has agreed appropriate guarantees and enforces the data subjects
real rights and effective remedies are available. suitable
According to Art. 46 Para. 2 DS-GVO, guarantees can be included in administrative agreements
gene, in mandatory codes of conduct of corporations (according to Art. 47 DS-
GMO), in the agreement of standard contractual clauses, in approved
code of conduct or in an approved certification mechanism
consist. Finally, for non-routine submissions, one of the
Special exceptions listed in Art. 49 GDPR apply. The meaning
of these conditions and exceptions is that they are based on
alternative way ensure that the data transfer does not lead to a
loss of fundamental rights.
For the data transfer to the USA, the European Commission
Special agreements have been made since 2000 to allow data to be exchanged
allow (Decision of the Commission of 26 July 2000 pursuant to the
Directive 95/46/EC of the European Parliament and of the Council on the
Appropriateness of the safe harbor principles and the
related "Frequently Asked Questions" (FAQ) guaranteed protection,
submitted by the US Department of Commerce, OJ L 215 of 25 August
2000, p. 7). It was known that neither the legal system nor the

Legal practice in the US provide a level of data protection comparable to that in the European Union is comparable. The first agreement with the United States Called "Safe Harbor", it stipulated that data-receiving bodies in the USA could undertake to comply with certain data protection rules, and through a self-commitment a safe haven for the European data could form. Then a data transfer was considered permissible. One effective review of these self-commitments in the US never took place. The agreement thus made violations of fundamental rights more European affected persons accepted. The ECJ is not surprising

with its judgment of October 6, 2015 (C-362/14 – Schrems I) the “Safe Harbor” agreement as unlawful.

With effect from August 1, 2016, the European Commission again Comparable agreement with the USA recognized, this time "Privacy Shield" referred to (implementing decision (EU) 2016/1250 of the Commission of 12. July 2016 in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the EU-US Privacy Shield due protection, OJ L 207 of 1 August 2016, pp. 1-112). This contained only a few additional provisions on "Safe Harbor", such as one Self-certification of the receiving bodies, with which they comply with the "Privacy Shield” and a promise to have an ombudsman at the US Department of State to order. A limitation of competencies the responsible intelligence services and security authorities in the USA however, did not take place.

The Schrems II judgment of the ECJ

With its judgment of July 16, 2020 (C-311/18 – Schrems II), the ECJ
the importance of the requirements of the GDPR for the transmission of personal
related data in third countries and these related to the USA
specified. He found that the "Privacy Shield" agreement
is contrary to Union law and void. The European Commission violated
violate the Charter of Fundamental Rights by signing this agreement with the US
as a justification for data transfers, although they do so
resulted in the data subjects losing their fundamental rights protection.
The ECJ based its judgment on two central criticisms of the legal
location in the USA. Firstly, the powers of the competent authorities
in the USA to access the transmitted personal data
(particularly pursuant to the Foreign Intelligence Surveillance Act (FISA),
1978, Pub.L. 95-511, Section 702 and Executive Order 12333 dated 4.
December 1981, largely revised by Executive Order 13470 dated
July 30, 2008), indefinite and disproportionate. On the other hand criticized
he that US foreigners have adequate legal recourse to defend themselves against such
Access is excluded. Although bilateral standard data protection
Sluggish with US data recipients still allowed, but not alone
sufficient. Rather, the person responsible in the European Union,
who transmits personal data to the USA, the fundamental rights of the
protect data subjects by "additional measures" from
that there is disproportionate access by the local government agencies.
According to the judgment of the ECJ, every person responsible for an IT system
applies, for which he cannot rule out that personal data

are transmitted to a third country, obliged to comprehensively assess the situation
to check. He must understand the law and data protection practice in this
Determine third country and, if there is no adequate level of data protection
prevails, the "additional
Take action. To the test program of the person responsible before the
Transfer of personal data to a third country has the European
Data Protection Committee (EDPB) issued a comprehensive recommendation (1/2020)
public. He also has detailed information in his recommendation 2/2020
given for possible assessments of the level of data protection (see for both
Recommendations https://datenschutz.hessen.de/infothek/europ%C3%A4i-
shear-privacy-committee-article-29-privacy-group).
If the person responsible for the necessary protection of fundamental rights is not in
is able, he has the data transmission and thus usually also the use
of the IT system that requires them. The data protection law
The supervisory authority is obliged to enforce these demands of the ECJ.
The judgment of the ECJ had only on the protection of personal data
to decide which are transmitted to the USA. The same problem of
Protection of fundamental rights also arises when US authorities act on personal
access personal data in the European Union. This is not only
according to the FIS Act, but also according to the Clarifying Lawful Overseas Use
of Data (CLOUD) Act of 2018, Pub.L. 115-141 (H.R. 4943) possible, der
on a clear legal basis from US authorities for a worldwide
data access aims.
All US telecommunication providers are obliged to do so. This term will
understood very broadly and in any case includes all software, cloud and

platform provider. They are all obliged to keep all data (content and metadata

ten) of electronic communication upon request and store it

as well as all stored information to the authorized US authorities

available, regardless of where they are stored. This

also applies to European subsidiaries of US providers.

Art. 48 GDPR is directed against this. He forbids a responsible person

or a processor, the transmission or disclosure of personal

related data by order of a court or an authority

third country, unless this is based on an international agreement.

Even if the ECJ has not decided the case, that a state

Agency of a third country by a company obligated to it in the

European Union requests that personal data be transferred to it,

In this case, the requirements of the Schrems II judgment must also be met

are valid. After that, those responsible may other companies, in particular

Contractors according to Art. 28 DS-GVO, personal data only

entrust if these are not obligated to foreign government agencies

are who can request the surrender of this data from you, or

additional protective measures prevent disclosure.

Digital sovereignty as a prerequisite for data protection

However, those responsible in Germany and Europe are to a large extent

IT systems dependent on US providers. These IT systems are

usually designed in such a way that they transfer personal data to the USA

average There they have access that is not legally controlled

open to government agencies. In addition, eligible state

Make US providers force them to provide personal data
from Europe, to which they - directly or via subsidiaries -
to hand over. Since affected people from Europe
when US foreigners cannot have this practice reviewed in court,
they lose their fundamental right protection through the transmission of the data.
Implementing the requirements of the Schrems II judgment is the task of the data
protection authorities. For this task, they have a resolution
and discretionary selection. You must and can decide whether
they vis-à-vis those responsible who violate the requirements of the ECJ
breach, how to proceed and what means they use to do so. in exercise
You must exercise this discretion when transferring data to the United States
or the commissioning of contractors who get into conflicts of loyalty
can, for the selection of their measures, the fundamental rights and
take into account the constitutional duties of those responsible. Included
three constellations can be distinguished:
1. Are companies developing new business models or digitizing
authorities their administrative services, they must from the outset
take into account that the GDPR - in the interpretation of the ECJ - each
Prohibits data transmission to the USA, which is not subject to additional
measures is ruled out that US authorities violate fundamental rights
able to access the data. They need their IT systems – in
As part of their commitment to privacy by design in accordance with Art. 25 DS-GVO
- designed in such a way that such data transmission is excluded.
This means that they use the hardware and software systems, platforms
must form and select and configure services in such a way
that no such data transfer takes place, or their contractors

choose so that they are not subject to the FIS Act and the Cloud Act.

2. Are foreign systems and services involved in the activities of the responsible
fully integrated into the everyday life of employees and customers
or citizens integrated, it must be taken into account in companies that through

a ban on transferring data to a third country with insufficient data protection
to transmit at least its fundamental rights to freedom of occupation and to
property to be restricted. In public bodies it may be
that they are legally without the foreign services or software
assigned tasks can no longer be fulfilled, for example the police theirs
Protection order or schools and universities their educational order.
If the effects of a ban on data transmission are taken into
be taken, it is crucial whether it is suitable for the person responsible
organizational and technical alternatives to the functions too
provide, which are fulfilled with the data transfer to the third country.
If such alternatives exist, only arise for the person responsible
"Exchange costs", but it will not be his business model or the results
fulfilling its statutory duties. Such "exchange
costs" can be extensive and not only include the monetary ones
Cost of new hardware, licenses or services. They are often with me too
difficult organizational changes or the change of
connected to usage habits. Nonetheless, in all of these cases
regularly the protection of the fundamental rights of the persons concerned
weight of the "switching costs" prevail.

3. However, there are no suitable organizational and technical alternatives,
can at companies their basic business model and thus
their economic existence in question. At government agencies
this will result in them no longer having their rights conferred by law
can fulfill tasks. If such a "functional failure" threatens, requires
the data protection response involves a difficult trade-off between
the protection of the fundamental rights of many data subjects and the
Protecting the fundamental rights of the company or the goals of state
task completion. This is made even more difficult by the fact that both
Threats to the fundamental rights of data subjects in the third country
as well as the negative consequences of failure to transmit data
can often only be recognized by difficult forecasts. To the through
Art. 8 GRCh to guarantee protection of fundamental rights are over
practical point of view, each technical-organizational alternatives to the
from the third country - here the USA - offered hardware, software,
Services and platforms required. Therefore, the fundamental right demands
from Art. 8 GRCh as a result of the Schrems II judgment of the ECJ, such
Creating alternatives and the technical dependency on the USA
to break through.

For the implementation of the Schrems II judgment, the existence of suitable
technical and organizational alternatives. The ECJ
thus demands indirectly from the European Union, the Member States and

those responsible for establishing digital sovereignty. digital sovereign
ity as a prerequisite and consequence of digital self-assertion can vary depending on

Policy field contain different goals. For the relevant legal

state context is the goal of digital sovereignty, that of those responsible

can select, design and control their IT systems in such a way that they

can fulfill its data protection obligations (see also Resolution

the DSK, creating digital sovereignty in public administration –

Better protect personal data, 2020).

Need for privacy-compliant alternatives

The high dependency on hardware and software, platforms and services

from the USA enables the large global providers to

to take advantage of situations. In the area of data protection, they demand e.g. B.

by the users, in unlimited and indefinite data processing

consent. From those responsible they demand business models,

transfer the data to third countries, consent and access options

to accept data and data processing. And from the European

Commission are asking you to consent to the exchange of data with the USA,

even if this results in fundamental rights of data subjects in the euro area

European Union to be shortened. Given the high dependency on

IT systems from the USA are digital sovereignty of those responsible

and the required protection of fundamental rights can only be achieved if appropriate

alternative data protection-compliant IT systems are offered

responsible persons can change.

This diversity in as many areas as possible of processing personal

Obtaining related data is not a task for the supervisory authorities,

but politics. Fulfilling them requires measures, among other things

economic and industrial, competitive, research, educational,

Legal and digital policy in the European Union and in the member states

states. This task is also fundamentally recognized by politicians.

Efforts to achieve more digital sovereignty are taking place in Germany and in the

European Union for several years. Because digital sovereignty

is not just a question of the rule of law and the protection of fundamental rights,

but also of competitiveness, of political self-determination

and innovative strength. It is not just a requirement for protection

of the data subject, but also for the protection of those responsible

against competitive disadvantages. That is why the European Union is making an effort

various legislative projects such as B. the designs for a digital

Services Act, a Digital Market Act, a Digital Governance Act or

an AI regulation gives control over hardware and software, data and

Data streams, standards and protocols, processes, services and

win infrastructure.

Political measures to achieve digital sovereignty

Digital sovereignty requires a variety of suitable data protection compliant

Alternatives to IT systems that require data processing in a third country

enforce or allow data access from a third country, the

does not have a comparable level of data protection as in the European Union.

Digital sovereignty is achieved when there are sufficient choices

for IT systems that comply with data protection requirements. Around

Enabling selection is a suitable legal framework

in the European Union and in the Member States, but also diverse

practical measures of selection, procurement and use of appropriate

IT systems necessary.

The concrete objectives of digital sovereignty differ according to

dependencies and options for action in the different

social areas of digitization. E.g. B.

– In-house developments of IT systems and the offering of our own

platforms and services from the European Union,

– the in-house operation of foreign IT systems by European responsible

literal (on-premise solutions),

– Sales, support and service of foreign information technology

by providers from the European Union,

– the legally compliant configuration of foreign IT systems under

conclusion of data transfers to a third country without sufficient

level of data protection,

– the use of technical-legal trustees who do not have a foreign

authorities are obliged to

– Sufficient transparency about the functions of the IT systems, in particular

special of forced data transfers, and

– Adequate self-assessment sovereignty over properties

and effects of IT systems and their risks.

Which objectives can be considered appropriate and sufficient,

is for the respective political, economic and technical field of action

to set.

With its Schrems II judgment, the ECJ demands that the European Union

and the Member States use their political options to act

the prerequisites for digital sovereignty and thus for the protection of fundamental rights

Digital sovereignty

protection in the digital world. If it's the Union's job and

of the Member States, the fundamental rights also in the case of data transmission in

to protect third countries, then they also have to cope with the extremely high

bility of foreign IT systems that are not European

respect fundamental rights. The through the charter of fundamental rights, the DS-GVO

and the Schrems II judgment of the ECJ

can only be achieved if those responsible in the European Union

have sufficient digital sovereignty. Both on the

Level of the European Union as well as many member states is digital

Sovereignty as a central political goal already formulated and in political

integrated strategies.

Tasks of the supervisory authority

The data protection supervisory authority has

wrestle) level of digital sovereignty the task of achieving the highest possible

achieve a level of protection of fundamental rights. She will take on this task

face different levels.

On the one hand, she encounters this problem again and again when she has complaints

the data subject must process according to Art. 77 GDPR, who

to oppose that a controller exercise their fundamental right to data protection

infringed by sending their personal data to a third country without

adequate level of data protection. You can refer to

that a person responsible who violates the specifications of the Schrems II judgment

of the ECJ violates, acts illegally. As a supervisory authority, I must

investigate the complaint and take remedial action. Shouldn't I do this in the

in a manner and to the extent that the data subject expects

they also exercise their basic rights according to Art. 78 DS-GVO before the administrative court through a lawsuit against me and the person responsible (as an additional party). make. It may also be possible against the person responsible directly in front of the sue the civil court or the administrative court.

Secondly, the Schrems II judgment creates new ones for the supervisory authority educational and advisory tasks. According to Art. 57 Para. 1 lit. b DS-GMOs “the public for the risks, regulations, guarantees and rights in connection with the processing and sensitize them about it enlighten" and according to Art. 57 Para. 1 lit. d DS-GVO "the persons responsible and the processors for the costs arising from this regulation raise awareness of obligations”. If through their enlightenment and advice also wants to contribute to solving the data protection problems, she will also to questions about possible technical and organizational alternatives and possible configurations of the IT systems. she will

explain that with new IT systems, the pro-problem of the loss of fundamental rights through data transfers to third countries must be taken into account and that the person responsible already operated IT systems must be checked to see whether this results in personal data Transfers data to third countries without an adequate level of data protection and provides sufficient additional protective measures for this. Otherwise must him to remedy the situation.

Third, the supervisory authority must, in fulfilling its task under Art. 57 Paragraph 1 lit. a DS-GVO, "(to) monitor the application of this regulation

and implement (to) enforce", choose a promising approach in order to

to reach the person responsible for the implementation of the data protection regulations.

In the case of planned IT systems, it will be the person responsible according to Art. 58 Para. 1

lit. d DS-GVO point out a possible data protection violation or they

even have to warn of a foreseeable violation. She is operated at

IT systems with data transfers to an insecure third country

responsible for the determinations on the legal situation required by the ECJ

and request data protection practices in the receiving third country and the

additional safeguards against disproportionate access

checked by the authorities of the third country. by the person responsible

they demand planning or consideration of which alternative IT systems

me and services he has checked what measures he needs to operate himself

foreign IT systems by himself or European contractors

workers he has considered or what configurations he has chosen to use

Data transfers to a third country without an adequate level of data protection

rule out. In order to carry out these checks and to protect data

to be able to reach fair solutions, the supervisory authority will help

those responsible who are willing to cooperate for suitable alternatives and

search for suitable configurations of the IT systems.

Given the proliferation of IT systems with data transfers in

Third countries without an adequate level of data protection is the task

To enforce the requirements of the Schrems II judgment, extremely large. To nonetheless

to be able to do justice to this task despite the limited resources,

every supervisory authority must develop a strategy that defines the task and

opportunities for improvement. I try this task above all

to do justice by relying on education and advice

and on the role model effect of successful examples. Solutions are above all

to be found in those areas where suitable alternatives exist that

perform the required functions without disclosing personal data

have to be transferred to an unsafe third country. Such an area

with a large impact and existing alternatives and design

Possibilities are video conferencing systems. Mainly aimed at this

in a first step my view when it comes to the specifications of the

implement the Schrems II judgment (see item 4). Other areas will follow.

3.2

Digital sovereignty and successful digitization projects

Digital sovereignty means that those responsible have the option

comply with their data protection obligations. It is therefore an

necessary prerequisite for digitization that conforms to data protection law.

Ensuring digital sovereignty and taking it into account at an early stage

of data protection thus form common essential success factors

for successful digitization projects.

It came about at the beginning of 2020 due to the COVID-19 pandemic

a special exceptional situation. This led and continues to lead

profound changes in daily life and has an impact on

different areas of life. For a variety of challenges

solutions had to be found, implemented and made available at short notice.

In the context of IT solutions, the focus during implementation was therefore in

many cases, initially on speed and the provision of indispensable

clear basic functionalities. Other aspects were these goals

subordinate and often deferred. This was especially true for

the data protection.

Overall, since the outbreak of the COVID-19 pandemic, there has been a sustained digital

growth that continued in the reporting period. Also

for the coming reporting period I expect a progressive increase

Digitalization. This is particularly evident in the public sector

in connection with the implementation of the Online Access Act (OZG).

This commits the federal, state and local authorities to the end

of the year 2022 a large number of their administrative services online

to make available and thus digitize.

Privacy-friendly digitization

Unlike in the exceptional situation at the beginning of the COVID-19 pandemic

must comply with data protection requirements in digitization projects

are consistently taken into account and implemented right from the start. this applies

in particular for the planning, the determination of requirements as well as for

any tenders. Finally, here are the basics and thus

the foundation for all further project phases as well as for the operation, the

maintenance, use and further development of the project results.

The comprehensive consideration of data protection as an integral component

Part of digitization projects favors the development of data protection

legally compliant solutions. So can through this approach

the principles of data protection in accordance with Art. 5 DS-GVO within the meaning of

Data protection through system design and through privacy-friendly

Default settings according to Art. 25 DS-GVO are implemented. This approach

proceeding offers the chance of data protection-friendly digitization

and thus safeguarding the rights and freedoms of those affected by digitization

affected persons in particular.

Therefore, a necessary condition for a privacy-friendly

Digitization the continuous and consistent consideration of data

intellectual property issues in all phases of digitization projects

project To do this, adequately competent

Resources are planned and made available as the project progresses

become. This applies to both the operational and the management level

of projects.

On the other hand, taking data protection law into account too late

Requirements diverse risks for the project success. This applies to both

legal issues as well as from a technical point of view. From a legal point of view

perspective can, for example, draft contracts with service providers,

who process personal data on behalf of Art. 28 DS-GVO,

be problematic. This is the case, for example, if service providers

other personal data arising in the course of processing as well

want to use for your own purposes. Technical level problems

occur about if in the context of software development of the principle

of data minimization according to Art. 5 Para. 1 lit. c DS-GVO only insufficient

implemented or the guarantee of the rights of those affected in accordance with Chapter

III DS-GVO is not technically supported.

The later such problems are recognized, the more costly and time-consuming

ver is usually their remedy, if this is still possible.

Sensitive time and budget overruns are particularly

Detection in late project phases is often the result. In the worst case

This can also lead to project aborts. Will be in such a

Case of responsibility for the failure of a project "data protection"

attributed, this obscures the actual causes and prevents that

Drawing the necessary lessons for future projects.

Digital sovereignty

Digital sovereignty as the basis for more data protection-friendly

digitalization

An essential basis of data protection law-compliant digitization

tion is digital sovereignty. It is given when the person responsible

IT systems that enable him to comply with data protection requirements

to meet the requirements (see Section 3.1).

This includes above all the possibility of the principles of data protection

according to Art. 5 DS-GVO in terms of data protection through system design

and through data protection-friendly default settings in accordance with Art. 25 DS-GVO

to implement and the security of the processing according to Art. 32 DS-GVO

to ensure.

When introducing new processing activities, it applies to controllers

first to check whether and to what extent it is possible to digitally

to act confidently. An example of the existence of digital sovereignty

is the field of video conferencing systems (VKS). Here are different

Providers of VKS software and VKS services represented on the market. For

As a result, those responsible who want to use VKS are faced with different

che offers for a wide range of possible application scenarios

Disposal. Those responsible in the area of the VKS are therefore in a position to

to act digitally confidently (see item 4). I expect those in charge to
Use digital sovereignty in this area to comply with data protection law
to provide and implement forme solutions.
Restrictions may apply, for example, if the market for
Software products or IT services in the affected area only to a very limited extent
or individual providers even hold a (quasi) monopoly position.
Also the existence of interrelationships or dependencies on others
Processing activities can lead to a restriction for a person responsible
effect of digital sovereignty. This is often particularly true
if lock-in effects come into play. The reasons for such effects
can be of many kinds. You can bond around in a strong way
individual providers lie if they rely heavily on their proprietary products
becomes. Were adjustments or individual developments based on this
carried out, these investments further strengthen the bond. Further
employees can get used to the products and services used
have, so that a change here to more or less strong reservations
might encounter. Overall, the lock-in should become more entrenched,
the longer it lasts.
As a result, the freedom of decision of a person subject to a lock-in is
those responsible are severely restricted or even no longer in fact
available. If a lock-in effect does not comply with data protection law

processing activities, data controllers can fulfill their obligations
according to Art. 24 DS-GVO. At least in this one

Case is a partial or even complete loss of digital sovereignty

determine.

Those responsible are not immune to such a loss of digital sovereignty

delivered powerless. In the short term, however, a lock-in effect can be

usually not significantly reduced or even eliminated. Rather it is necessary

this often involves a lengthy process and not inconsiderable effort

gene on the part of the person responsible. In a first step, existing

Dependencies are checked, evaluated and rated. Building on the

thus obtained overview, can then take action to regain the

digital sovereignty can be implemented, for example through targeted dismantling

of dependencies. At the same time, new IT projects should always have theirs

Influence on the digital sovereignty of the person responsible is also taken into account

become. For example, conscious diversification can help

used products and IT services as well as the use of open

Standards have a positive impact.

Especially in the public sector, the recovery of digital souvenirs

rity and its maintenance the corresponding political will,

the willingness to implement it and a not inconsiderable perseverance

in advance. Last but not least, the employees must also

be taken away from the public administration.

Outdated Technology

The digital sovereignty responsible person is not due to the introduction of new ones

Processing activities limited. Rather, even with existing

processing activities the existence and persistence of digital

to ensure integrity. This applies first and foremost to implementation

the principles of data protection in accordance with Art. 5 DS-GVO.

In relation to ensuring the security of processing in accordance with
Art. 32 GDPR, the state of the art is of particular importance
to. Come to the processing of personal data, for example
Software or hardware components used for which no updates
more are provided, it can usually be assumed that these
Components also no longer correspond to the state of the art. Also
can change the framework for the use of technologies with
change significantly over time. This can result in a formerly known as
technology that can be used in compliance with data protection law as no longer
is to be considered in accordance with the state of the art. An example of this is

the use of fax for the transmission of personal data (see
Clause 18.5).
In Art. 32 Para. 1 lit. d GDPR, the security of the processing
called for “a procedure for periodic review, evaluation
and evaluation of the effectiveness of technical and organizational
Measures to ensure the security of processing” implemented
and should be operated. Accordingly, the GDPR takes into account
here explicit changes in the framework conditions of processing
activities. It follows that those responsible for these changes
meet and, if necessary, actively adapt to the ones they have taken
have to take technical and organizational measures (TOM),
to continue to ensure the security of the processing. Can
for a necessary need for adjustment no corresponding adjustment
possible solutions to ensure compliance with data protection law

are identified, there is a loss for the associated processing activity

of digital sovereignty. Finally, a person in charge

in this case, no choices regarding those made by him

TOM's more.

When using outdated and no longer compliant data protection

bare technologies, their replacement contributes to recovery

lost digital sovereignty. However, such a replacement must

not necessarily take place in one step in all cases. This is how it could be used

obsolete technologies may be successively reduced. Also

could be an outdated technology for various processing activities

replaced by different technologies. This should just about

Technologies such as fax may be a promising approach.

support from my agency

During the reporting period, I received one in the public sector in particular

Numerous inquiries about different digitization projects. Also in

related to the use of outdated technology

contacted several responsible persons. Such requests for advice reached

my authority increasingly in early project phases or even before

project start. I very much welcome this development, since the chances of success

my advice increase significantly the earlier my employees

employees are involved.

They like to be involved in digitization projects with their specialist knowledge and their

Experience to advise. However, this advice does not include

Taking on operational tasks in projects, such as the preparatory work for training

writing documents or the creation of specific requirements.

Also, within the scope of a consultation, no examination or even approval of documents are made. This would result in conflicts of interest with my supervisory task arise. In addition, such a
Support the capacity possibilities of my authority by far would exceed. The same applies to an official one, which is often requested Release of processing activities as a whole. For such a comprehensive send confirmation of data protection compliance of a processing activity would be data protection certifications according to Art. 42 DS-GVO suitable means.

Examples of successful consultations in the context of digitization projects can also be found in this activity report (see Sections 4.2, 7.3, 9.7, 13.2 and 17.4).

I would like to continue the successful consulting practice in the past continue future. At the same time, I would like to call on those responsible to their digitization projects for sufficient competence and resources in the area of data protection, if this has not already been done.

Conclusion

The existence of digital sovereignty is a key success factor for data protection-friendly and successful digitization. Here forms digital sovereignty is a necessary prerequisite for a data Design and implementation of activities in accordance with property rights processing of personal data. Therefore, those responsible should be straight in the public sector the production and maintenance of their digital Actively practicing and shaping sovereignty. In addition, existing Deficits in the area of digital sovereignty uncovered and remedied

become. I am aware that these tasks are the responsibility of those responsible

require ongoing efforts and all those involved are faced with challenges

make changes. At the same time, I see one in digital sovereignty

indispensable basis for the protection of the rights and freedoms of

persons affected by the processing of their data.

Progressive digitization can also be expected in the future.

Especially in the public sector in the coming reporting period

several projects are realized, not least in connection

with the implementation of the OZG. My employees will

continue to provide active advisory support and thereby contribute to the

contribute to successful and data protection-friendly digitization in Hesse.

video conferencing systems

4. Video Conferencing Systems

video conferencing systems

As far as the tasks, IT systems to deal with the corona pandemic

use (see item 2) and in the use of IT systems a digital sovereignty

to achieve security that enables those responsible to comply with the specifications of the

to comply with data protection law (see Section 3), may contradict

becomes the tension when using video conferencing systems

(VKS) as in a magnifying glass in a special way. she is for this

The aim of maintaining the functions of a company or an authority despite the

bots to avoid physical contact, to maintain, indispensable.

However, it leads with many widespread VKS, those of US American

Providers, to transfers of personal data in

the USA and thus to a loss of fundamental rights of the persons concerned

sons (see Section 3.1). Solutions for data protection-compliant conditions must
can be found through the selection and design of VKS. This chapter
shows both the development towards the tension between
legal requirements, technological dependency and social needs
of technology use as well as the possibilities of problem solving
data protection compliant system design.

4.1 Video conferencing systems – here to stay

Video conferencing systems (VKS) have since the beginning of the COVID-19 pandemic
gained massively in importance. While the deferral of privacy
legal issues at the beginning of the pandemic seemed justifiable
can now be expected from those responsible that they are demonstrably on
paved the way towards the use of solutions that comply with data protection law
have. My authority will pay special attention to the future
Data protection when using VKS.

In the professional and private environment, we use a variety of different
Media for interpersonal communication. To the classic
Communication media such as letter post, telephone or e-mail came into use
Add other forms of communication to the past, such as the use of
messenger services. These have met with very broad acceptance and
have found their place in our communication in a very short time
tion behavior secured.

VKS can be used for direct communication.
A VKS is a communication medium in which
two or more participants come together virtually for a video conference

and by means of transmission of audio and video data simultaneously (synchronously) with
communicate with each other. This core functionality depends on the deployed
VKS has been supplemented with additional functionalities, such as the option of working together
View presentations, share screen content, collaborate on one
whiteboard or exchange text messages. Altogether
ten VKS a variety of opportunities for direct interpersonal
Communication, even over long distances.

From a data protection perspective, when using VKS,
the so-called "content data" is important, for example audio
and video data as well as exchanged messages and documents. At
It should be noted that these do not only affect conference participants
must, but can also refer to third parties. In addition there are
Son-related data for the provision of the VKS and for the implementation
of video conferences are required, as well as data that is part of the
usage are generated. All this data is in a data protection law
to be taken into account.

I. VKS in the COVID-19 Pandemic and Beyond

With the onset of the COVID-19 pandemic, public and non-public
public positions since the beginning of 2020 e.g. with the challenge
confronted with reducing direct personal contacts to a minimum.
This did not only apply to employees, keyword "home office". So had to
For example, schools develop concepts for distributed teaching and
implement to react to school closures, keyword "distance
lessons" (see Section 4.2). The use of VKS often offered itself as a solution.

Due to the exceptional situation at the time and above all the urgent

Last but not least, the need to establish very short-term solutions also occurred

data protection requirements in the background. my authority

has taken these special challenges into account and accordingly

traded. For example, a temporary toleration for the

Use of VKS and other applications for use in schools

pronounced (see Section 4.2).

The transitional use of data protection problematic VKS

was justified against the background of the special exceptional situation.

However, such a commitment should not be permanent. Accordingly

those responsible had to and must use the transitional period and

on the way to the use of data protection law-compliant VKS.

As the COVID-19 pandemic progressed, it also became foreseeable that

the use of VKS in many areas beyond the pandemic

should take place. In this respect, those responsible must now from the permanent

video conferencing systems

Use of VKS assume. This realization reinforces the need for

Provision of data protection-compliant solutions. The switch to

a VKS that conforms to data protection law cannot and does not need to be ad hoc

thorough preparation and appropriate implementation.

II. Data protection-compliant design of VKS

In order to use VKS in compliance with data protection law, these different

meet all requirements. These range from planning and

Implementation of a project to provide a VKS about the operation and

the maintenance of such up to its use. these requirements

apply regardless of whether public or non-public bodies VKS

insert.

The planned application scenarios of a VKS serve as a starting point.

From a data protection point of view, a legal

basis for the processing of personal data in accordance with Art. 6 Para. 1

DS-GVO are available. Also, according to Art. 5 Para. 1 lit. c DS-GVO

necessary data minimization are checked, whether a

equivalent and milder means from a data protection point of view

is available. Should such a remedy be available, this would be the one

VKS preferable.

As part of the identification of alternative products and IT services for the

Implementation of a VKS should, in addition to functional requirements, such as

the number of participants to be supported or the availability of certain

Functionalities, aspects of data protection comprehensive consideration

find. Finally, through the selection, the foundation and the framework

conditions for the future VKS and thus for the possibilities

for the data protection law-compliant design of the same. A be-

The operating model is of particular importance here

data protection implications. You can choose from the

Self-operation, operation by an external service provider and the user

of an online service. If there is no complete self-operation,

must meet the data protection requirements for the integration of

processors are fulfilled. This also includes the completion of a

Contract according to Art. 28 Para. 3 DS-GVO. Does it go beyond that – how

with many widespread VKS - to a transmission of personal

Data in third countries, the requirements from Chapter V of the

to comply with GDPR. It should be noted in particular that the requirements

Changes made by the ECJ in its decision of July 16, 2020 (Schrems

II) must be complied with for data transfer to the USA (see Section 3.1).

After the decision for a product or an IT service and that

associated operating model has been taken must be implemented

of the VKS the principles for the processing of personal data

according to Art. 5 DS-GVO by appropriate technical and organizational

cal design of the system in accordance with Art. 25 GDPR.

In addition, there are technical and organizational measures (TOMs).

Ensuring the security of processing in accordance with Art. 32 GDPR. The

arrangements made and the TOMs taken must be within the framework of

Operation and maintenance are regularly checked and evaluated for their effectiveness

and evaluated to ensure that the VKS is used in compliance with data protection law

ensure permanently.

For the implementation of a video conference in compliance with data protection law

these are initially set up accordingly by their organizers.

This includes, for example, the activation of content encryption

and the deactivation of unnecessary functionalities. Furthermore, must

the participants in advance with appropriate information about the

general conditions relevant to data protection for the video conference

become. It may also have to be effective in accordance with Art. 7 DS-GVO

consents are obtained. Finally, during the implementation

of a video conference, compliance with data protection regulations

be ensured.

More information on the requirements for data protection

forms of use of VKS, the orientation aid video conferencing system

teme of the conference of independent data protection supervisory authorities

federal and state governments (DSK) (DSK, orientation guide

Video conference systems, https://datenschutz.hessen.de/sites/datenschutz.

hessen.de/files/OH-Videokonferenzsysteme.pdf). In addition, I'm open

my authority's website for general information on the use of

VKS as well as information for decision-makers and users

provides (video conference systems - general, https://datenschutz.hessen.de/

data protection/it-and-data-protection/general).

III. On the way to data protection-compliant VKS

In the coming reporting period, my authority will increase

pay particular attention to the data protection-compliant design of VKS.

I therefore call on those responsible in Hesse to – if not already

takes place - on the way to the data protection law-compliant use of

to make VKS. I assume that the information provided

and orientation aids offer valuable support along this path.

In addition, my employees have just im

video conferencing systems

various projects in an advisory capacity in the public administration

slides and will continue to do so. The path taken should

be documented by those responsible and to my authority

can be proven.

In conclusion, it should be noted that VKS is likely to have the

beyond the COVID-19 pandemic, it has a permanent place in the portfolio of

cation media of many responsible persons are retained. Also is with one

further development of the underlying software and IT services

to meet the increasing demands of users

and to offer solutions for new fields of application. Offerer

von VKS are called upon to consider the concerns of data protection

into account and thus enable those responsible to

to provide and use VKS in accordance with property rights. I expect that

in particular providers of online services in third countries their

continue and intensify efforts unabated.

4.2

Use of video conferencing systems in schools and universities

Since the start of the corona pandemic at the beginning of 2020,

due to contact restrictions, video conferencing systems (VKS) strong

gained importance in schools and colleges, for example

the lessons or the lectures, but also exams under pande-

mix conditions to perform. you in a data protection-compliant

Operation to transfer without their function for schools and colleges

Impairing was a key task for me during the reporting period

and my authority.

I. Challenges for schools

On Friday, March 13, 2020, changed due to the corona-related

Lockdown of everyday teaching for the students as well

the teachers at the Hessian schools radically. School life like it

up to that point everyone knew and appreciated was from the one

turned upside down on the other day. As a measure of contact

reduction to curb the spread of the corona virus remained

Schools closed and teachers had to think about how

the students are taught in their own four walls

can. Many schools were looking for ways on how to teach

as was customary at the school, under the current conditions

ments can be carried out in the best possible way, and came to the conclusion that

this can best be achieved with the help of VKS. required for this

the schools a VKS, which even with an Internet connection with a low

stable bandwidth and latency, self-explanatory in handling

is, as there is little or no time for the training of the teachers as well as the

Pupils stayed, and provides the necessary comfort so that the

Lessons could be made attractive. Due to the shortness of time that

remained for the selection of an appropriate VKS, data protection became frequent

placed in the background and often those already on the market were replaced

established VKS – mostly those with US operators – for the

distance learning used.

In the interest of combating the corona pandemic, the HBDI decided at the end of March

2020 transitional use of VKS in schools largely for everyone

Available applications on the basis of Article 6 Paragraph 1 Subparagraph 1

lit. d and e DS-GVO tolerated, even if their data protection conformity is still

was not finally clarified. Associated with this was the request for that

Hessian Ministry of Education (HKM), for a data protection-compliant solution

by the start of the 2020/2021 school year. In response to this

a number of staff councillors, teachers, parents as well as students

and students who expressed concern that in

Schools may use VKS that comply with the applicable

cannot and do not comply with data protection requirements

the data protection-compliant handling of your data within the framework of the use of the

data processed by the respective VKS.

As a result, the HKM was unable to meet the deadline set by the HBDI,

because of the size of the project, for more than 2000 schools it is a central

trally provided by the country VKS (country VKS) to establish, as well as the

Requirement, possibly make a Europe-wide tender

to have to, there had been delays. Since the dama-

time, a realization of the Landes-VKS project only in the first

Half of 2021 seemed possible, the HBDI in August 2020 is the request

of the HKM and may have tolerated its use

VKS that does not comply with data protection law is extended until July 31, 2021 at the latest. The

however, further toleration was linked to the conditions that a)

each school in the concrete individual case in advance the necessity of the use

of a VKS checks and b) if the responsible school authority has a data protection

offers a compliant application as an "on premise" solution, this is mandatory

is to be used.

The schools received further support from the HBDI at the beginning of the year

2021 by giving tips for safe lessons with VKS and

video conferencing systems

a sample consent form for the use of VKS in schools

made available on its website.

At the end of March 2021, I recalled that the toleration of the HBDI for the

Use in particular US VKS expires on July 31, 2021.

At that time it was to be assumed that by the beginning of the

new school year 2021/2022 with the state VKS an application for

is available, which both the technical and the data protection

meets legal requirements. This would not be the further use

data protection compliant VKS neither necessary nor data protection law

been allowed. This note has the most diverse reactions in the

cultural area caused. Many participants welcomed this step

urgently, in particular that the result is a legally secure data protection

compliant instruction of the pupils should be possible. I

saw me due to the clarification that the toleration is now actually being phased out

allowed, but also exposed to strong criticism. In particular, that too

Microsoft Teams program is said to be affected by this, leaving many stakeholders

startle. There was concern among the students that

Parents, teachers, but also school authorities widely that without this system

distance learning, which may become necessary, at many schools

is not realizable. This concern was particularly against the background

to see that at the beginning of the pandemic in the so-called first lockdown

many bad experiences have been made with some other products

were, as there were frequent disconnections during distance learning

came. In addition, the users had now after

their own statements made them familiar with a VKS and had

for example Microsoft Teams due to its diverse technical

learned to appreciate opportunities. School authorities have also approached me

come and have informed me that they have many expensive ones

would have procured licenses that would have been worthless as a result of the announced procedure

would. The criticism was brought to me in various forms

and handed over from a state parliament petition submitted by a student

Letters addressed to me from school authorities and various inter-

meal replacements, through to diverse submissions from concerned schoolgirls

and students, parents and teachers at my agency.

This lack of understanding on the part of many of those affected and the desire

to counter the greatest concern of those involved that a new, on the part of the

The VKS made available to HKM does not bring the range of functions with it

like Microsoft Teams does, caused me to

In mid-June, a clarification on Microsoft Teams and the phasing out of the

to publish tolerance. As in the letters to the school authorities,

the interest groups and when answering the state parliament petition,

I have pointed out that the expiry of the

Only the video conferencing function of Microsoft Teams is affected

is. Other features of MS Teams (e.g. chat function, exchange of

documents) and also the other sub-products of Microsoft 365

initially continue to be used by schools in the pedagogical area,

until an audit of the data protection compliance of Microsoft 365 by the

Conference of independent data protection officers has brought clarity.

In this context, however, I have also made it clear that on the part of the HKM

A nationwide VKS will be made available by July 31, 2021

should and thus the factual basis for the schools in Hesse no longer applies,

to use other VKS.

I have also pointed out the current legal situation again. This will

currently in particular by the so-called "Schrems II judgment" of the European

Court of Justice (ECJ). According to this judgment, the transmission of

personal data of European citizens in states,

that do not guarantee the data protection standard of the DS-GVO, without additional

Protective measures are prohibited (see Section 3.1 for details). With the use of the

Landes-VKS would Hessian schools (subject to my examination) the

meet the standards required by the ECJ.

Of course, I was also aware that it was due to

school-specific processes in the individual schools in the state

different timings of the migration could occur. For this reason

I was willing to share the resulting delays, so far

it is recognizable that the schools are moving towards a data protection compliant

hit VKS. However, I walked away at the time

from that schools by the end of the first half of the school year at the latest

completed the conversion in 2021/22.

At the beginning of July 2021, I was informed that the introduction

of the state-wide VKS for the schools of the state of Hesse

will obviously be further delayed. The delay is due to a

application for examination in the award procedure. Due to the delay, the

originally announced date for the introduction of the state VKS.

Due to the fact that the state VKS will not be in place by August 1, 2021

Could be put into operation, nothing has happened to the phasing out

Toleration for the use of US VKS in particular changed.

It is important to me to maintain a data protection law-compliant state in this

area and the ongoing restriction of fundamental rights

to keep the number of victims as low as possible. Just like the Hessian ones

I had trusted schools that the state VKS at the beginning of the

School year 2021/2022 will be available and through the schools

video conferencing systems

can be used. I have now reacted to the changed circumstances

and announced that I would not take any action against schools

who would like to switch to a data protection-compliant video conferencing

cross system is not possible because the state VKS is not yet available

stands. As soon as the schools can use the state VKS, I expect

but that a changeover by the schools to the state VKS quickly

will take place. Again, I will describe the circumstances in each school

take into account and a conversion phase from the provision of the

Grant state VKS by the HKM.

On December 27, 2021, the Frankfurt Higher Regional Court determined that

that the award procedure was defective. The HKM must therefore again

carry out an award procedure. A state VKS is therefore probably only

expected at the beginning of the 2022/2023 school year. This changes mine

However, there is nothing fundamental about giving the schools the time

you need to move towards a country-wide, consistent and privacy-

to change compliant VKS.

II. Challenges for universities

The universities of the state of Hesse were also involved in mid-March 2020

confronted with the conditions of the corona pandemic and the lives of the

Students and teachers have changed significantly. Instead of in a full

len lecture hall together with fellow students at the courses

to take part had to use other routes due to the contact restrictions

be found to provide the required scholarly communication

to perform. As with the schools, it made sense to use VKS,

to bring the courses to the student apartments.

Here, too, data protection was taken into account when selecting the systems used

often not placed in the foreground, but on established ones on the market

providers who offer a high level of convenience and a stable connection

promised.

On the part of the then HBDI, in spring 2020, the Hessian

tian universities clarified that the opportunities available to the schools at

the selection of a VKS were granted, also for the university sector

are valid. This meant that in the interests of flexible combating

Corona pandemic also in this area temporarily the use of

VKS on the basis of Article 6 Paragraph 1 Subparagraph 1 lit. d and e GDPR largely

was tolerated, even if their compliance with data protection law is not yet in place

was finally clarified.

In the months that followed, my predecessor and I went to college

and also the Hessian Ministry for Science and Art (HMWK)

on the topics of data protection-compliant use of VKS and also

the data protection-compliant implementation of remote examinations by the

Hessian universities advise.

At the beginning of July 2021, I finally wrote a letter to the praesidia

of the Hessian universities and pointed out that the

according to the principle of equal treatment also for the Hessian universities

valid, toleration for the use of almost all common VKS in schools

expires on July 31, 2021. Also in Hessian universities must be grounded

the current legal situation for legal conditions during use

be taken care of by VKS. According to these specifications, VKS are either too

operate that it is ensured that no personal data

transferred to unsafe third countries without adequate safeguards

gene, or they are controlled by other data protection law-compliant VKS

to be replaced (see Sections 3.1 and 4.1 for more details). In addition, universities must

design the VKS used in accordance with data protection. Above all, you must

be designed in such a way that they meet the requirements of Art. 25 Para. 1 DS-GVO

according to a data protection-compliant system design, and so on

be configured to meet privacy-friendly requirements

Default settings according to Art. 25 Para. 2 DS-GVO. Besides that

you must ensure the security of data processing in accordance with Art. 32 DS-GVO

ensure permanently. To the Hessian universities enough time

for the necessary conversions and adjustments and to

Planning and preparations for the winter semester 2021/2022 are not allowed

I will not endanger it before the end of the winter semester

take supervisory action.

I will continue to support the universities in the transition processes in the future

advise and support and thus on data protection compliant conditions

work towards Colleges responsible for transitioning to lawful states

need longer than until the end of the winter semester 2021/22

Contact me and we can do one thing together if possible

Search for GDPR-compliant operation of suitable VKS. Here we will

also in the consideration of university-specific requirements

VKS and the requirements of the protection of fundamental rights suitable solutions

find. I am already standing with the HMWK and Ver-

representatives of the universities in a close exchange on the question of which

VKS in which embodiment can be used in the future to the

high demands of university teaching on such a system

to become, without neglecting data protection.

III. Technical requirements for data protection-compliant VKS

A VKS designed for use at schools and colleges across the country

Hessen should be suitable, must meet certain technical requirements

view of data protection. These result from the specific

cial conditions that work in such institutions entails.

When using a VKS, different categories of personal

related data is processed, which is only partially available for the users

are directly recognizable. During the processing of image and sound data,

which allow a personal reference is obvious, this is the case with those

Data that is processed “in the background” is not necessarily the case. In addition

includes such data whose processing is essential for a video

conference can come about at all, e.g. B. the IP addresses of the

participants or information about who is communicating with whom.

But also such data that the provider of the VKS for other reasons

processed, this includes, for example, the so-called telemetry data that the

Provider certain conclusions about the behavior of the VKS or about

the end device with which the VKS is used.

To what extent such data actually arise, allow a personal reference

or can even be problematic from the point of view of data protection

depending on the respective circumstances. On the one hand process different

VKS also different data. Schools and colleges need to

therefore clarity about this already when selecting a suitable system

get what data this is. On the other hand, type and quantity

of data also due to the organizational circumstances of the provision,

of the operation and maintenance of the VKS.

A basic distinction is made between three operator models, which

responsible with regard to the bodies involved in data processing

and the personal data processed there

Need to become:

1. If you run a VKS yourself, those responsible (university

len, schools or school authorities) the underlying software as well as

possibly additional services and services. Installation,

Configuration, operation and maintenance are carried out entirely by the

responsible and based on its own IT systems.

2. When operating your own, internal VKS by an external service

leister relies on its resources and expertise. kind,

The scope and design of the tasks assumed can be

vary greatly from case to case. Depending on the scope of the services provided

ments and the specific design in individual cases

the external service provider then according to a processor

Art. 4 Para. 8 DS-GVO act, whereby the requirements of Art. 28

DS-GVO, for example related to the conclusion of an order

employment contract, must be taken into account.

3. Finally, to conduct video conferencing at a

online service can be accessed. This is in the

usually a standardized offer from a service provider who

deokonferenz either directly as a telecommunications provider

offers to the market or for those responsible as processors

acts in accordance with Art. 4 Para. 8 DS-GVO.

If the VKS is provided and operated using a

contract processor, an external service provider or an online service,

the person responsible must take into account which personal data

Data from the providers of the VKS about the technical facilitation of the conference

also processed for their own purposes. Such processing requires

each case of a separate legal basis both on the part of the provider

as well as on the part of the person responsible for the transmission

the provider. The existence of such a legal permit is for the

Difficult to justify use of VKS in schools and colleges.

In addition to the provision and operation of the VKS, the type of use is also important

consider. If the VKS is used via a private end device of the learners and

teachers, the provider of the VKS may allow this under certain circumstances

through additional information (e.g. the designation of the device or other

their installed software) more precise conclusions about the identity and the

behavior of the user. Finds a use from the private

network of the person out instead, e.g. B. in the context of distance learning, so

similar conclusions can be drawn from the connection data
pull out of the network of the educational institution when used
would grant a higher level of anonymization.
As a rule, the school or university can access the processing of personal
ment-related data through the VKS influence. About appropriate
Configurations must ensure that the principles of processing
personal data according to Art. 5 DS-GVO, such as the data mini-
tion, are guaranteed. Such configurations can, for example
the deactivation of the transmission of unnecessary telemetry data to the
provider of the VKS or the hiding of the video background in the video
deo transmission from the private residential and living area of learners
include.
See more about the requirements for VKS: https://datenschutz.hessen.de/
data protection/it-and-data-protection/general.

5. Europe, International
Europe, International
Cooperation with other European supervisory authorities
With the entry into force of the GDPR, as in the 47th, 48th and 49th
Activity report described, numerous innovations for the cooperation
of the supervisory authorities in Germany and Europe. The GDPR
obliges the European data protection supervisory authorities, in cases
cross-border data processing in an effort to reach a consensus
(Art. 60 Para. 1 Sentence 1 GDPR), to cooperate closely. 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, which as

Link between the HBDI and various bodies outside of Hesse

sens in Germany, Europe and the world.

Process of cooperation and coherence according to Chapter VII GDPR

All complaints, inquiries and reports from Ver-

protection of personal data according to Art. 33 DS-GVO

are first checked in the specialist departments to determine whether a

processing that exceeds the obligation to cooperate

with other European supervisory authorities. A cross-

According to Art. 4 No. 23 DS-GVO, progressive processing is present if the

Controllers or processors 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.

According to the concept of the so-called one-stop shop introduced with the GDPR

is a supervisory authority for cross-border data processing

– in principle, the supervisory authority at the location of the main office of the

Responsible or processor (Art. 56 Para. 1 DS-GVO) - as

lead supervisory authority single point of contact for the responsible

and processor (Art. 56 Para. 6 DS-GVO). I.e., a sub-

only has to take himself with him because of one and the same data processing

deal with a supervisory authority. But this does not mean that

the lead supervisory authority decides alone. Rather act

in addition to the lead supervisory authority, all other affected parties

supervisory authorities in the decision-making process. "Concerned"

are, according to Art. 4 No. 22 DS-GVO, all supervisory authorities in whose sovereign

territory where the controller or the processor is established,

individually affected persons ("data subjects") have their place of residence or

where a complaint has been lodged.

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)

tem). The working language in the IMI system is English.

Complaints, reports according to Art. 33 DS-GVO and other inquiries

cross-border reference, which is the case with the European data

in a first step in a procedure

Art. 56 DS-GVO to determine the responsible and affected

supervisory authorities in the IMI system. Here are the facts

to prepare for the other supervisory authorities, in English

summarized and the presumed lead supervisory

authority and the supervisory authorities presumably affected.

All regulators will then have an opportunity to review the case and

as the lead or affected supervisory authority.

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

lies with the HBDI, since e.g. B. the person responsible is established in Hesse,

heads the European and International Office via the IMI system

received complaint, inquiry or report according to Art. 33 DS-GVO

along with other documents to the relevant specialist department at the HBDI,

which then, after a thorough examination of the facts, establishes contact with

responsible.

In the event that the lead management for a request received by the HBDI

complaint, request or report according to Art. 33 DS-GVO at another

European supervisory authority, transmits the staff unit Europe and

International these via the IMI system for processing to the respective

lead competent authority. To do this, the input and all

other documents necessary for processing and relevant information

information to be translated into English. As the supervisory authority concerned

the HBDI participates in the decision-making process in these procedures and

remains in the so-called one-stop shop contact person for those submitting and

informed at regular intervals about the status of the processing.

The lead supervisory authority and the supervisory authorities concerned

work closely together in the cooperation process and try to

to achieve sens (Art. 60 Para. 1 DS-GVO). The lead supervisory authority

examines the case and submits to the concerned supervisory authorities after the completion of the

investigations before a draft decision (Article 60 (3) sentence 2 GDPR).

The supervisory authorities concerned can object to this draft resolution

lodge an objection if there are concerns (Article 60 (4) GDPR).

64

Europe, International

In the event of irresolvable differences of opinion, the matter will be

European Data Protection Board (EDPB) in the consistency procedure

Art. 63 DS-GVO for a binding decision.

The aim of this way of working provided for by the GDPR is a uniform

Application of the GDPR by the supervisory authorities across Europe. There

the GDPR for this mechanism of European cooperation

does not provide for a trivial limit, it applies to a large number of everyday things

Complaints reaching the HBDI.

Increased number of cases and increased examination effort

The number of complaints, inquiries,

Art. 33-Notifications and procedures for mutual administrative assistance increased in the

reference period compared to previous years.

European procedure

Art. 56 procedure overall

Art. 56 procedure with

dismay

Art. 56 procedure with

leadership

Art. 61 procedure (administrative assistance)

Number 2019

Number 2020

Number 2021

633

17

4

65

812

32

7

26

1419

47

16

92

During the reporting period, the Europe and International Office

a total of 1419 Art. 56 procedures registered in the IMI system

possible impact or leadership to examine. In 47 of these procedures

the European and International Office has classified the HBDI as "affected"

reported, subsequently dealt with the content of the matter and

participated in the decision-making. In a further 16 proceedings, the

HBDI to process the complaint as the lead supervisory authority

accepted.

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

GMOs continue to increase. Often affect those of another European

requests for administrative assistance made to me by the supervisory authority, specific cross-border

ongoing administrative procedures in which I represent the requesting authority

to a person responsible or processor in sovereign

bid should be active. However, general legal and

Questions of interpretation on DS-GVO topics - without reference to a specific one

Case - brought to us, which then in-house through the specialist departments or

65

coordinated at national level in appropriate working groups and

get answered. It is to be expected that this trend will continue in

continue next year.

Approval of Binding Corporate Rules

In addition to the cross-border transactions to be processed via the IMI system
administrative procedures was another focus of the staff unit's activities
Europe and International in review and approval in the year under review
of Binding Corporate Rules (German: binding internal data protection
schriften, in short: BCR) according to Art. 47 DS-GVO, which - also due to the
so-called Schrems II judgment of the ECJ of July 16, 2020 (Case C-311/18) and
the ineffectiveness of the EU-US Privacy Shields - as a transfer instrument for
Data transfers to third countries are becoming increasingly popular.
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.
BCRs are developed in a Europe-wide cooperation process by supervisory
authorities of several Member States examined jointly. Also acts here
a supervisory authority as lead (so-called BCR Lead) and coordinates it
Procedure. Another regulator or two will become supportive
working as a so-called co-examiner. In addition, since the GDPR came into force and
in contrast to the previous so-called mutual recognition procedure, all European
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.
Only if this opinion is positive, i.e. a majority in the EDPB

Member States votes in favor of approving the BCR, the federal
leading authority issue an approval notice, which then also
is binding for the other supervisory authorities. All European supervisory
Authorities are thus held more accountable and obliged.
The aim of the process innovation is greater standardization of the
BCR, which also means a new and increased examination effort for the
supervisory authorities.
Since Hessen is often the location of large global companies
mensgruppen, I am very often in BCR approval procedures as

Lead management involved within Germany or even Europe-wide as a so-called
BCR Lead in charge. There are currently almost 300 applications in Europe
pending approval of BCR. I am for 13 of these BCR procedures
Europe-wide in charge as BCR Lead. Of these, five were BCR approvals
approval procedure as a result of Brexit by the British data protection supervisory
authority as the new BCR lead. In 27 other BCR procedures
I took over the lead within Germany. with that am
I am responsible for most BCR procedures throughout Germany.
Participation in committees of the DSK and at the level of the EDSA
In addition to the tasks in cross-border administrative procedures and
The European and International Office works on the BCR review
national and European level in various working groups
the DSK and working groups of the EDSA.
At the European level, the staff unit has the representation of Germany in
of the International Transfers Subgroup. The subgroup 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 affairs in various drafting teams and task forces

and reports together with colleagues from the LDA Bayern

and the BfDI constantly inform the German supervisory authorities about the work of the

Subgroup and developments in the field of European and domestic

international data protection law. The feedback from the German

The HBDI, as country representative, then brings supervisory authorities to the

discussions at European level. This is how it works e.g. B. Influence on

adopt guidelines and recommendations to be adopted by the EDPB,

which is then decisive for the later supervisory activity and

become 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,

Agendas and minutes), which the administrative department partly by e-mail, but

also electronically via the Confluence web platform and to the

relevant specialist departments at the HBDI - be it for mere information

and knowledge or possibly further cause - forwarded

Need to become. This puts the specialist departments in a position to be active and

to contribute creatively to the work at European level and e.g. B.

through participation in ad hoc groups or early commenting on pa-

piers that are in the draft stage, impact on the European

take the opinion-forming process.

At the national level, too, the Office for Europe and International Affairs has the

Participation in working committees of the DSK continued. The staff

continue to lead the nationwide organization working group

and structure. The working group supports the work of the DSK in important areas

organizational issues and develops concepts and processes for

better dovetailing of work at German and European level. A

Another topic that the working group is working on intensively

Questions arising from European cooperation under Chapter VII of the

DS-GVO, including the specific handling of these procedures

in the IMI system. In addition to organizing regular working group meetings

the Office for Europe and International Affairs keeps abreast of developments here

to be monitored and evaluated at national and European level in order to

the colleagues of the other German supervisory authorities

to be able to report. In addition, the Office of Europe and International

national for the HBDI also at the meetings of the working group

International traffic part, cross-border issues

data transmission in mind.

6. Fine Proceedings, Court Proceedings

fine proceedings, court proceedings

6.1

Juridification of the work of the HBDI

Before May 25, 2018 was working in the Data Protection Inspectorate

characterized by exams, few formal measures and a small one

Canon of moderate fines. Since the GDPR came into effect

Art. 58 GDPR provides a wide range of powers.

Their mode of action and interaction are now familiar

Data protection supervision has picked up speed under sail and the course

committed to effective enforcement of the GDPR.

Despite all the theoretical preparation, it was not yet fully developed in advance

Scope to be estimated, such as the new administrative practice under the GDPR

would actually look like. The new regulations on measures and

Sanctions from Art. 58 DS-GVO have the administrative action of the data

protection supervision has changed significantly. In addition to a strong expansion of tasks

of a supervisory authority, administrative practice has become more formal. The

Today's supervisory procedure is characterized by traditional administrative action

according to the Administrative Procedures Act. Hearings, Decisions and

setting penalty payments is part of everyday life. Is the threshold

exceeded and the decision to carry out a fine

procedurally fallen, the new component of the effective,

proportionate and dissuasive fine in the millions.

The fine procedure is based on the national standards in the OWiG

and the StPO, which are supplemented by § 40 BDSG.

The more intrusive enforcement measures and

in particular the setting of fines as well as the obligation

ment to deal with and resolve complaints, at a considerable rate

Increase in lawsuits against the regulator.

This in turn has an effect on the work of the authority that carries out its procedures

operate and document in this way and justify their decisions in this way

must withstand judicial review. This will be in

Explained in more detail below using the example of the fine procedure.

6.2

Developments on fines

The wide range of fines and the simultaneous Europeanization of the procedures

has renewed interest and great attention to the decisions of the

elicited oversight. This concerns the interests of the persons concerned

and companies that pay a lot of attention to the high fines

give, but also through the cooperation obligations according to Chapter VII of the

DS-GVO caused interest of the supervisory authorities of other member

states. If a company has a branch in several Member States,

then the need for harmonization of the application of the law

of the GDPR particularly clearly. The whole thing is accompanied by a high

Public interest in sanctioning by fines.

Especially in 2021, fine proceedings according to the DS-GVO by the

The amount of the fines imposed has reached new dimensions. But

not only the amount of fines plays a major role. For the work of

fine office in my house are two further developments of particular

their relevance: the importance of the consistency procedure in fine proceedings

and issues relating to the publication of fines

in the press.

The fine in the dispute settlement procedure

In 2021, the highest fines are for privacy breaches

been imposed since the GDPR came into force. The Luxembourg revelation
supervisory authority has 746 million euros against a large online trade and the
Irish regulator has €225m against a messaging service
imposed. Both procedures were cross-border procedures. It was
Therefore, the regulations on cooperation according to Art. 60 et seq. DS-GVO apply
to consider.
The proposed decisions had to undergo the critical examination of the EU
to the supervisory authorities concerned across Europe. in the fine proceedings
The Hessian fine office was also against the large online trade
comment requested. After viewing the more than 100-page comprehensive
English-language decision proposal was between the German
supervisory authorities a timely English-language statement on coordinated
dine, which was then forwarded to the lead agency. This
The case did not go into the consistency procedure.
In the proceedings against the messaging service in which Hessen itself
was not involved, it came to a dispute settlement procedure before the
EDPB according to Article 65 Paragraph 1 lit. In conjunction with Art. 60 (4) GDPR. It
eight appeals were heard, which the Irish regulator is addressing
had not connected. In the decision, the Irish regulator
among other things instructed to pay the fine against the messaging service
increase. The EDPB's 89-page dispute settlement decision contains more
Details of the appeals and the decision can be found (https://

fine proceedings, court proceedings
edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_
whatsapp_redacted_en.pdf).

The decision of the EDPB also indicates by its publication for

those responsible a look at the inside of the coherence procedure

free. It makes it clear that the amount of the fine does not depend solely on the

decision of a supervisory authority is dependent.

For the practice of the supervisory authorities, this means that a supervisory

driving and the possibly subsequent fine proceedings are very difficult

spend a lot of time on i. i.e. R. short response times. The

Draft decision of the final decision must be in English

be translated and written in such a way that it can be read without knowledge of the

procedural regulations in the respective country is understandable. Just in the year

In 2021, the scope of the change in the procedure for data protection

supervision has become clear.

fines in the press

In 2021, there has also been more focus on the question of whether via a

fine proceedings can or should be reported in public, and

if so, in what form this may take place. The fines can be theirs

deterrent effect for third parties not affected by the procedure, only

develop when the public learns about them. A way of the past

Publication is the inclusion of a case description in the annual

activity report. These are anonymous descriptions

selected cases.

The new dimension of fines has been recently

by some supervisory authorities the path of the press release as a further

ter possibility of informing the public is discussed and used.

There is no legal regulation on this either in the GDPR or in

the German data protection regulations. Therefore, in my view

more restraint required. The discussion about the

publication of fines in the press by the decision of

Higher Administrative Court of Münster in urgent proceedings – decision of the Higher Administrative Court of Münster of May 17, 2021

– Az.: 13 B 333/21. The decision deals with the admissibility of the

Publication of a fine by the Federal Network Agency.

In an urgent procedure, the OVG Münster had the prospects of success

of an asserted public law injunctive relief

decide. Among other things, the OVG comes to the conclusion that public

authorities are generally entitled to do so without special authorization

are, in connection with the task assigned to them

carry out press, public relations and information work. official

Statements that represent a direct encroachment on fundamental rights or

tantamount to such an encroachment on fundamental rights as a functional equivalent,

however, regularly require justification by a statutory or

direct constitutional authority.

Whether the administrative courts responsible for data protection issues

solution can be transferred to the situation of the data protection supervisory authorities,

remains to be seen. With the tasks from Art. 57 DS-GVO and Art. 58 Para. 3

lit. b DS-GVO there are good reasons for a different result than the OVG

to come to the Federal Network Agency in summary proceedings.

But it is certainly important that every decision about a report

a fine is to be made on a case-by-case basis. It's about to

take into account that the press release has a pillory effect
significantly negative consequences in terms of "name and shame"
can be solved. On the other hand, the public also has a
interest in the information. This raises the question of whether and how and
to what extent to draw attention to an imposed fine
is. My authority decides on this on a case-by-case basis.
The fact that some regulators publish fines
and others not, many a press release the name of
company reveals, while others do not, results in a colorful landscape
of publications. It becomes even more colorful that some fines
is not announced at all. This different press work plays for
the quality of the case collections for the fine procedure plays a key role.
The private case collections, the law firms, management consultants
and press representatives can only produce and publish one at a time
small excerpt from the actual work of the supervisory authorities.

6.3
fine proceedings

The range of offenses to be pursued in the administrative offense proceedings of the HBDI
All in all, the violations of data protection law are wide-ranging. In the
The focus of the processed fine proceedings in Hesse were unlawful
Moderate data processing by employees acting on their own authority
and employees.

Overview and Developments

In the reporting period, 86 new administrative offense proceedings were initiated
directs. The number of newly pending proceedings thus remained almost unchanged

fine proceedings, court proceedings

the level of the previous year. The focus of the work was on this

year in the area of employee excess (see below), with frequent violations of

the purpose limitation principle in accordance with Article 83 (5) lit. a i. in conjunction with Art. 5 Para. 1

lit. b DS-GVO were to be checked. However, there were also fine proceedings

against small, medium-sized and also larger companies in particular because of

Violations of the principles and lawfulness of processing (Article 5,

6 and 9 DS-GVO), the rights of data subjects (Art. 12 et seq. DS-GVO) and the

Security of processing (Art. 32 DS-GVO). It was about

Facts from a wide variety of subject areas, from unwanted

Advertising without consent via video surveillance in public

small space to the illegal processing of health data

in the employment relationship.

As a result, in the year under review I dealt with 16 procedures with a fine

scheid and fines totaling 47,750 euros

fixed. I know the amount of the fines in each individual case

Look at Art. 83 Para. 2 DS-GVO taking into account all relevant ones

Circumstances always determine with a sense of proportion what is in the wide range

of the amounts imposed in each case from 100 euros to a total of 42,000 euros

reflects.

employee excess

As in earlier activity reports (see 48th TB, Section 15.1, 49th TB,

Clause 16.1) described in detail, unauthorized data processing

ments by employees who go beyond service and employment law

Defying employer's instructions and own private purposes

pursue data protection violations i. s.d. GDPR (the so-called

“staff excess”). In the year under review, my agency received a large number of

Cases examined in this context and also punished with a fine.

For example, there were issues related to the

improper use of data from the so-called "corona lists" in

in gastronomy or in corona test centers by the employees there

and violations by Hessian police officers.

Selected Cases

– A police officer asked several people over a long period

from his family environment without official reasons in various

police systems and systems available to the police. The

I have violations with fines totaling 1,800.00 euros

punished. The fine notice is now final. previously had

the public prosecutor's office the criminal investigation

the suspicion of violation of private secrets (§ 203 StGB)

asked, since it could not be proven that the obtained through the queries

data was passed on to third parties.

– In another case, a police officer tried after the separation from

to restore contact with his partner. After

several unsuccessful conventional attempts to establish contact

me he used the EWO system available to him at work,

to research his ex-girlfriend's new address. On

this way he learned that this had meanwhile moved to another federal state

was warped. The official finally drove to his new apartment

ex-girlfriend and actually met her in front of the house entrance. This
frightened the former partner so much that she
reported his behavior to the local police station. Behaviour
of the police officer was fined a total of 600 euros
punished. The decision is final.

– The subject of another procedure were multiple queries
a police officer regarding information about a colleague in the
police information systems ComVor and POLAS. background
The inquiries were not an official reason, but a private one
Curiosity due to rumors about a supposed
criminal proceedings. A fine of 500 euros was imposed
imposed. Here, too, no appeal was made against the fine decision
inserted.

– A police superintendent made private purchases on an internet platform
high quality notebook. Because the seller subsequently to no
Negotiations about the agreed method of payment, used the
Officials use the POLAS information system to access information about the
to reach the person of the seller. Following the police officer sent that
Seller several messages in which he added this, among other things
whose date and place of birth include the current and previous ones
named residential addresses. By naming the ones from the POLAS queries
obtained information, the police officer wanted his demand for a
Emphasize alternative payment method. The seller brought
However, to report the facts. The behavior of the police officer
was punished with a fine of 400 euros.

Improper use of contact tracing lists

In another case, arising in the context of economic activity
a bistro, a guest complained about the cold food and
eventually left without paying this one. To find the guest
74
fine proceedings, court proceedings
chen, several visitors to the bistro were phoned by employees
of the restaurant contacted. For this purpose, the telephone numbers were used
which were deposited by the guests as corona contacts. At least one
Contact could not be made due to the complaint lodged with my
authority to be proven.
Use of contact tracing data constituted a violation
against the purpose limitation principle according to Art. 5 Para. 1 lit. b DS-GVO,
which can be punished according to Article 83 (5) (a) GDPR. personal
collected data of the visitors, which are collected by means of the so-called
th "Corona Lists" are recorded exclusively for the purpose
use to enable contact tracing of infections. The
Use of this data for other purposes - including other communication
cation with the guests – is not permitted.
The procedure ended with a fine being imposed on the owner of the
bistros in the amount of 170 euros. The effects of the
The financial situation of the entrepreneur affected by the corona pandemic,
the insight and the constructive cooperation with the supervisory
authority takes into account with a significantly mitigating effect when assessing the fine.
Working group "Data protection violations by the Hessian police"
Data protection violations by Hessian police officers
were taken as an opportunity to set up a joint working group of the

State Police Headquarters (LPP), the project Secure Data Hesse and
my authority on the subject of "data protection violations at the Hessian
lizei" to form. The aim of the working group was in particular to improve
the procedures in place for reporting breaches of protection
personal data (according to § 60 HDSIG, Art. 33 DS-GVO or § 65
BDSG i. V. m. § 500 StPO) and the acceleration of processing data
violations of property rights by Hessian police officers.
In a total of six meetings and a final meeting
votes have been taken that are suitable for improving the procedures for data
security incidents both with the Hessian police and with mine
optimize authority. The working group has, among other things – partially
with the involvement of the Hessian Ministry of Justice (HMdJ) - questions
on personal protection reporting accountability
Data discusses the critical importance of prompt reporting of
Data breaches emphasized, suitable information channels for rapid clarification
determined and the relationship between disciplinary, supervisory and fine procedures
drive cleared.

Another focus of those involved was on the concept of prevention. The
Working group prepared a report on recent fines
against employees of the Hessian police for data protection violations,
to draw attention to possible sensitive consequences of excess staff
close. The report was entitled "The Hessian Commissioner
for data protection and freedom of information imposes fines for unlawful

moderate data queries – It can get expensive!” on the Intrapol page of the

Project Secure Data Hessen published.

The working group met for the last time in November. All parties

agreed that the results achieved should be rated very positively.

This very constructive exchange should be continued.

6.4

Administrative court proceedings under data protection law

The clear trend of the last three reporting years is continuing. The number

administrative court proceedings continue to rise. have been added

Proceedings in the second instance before the Hessian Administrative

Court of Justice, and requests for a preliminary ruling under Art. 267

TFEU before the ECJ.

To the statistics

While in 2018 no proceedings according to DS-GVO before the administrative

were conducted, there were 21 in 2019 and 25 in 2020. In the

In the year under review, 34 proceedings were pending. Of the 34 court cases

from 2021 and the pending procedures from 2019

and 2020, seven were able to vote in favor of the HBDI with dismissal

be completed. Two judgments were made against the HBDI. Of the

Proceedings were terminated in the year under review by withdrawal of the lawsuit and

four by setting after mutual declaration of settlement. End

In 2021 there were still 32 procedures from 2019, 2020 and

2021 pending.

With the exception of the proceedings before the ECJ, my legal department conducts the court

process without external legal support.

Wiesbaden Administrative Court

In the year under review, a great many of the legal proceedings before the

Wiesbaden Administrative Court negotiated.

76

fine proceedings, court proceedings

Lawsuits were filed against my authority in various constellations.

On the one hand, the lawsuits were directed against decisions in which orders

ments or instructions according to Art. 58 Para. 2 DS-GVO have been made

were. In other cases, complainants turned against the company

direction of my authority about the result of the supervisory procedure. The

happened mainly in cases where a complaint was made because of a

alleged violation of data protection law, but

my authority came to a different conclusion and such a violation

For example, has not been confirmed.

The number of complaints for failure to act against my authority has also increased.

According to Art. 78 Para. 2 DS-GVO, each data subject has the right to a

effective judicial remedy if the competent supervisory authority

does not deal with a complaint or the data subject does not

within three months of the status or outcome of the pursuant

Art. 77 GS-GVO has informed about the complaint.

This option for the persons concerned has this year

increasingly important. You have filed suits for failure to act,

because they do not have this within the specified period of three months

result or an interim status had been informed. In most

cases, the period of three months was exceeded by a few days. Because of

the sharp increase in complaints with the same personnel

It is becoming increasingly difficult to deal with complaints in a timely manner.

In many cases, the lawsuits were directed against an alleged inaction, which
but actually not available. Here were the conditions for a complaint
not before or there were misunderstandings about the purpose of Art. 77 and
78 GDPR. Frequently it could be observed that claims based on
are to be asserted under civil law, in administrative disputes
were put forward, such as B. Claims for damages under Article 82
DS-GVO or deletions. In these cases, the plaintiff side was
usually not represented by a lawyer.
Technically, the focus of the administrative disputes was in the application
Scope of Art. 13 GDPR (duty to provide information), Art. 15 GDPR
(information), Art. 17 GDPR (deletion), Art. 21 GDPR (objection),
Art. 22 GDPR (profiling), Art. 33 GDPR (reporting of data breaches)
and Art. 40 DS-GVO (code of conduct) as well as § 26 BDSG (employee
data protection).
Kassel Administrative Court
Against first-instance decisions of the administrative court
the admission of the appeal under the conditions of § 124 VwGO
77
The Hessian Commissioner for Data Protection and Freedom of Information
50th activity report on data protection
be requested. In Hesse, the administrative court in Kassel is the
Appeal body in administrative court proceedings.
In the reporting period, the approval of the appeal was granted in three
applies, in two proceedings by the plaintiffs, in one by me. until
At the end of the year, a procedure for the admission of an appeal was completed,
because the plaintiff was not represented by a lawyer. In the other cases, the

Decision of the Administrative Court on the admission still pending.

Preliminary ruling request to the ECJ

Coming to the administrative litigation and the second instance proceedings

in the fourth year since the GDPR came into force, the clarification of disputed issues

in the interpretation of the GDPR by the ECJ.

The courts of the Member States are responsible for the application of Union law

competent courts. In order to ensure effective and consistent application of the

ensure Union law and prevent diverging interpretations,

national courts can (and sometimes must) refer to the Court of Justice

turn and ask him for an interpretation of Union law, such as that

compatibility of their national legislation with the primary

to be able to examine on right. Subject of the reference for a preliminary ruling

can also be the examination of the validity of a legal act of the Union. The

The Court does not respond with a mere expert opinion, but with a

reasoned judgment or resolution.

The national court to which the judgment or order is addressed

must, when deciding on the legal dispute pending with him,

respect the interpretation of the Court of Justice. In the same way, the judgment is binding

of the Court other national courts dealing with the same problem

(see https://curia.europa.eu/jcms/jcms/Jo2_7024/de/). For the

development of data protection, these procedures are of a very special nature

Relevance because they are fundamental issues with far-reaching implications for the

clarify the entire Union (item 1). The authority therefore commissions in these cases

specialized litigation representatives, which, given the weight of these proceedings,

is essential, even if it challenges the official budget financially.

With references for a preliminary ruling C-552/21 and C-634/21 are two

Proceedings initiated at the ECJ on requests from the Administrative Court of Wiesbaden. The

However, submission C-552/21 was terminated without a decision. In which

underlying administrative court proceedings before the VG Wiesbaden

the lawsuit was withdrawn towards the end of the reporting year and thus

the request for a preliminary ruling is irrelevant.

78

police, judiciary

7. Police, Justice

police, judiciary

7.1

Developments in security and

law enforcement agencies

Important current developments in the field of security and criminal

enforcement authorities, especially in the case of police video surveillance

and data analysis, are in an overarching and European context

to see.

The rapid technical developments and the associated

data protection issues have also arisen in recent years

work of security and law enforcement agencies.

The cameras used for video surveillance are always powerful

has become more powerful and is now about able to display video images in high

produce resolution and sharpness. This also has the detectability

of people overall and more distant significantly improved what

Effects on the requirements for the design of the video surveillance

has security measures. It is an essential task of my authority

therefore, especially in the context of my consulting work for the police and

Security authorities, ensure that only those permitted by law
areas and these only to the required extent in terms of space and time
be monitored.
The question of the
Admissibility of intelligent video surveillance - corresponding legal re-
there have already been some successes in some state police laws. Difficult
The main focus here is on the constitutional design and
Formulation of the legal limits of such video surveillance.
The latter is particularly important when using face recognition software
would be a big part. The developments are also at the European level
level and the experience of countries that already have such a technique
use longer, relevant for the future data protection assessment.
The European Data Protection Board (EDPB) and the Euro
European Data Protection Officer (EDPS) in June 2021 on the subject of artificial
intelligent intelligence (AI) in a joint statement called for
fen, AI systems for the automated recognition of human characteristics
and to prohibit other uses of AI with a risk of discrimination (https://
edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-
recognition- human-features-publicly-accessible_de). This opinion

5/2021 (available in German at: https://edpb.europa.eu/our-work-tools/
our- documents/ edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-pro-
posal_de) was issued on the European Commission's proposal for a
Ordinance laying down harmonized rules for artificial in-

intelligence (Artificial Intelligence Act). EDPB and EDPS refer
that given the extremely high risks associated with the
biometric remote identification of people in public spaces
blanket ban on using AI for automated detection
human characteristics in public space, no matter in which context,
including facial, gait, fingerprint, DNA, voice and typing
holding recognition as well as recognition based on other biometric or
behavioral characteristics, is required.

However, the topic of AI is not only in focus at the European level
of the data protection supervisory authorities and committees. The Federal
commissioned for data protection and freedom of information (BfDI) in the year
2021 on the use of artificial intelligence in law enforcement and
renabwehr carried out a public consultation process (https://www.
bfdi.bund.de/DE/DerBfDI/Contents/Consultation Procedures/AI Criminal Prosecution/
KI- criminal prosecution-theses-BfDI.html).

As early as June 2020, the EDPB was critical of the use of a private
Facial recognition technology services, such as Clearview
AI, voiced by law enforcement agencies in the European Union
and found that as things stand this is unlikely to be the case
is in line with the EU data protection regulations (https://edpb.europa.eu/
news/news/2020/thirty-first-plenary-session-establishment-taskforce- tiktok-
response-meps-use_de).

The EDPB is also currently working on the creation of guidelines for use
facial recognition technology by law enforcement agencies.

The national data protection supervisory authorities in Germany accompany the
Elaboration of the mentioned documents at European level. For my

Authority they will play an important role in the assessment of future

Projects of Hessian authorities play. Therefore, the local security

and law enforcement agencies called upon to adhere to these European

Opinions and guidelines to orient to data protection compliant

to develop solutions.

But also at the level of the data protection conference (DSK) there is a

alternative with current IT developments, for example in the police sector.

With its resolution “Police 2020 – see risks, opportunities

use!” from April 16, 2020 (available at: https://www.datenschutzkonferenz-

police, judiciary

online.de/media/en/Entschluss%C3%9Fung_99_DSK_TOP%2012_final.pdf)

on the new "data house" as part of the Police 2020 program

through evaluation and research platforms with regard to the earmarking

principle of education taken into account. An automated application for

Data analysis is carried out with hessenDATA for the databases of the Hessian

police already used.

The connection of a variety of sources of knowledge and databases

provides the police authorities and data protection with a view to

required separation between the different processing purposes

facing special challenges.

A position paper by the BfDI on the principle of earmarking in political

time information systems also deals with this topic

critically apart (https://www.bfdi.bund.de/SharedDocs/Downloads/

DE/DocumentsBfDI/Statements/2021/Positionspapier_Zweckschluss-

Police.pdf?__blob=publicationFile&v=1).

My authority, together with the other German and European

European data protection supervisory authorities are facing major challenges

with a view to the technological developments presented and will

corresponding projects and legislative activities in Hesse

closely and offers the authorities planning such systems

introduce and operate, their advice.

7.2

Data protection controls at police authorities and the protection of the constitution

The legal regulations stipulate that my authority in the police

implements certain privacy controls. For 2021 were

the right-wing extremism file (RED) and, for the first time,

Exercises in the second generation Schengen Information System (SIS II)

to consider. There were also reviews of data protection controls

of the covert measures from the previous year.

In 2021, various data protection checks were carried out

different police authorities and the State Office for Constitutional

protection in Hesse (LfV Hessen). All checks were made by those involved

constructively supported by the authorities.

The first data protection controls on covert measures according to § 29a

HSOG were carried out by my authority at the Hessian police in

2020. These have been continued since the last activity report was published

and further evaluated.

One focus of the audit was the existence of the respective

authority. Depending on the covert measure, the order is made by

judicial decision or the police authority. In the latter case, the

Order by the management of the authority or one of the authorities

the management commissioned officials or commissioned officials.

§ 15 HSOG

(...)

(3) Except in the case of imminent danger, measures are ordered in accordance with Paragraph 1 No. 2

by the management of the authorities or an employee commissioned by them or one of

these commissioned employees, unless a judicial order is issued in accordance with paragraph 5

is required.

(...)

As part of the data protection control, it was determined that a

Police headquarters in the instructions two people as commissioned officials

were intended. A determination of two servants is however

incompatible with the legal basis. In the course of the follow-up of the

Data protection control, the affected police headquarters adjusted the service

instructions to the legal requirements.

As already mentioned in the last activity report, notifications

genes of the persons concerned after the completion of an undercover operation

sometimes not to a sufficient extent and not always sufficient in terms of content

the legal requirements. At my instigation, a

created a comprehensive form that now meets the requirements of §§ 50 and

51 HDSIG conforms.

§ 50 HDSIG

The person responsible has information in a general, understandable and easily accessible form

to provide information in clear and plain language about

1. the purposes of the processing carried out by him,

2. existing with regard to the processing of their personal data

Rights of the persons concerned to information, correction, deletion and

restriction of processing,

3. the name and contact details of the person responsible and the contact details of or

the data protection officer,

4. the right to ask the Hessian data protection officer or the Hessian data protection

commissioned to call, and

5. the accessibility of the Hessian data protection officer.

82

police, judiciary

§ 51 HDSIG

(1) Is the notification of data subjects about the processing concerning them

personal data in special legislation, especially in the case of covert

Measures planned or ordered, this notification has at least the

to contain the following information:

1. the information specified in Article 50,

2. the legal basis of the processing,

3. the storage period applicable to the data or, if this is not possible, the criteria

for determining this duration,

4. where applicable, the categories of recipients of the personal data, too

the recipients in third countries or in international organizations, as well as

5. If necessary, further information, especially if the personal

Data was collected without the knowledge of the data subject.

(...)

In the reporting period, the statutory

prescribed, regular data protection controls of right-wing extremists

mism file (RED) instead.

§ 11 RED-G

(1) Pursuant to Section 9 (1) of the Federal

of the Data Protection Act of the Federal Commissioner for Data Protection and the

Freedom of Information. Those entered by the countries in the right-wing extremism file

Data sets can also be obtained from the respective state representative for data protection in

connection with the performance of their examination tasks in the federal states

as far as the federal states are responsible according to § 9 paragraph 1. The or the federal

Commissioner for data protection and freedom of information works in this respect with the

State Commissioner for Data Protection.

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

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

(...)

The RED was established in 2021 at the LfV Hessen and a police headquarters

checked with regard to the persons newly saved in 2019/2020.

As part of the data protection control at the LfV Hessen, I found that

that the design of personal files has improved in recent years

became. From the now uniformly designed forms, the

Understand storage requirements sufficiently. The tested memory

safeguards corresponded to the data protection regulations.

At a police headquarters, among other things, Storage of contact

sons.

§ 3 RED-G

(...)

2) Contact persons according to paragraph 1 number 1 letter b double letter mm

Persons for whom there are actual indications that they are with the persons listed in § 2 sentence 1

persons mentioned in number 1 or number 2 not only fleetingly or in an accidental

tact and through them further information for the enlightenment or

combating violent right-wing extremism can be expected.

(...).

For complete traceability of a storage of contact persons

Additional tests were carried out at the Hessian State Criminal Police Office

(HLKA). The storages triggered by the police could be understood

are not and were not to be criticized in terms of data protection law.

In 2021, the tenders were examined for the first time in accordance with Art. 36

Para. 2 Council Decision 2007/533/JHA of June 12, 2007 on the establishment

tion, operation and use of the Schengen Information System

second generation (SIS II decision).

Art. 60 Decision (monitoring of N.SIS II)

(1) Each Member State shall ensure that an independent authority (hereinafter referred to as

"national supervisory authority") independently indicates the lawfulness of the processing

SIS II personal data in their respective territories and the transfer thereof

from their sovereign territory and the exchange and further processing of additional information

information monitored.

(2) The national supervisory authority ensures that the data processing operations in

their N.SIS II at least every four years according to international audit standards

be checked.

The questionnaires and specifications for this data protection control were

responsible coordination group of the European data protection supervisory

authorities for the SIS II (SIS II SCG, https://edps.europa.eu/data-protection/

european-it-systems/schengen-information-system_de) to create a

to enable uniform testing in the member states of the Schengen area

. Alerts are issued in accordance with Article 36 (2) of the SIS II Decision

at the Hessian police for preventive purposes (cf. § 17 HSOG, for targeted

84

control or police observation) or repressive purposes (cf.

§ 163e StPO, for police observation).

police, judiciary

Art. 36 Resolution (Aims and Conditions of Bidding)

(...)

(2) An alert of this type is permissible for criminal prosecution and to prevent

Dangers to public safety if

a)

there are factual indications that a person has committed a serious crime,

e.g. B. one of those mentioned in Article 2(2) of Framework Decision 2002/584/JHA

criminal offenses, plans or commits, or

b) the overall assessment of a person, in particular on the basis of the

criminal offences, gives reason to expect that they will continue to commit serious criminal offences, e.g. Legs

the offenses referred to in Article 2(2) of Framework Decision 2002/584/JHA,

will commit.

(...)

§ 17 HSOG

(1) 1The police authorities can determine the personal details of a person and the registration number

chen and other features of the motor vehicle used or deployed by her

police wanted inventory for police observation or targeted control

write out. 2Police search records within the meaning of sentence 1 are the search data

Part of the Federal Criminal Police Office according to the provisions of the Federal Criminal Police Office Act

and at the Hessian State Criminal Police Office according to the provisions of this law

managed police information system. 3The search files of the police

Information system also includes the information according to the regulations of the Schengen implementation

alerts permitted under the Schengen Information System.

(...)

§ 163e StPO

(1) The alert for observation during police checks that the

Permit identification of personal details can be ordered if sufficient actual

there are factual indications that a criminal offense is of considerable importance

was committed. The order may only be directed against the accused and only

be taken if the investigation of the facts or the determination of the

Whereabouts of the perpetrator in another way significantly less promising or

would be significantly more difficult. The measure is permissible against other persons if

on the basis of certain facts it can be assumed that they are in connection with the perpetrator

stand or such a connection is established that the action for exploration

of the facts or to determine the whereabouts of the perpetrator and this

otherwise would be significantly less promising or significantly more difficult.

(...)

Approximately 10% of the tenders were subjected to a random check

withdrew, due to the frequency of more alerts to the police

Observation than targeted control were checked. The privacy

control of the alerts according to Art. 36 Para. 2 SIS II Decision

until the editorial deadline for this activity report.

I will discuss these privacy controls in the next activity report

inform further.

7.3

Video surveillance of the Hessian police and

security authorities

In advising on projects for video surveillance of the police and

Danger prevention authorities on the basis of § 14 paragraph 3 HSOG I contact

in particular the following criteria and standards to determine admissibility

such video surveillance measures in publicly accessible places

to consider.

In the period under review – as in previous years – my

Authority regularly on various video surveillance measures of the

Police and security authorities consulted. video surveillance

on the basis of Section 14 (3) HSOG make a large part of my

consulting activity.

Section 14 (3) HSOG

(...)

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

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

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

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

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

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

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

(...)

With regard to the conception and reorientation of video surveillance

I regularly refer to the following principles and

was able to influence the authorities concerned accordingly:

86

police, judiciary

In these cases, my authority acts in an advisory capacity

no legal obligation to test and accept prior to installation

commissioning of video surveillance systems. Compliance with

legal requirements is on the part of the responsible public authorities

ensure. However, the public authorities usually contact

to my authority and let me ask you about the specific design of the

respective video surveillance system. As part of this consultation

will include the crime survey to be carried out for the respective location

analysis, privacy masking (including outdoor catering),

assembly restrictions, signage and the storage

permanently discussed. An inspection of the commissioned system

can then take place at any time without notice from my authority.

The first requirement for a video surveillance measure is that

a crime analysis supports the necessity of the measure. This

is only the case if it involves a crime focus

typical street crime. The anti-danger purpose

the video surveillance is here in particular, the crime by a

increased risk of detection and prosecution in those under video surveillance

reduce areas.

It is also important to ensure that the necessary video surveillance

private zones can be masked out so that, for example

wise living spaces, interiors of shops, but also outdoor areas

of restaurants and cafes as far as they are for more than a short stay

are not intended to be captured by video surveillance. For this is

to design the video surveillance in such a way that the affected areas

are not first recorded by the cameras.

Incidentally, the requirements for recordings at meetings

specifically regulated and restricted in the Assembly Act (VersammlG).

(§§ 12a, 19a Assembly Act). Insofar as the video surveillance

collection is not permitted, the cameras should be switched off for the

Meeting participants be recognizable. This can be about visible

covers of the cameras or through technical precautions, such as

for example, through so-called assembly blinds mounted on the cameras

and then visible in front of the lenses at meetings

will drive, take place.

87

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

Section 12a (1) Assembly Act

(1) The police may take video and audio recordings of participants at or in connection with

prepare with public meetings only if actual evidence the

Justify assumption that from them significant threats to public safety

or go out in order. The measures may also be carried out if third parties

inevitably be affected.

(...)

The signage of the video-monitored areas is to be carried out in such a way that

that they are sufficiently recognizable and perceptible for the persons concerned

is acceptable. Therefore, the information signs should be attached in such a way that

it is clearly visible which area the video surveillance covers and who

who are responsible and how they can be contacted.

Further instructions and information will be on the signs

for data protection considerations by my authority within the framework

of the consultations expressly recommended.

Finally, the storage duration of the video recordings must be proportionate

be cheaply designed. In Section 14 Paragraph 1 Clause 2 HSOG, on the in Section 14 Paragraph 3 Clause

4 HSOG is referred to, there is only one regulation, which is the destruction

of documents after two months at the latest.

Section 14 (1) HSOG

(1) The police authorities may also use personal data other than those specified in

§§ 6 and 7 mentioned persons at or in connection with public events

or collections if factual indications justify the assumption that

that at or in connection with the event or gathering criminal offenses or

non-minor administrative offenses threaten. The documents are two at the latest

months after the end of the event or gathering, insofar as they

not to avert a danger, to prosecute a criminal or administrative offense or

are required for the execution of sentences. Processing for other purposes is not permitted.

§ 20 paragraph 8 remains unaffected.

(...)

In accordance with the principle of proportionality, my

Authority basically a storage period for such video recordings

on the basis of § 14 para. 3 HSOG of a maximum of 14 days - if they

are not required for specific procedures – as permissible and advises the

competent authorities to that effect. Consequently, the video surveillance

be technically designed in such a way that the records

automatically deleted after the permitted storage period has expired.

88

police, judiciary

7.4

Queries in the driving aptitude register in the pursuit of

traffic violations

During the reporting period, my authority received several complaints to

early data queries in the driving aptitude register as part of the processing

of traffic violations. Here could in cooperation with the

Kassel Regional Council, Central Fines Office, a fundamental one

Change in the process can be achieved.

The Federal Motor Transport Authority operates on the basis of the Road Traffic Act

(§ 28 StVG) the driving aptitude register (FAER). Querying data from

the FAER are for the competent prosecuting authorities under the

Processing of traffic offenses regularly required to

for the punishment of violations to determine whether by the data subject

criminal offenses or administrative offenses are repeatedly committed which

related to road traffic. Regarding the question of

legally permissible time of a query in the FAER as part of the

Processing of traffic offenses by the government

sidium Kassel, Central Fines Office (ZBS), went in the reporting period

several complaints.

In the FAER, information about road users who are on the road

traffic have become conspicuous, stored, insofar as the offense committed

action rated with points according to the driving aptitude rating system

is. Specifically, the complainants submitted that

Inquiries by the ZBS to the FAER were made at a time when

when there was no underlying requirement. Because the information

from the FAER only for the individual sanction in the corresponding

Traffic offense procedures are required is a requirement

for the relevant data collection in the opinion of my authority

given if the procedure after the assessment of the present

information against a specific vehicle driver.

The original procedure already saw a FAER query at the KBA

at a time when, after a summary examination of the expert

consider the hearing of the person concerned and the owner information has been provided

was triggered. At this point, however, the addressee of the accusation

have not yet had an opportunity to comment on this and, if necessary

to appoint another person as the responsible driver or

to state other reasons that further prosecution of the traffic

inhibit an administrative offense or the prosecuting authority within the framework of

application of the principle of opportunity refrain from further prosecution

permit. This procedure was therefore suitable for data collection

trigger, which is not (yet) required at this time and therefore considered

were not permissible under data protection law.

After my authority discussed this problem with the ZBS,

a change in the relevant specialist procedure has now been triggered. Provided

after owner information and summary examination, a hearing as those affected

or affected person, no FAER query is initially carried out.

Such a query is now only after a period of time that the

seven-day feedback period with regard to the hearing of those affected

and mail delivery times are taken into account. However, this is also a prerequisite

at this time the necessity of the query, d. h. that the

allegation after the hearing or the end of the relevant period

directed against this person concerned.

8. General administration, municipalities

General administration, municipalities

8.1

Current developments in public administration

With three clicks to apply for a driver's license

– Challenges of data protection law

administrative modernization

Faster, more efficient, more user-friendly and also cheaper?

The provision of services by the administration to citizens

and business aims through the use of e-government procedures

be modernized. A diverse and complex undertaking, such as

the attached diagram explains it very well. Also with a view

data protection law raises many tricky questions. The following

The article gives an overview of the developments in 2021 from data protection

legal perspective.

Final sprint for the implementation of the OZG

This is an essential component of the implementation of a modern administration
Law passed in 2017 to improve online access to
administrative services (Online Access Act – OZG). The law obliges
Federal, state and local governments, their administrative services by the end of 2022
- for example the application for a driver's license - via administration
also offer digital portals. Digitization is affected by this
of 575 administrative services.

In order to realize this mammoth project in the planned period,
etc. developed the so-called "One for All" (OfA) principle. The EfA principle
is the idea of an efficient and cost-saving administrative digitization
talization. If, for example, the state of Hesse submits the application for granting
of a driver's license digitized as an administrative service, the authorities should
other federal states join the solution and they too
to be able to use.

As far as the provision of portal solutions or the implementation
digital administrative services using the OFA principle,
there are several difficult ones from a data protection point of view
legal issues, e.g. e.g.:

– Which responsibilities within the meaning of the GDPR (responsibility,
Joint responsibility, order processing) arise between

between the different parties involved in the digitization process
actors – e.g. B. the entity developing the system (Country A), which

driving unit (IT service provider) and the subsequent user unit (country

B, federal government, municipality)?

– How can the legal consequences linked to this be efficiently implemented

become? Is it necessary to create new legal bases or

are contracts to be concluded?

– Must for the processing of personal data in the OZG context

new legal bases are created or are they already sufficient

existing legal basis?

– If legislative action is necessary, who must

take action, the federal government or the states?

– What technical and organizational requirements are there for a

administration portal and to provide a digitized administration service?

For these and other topics it applies - despite the extremely tight implementation

period of time - compliant with data protection law and manageable in practice

to develop solutions.

My authority is in regular and close contact with them

the data protection officers of the federal and state governments, the OZG coordinator

nators of the state of Hesse, project managers for digitization

individual administrative services, the central Hessian service providers for

Information and communication technology and the federal IT cooperation.

Kick-off for register modernization

In order to enable the use of digital administrative services for citizens and

organizations to further improve, the many public

register can be adjusted. In April 2021, the law on

Introduction of an identification number in public administration and

to change other laws (Register Modernization Act – RegMoG)

announced. The newly created regulations are intended to

uninformed administrative services are supported. The implementation follows

the idea of the once-only principle: citizens and

Organizations should only provide the necessary information once

administration to submit. With the consent of the users

and users should have the data reused and shared with other authorities

can be exchanged easily and safely.

A necessary prerequisite for this is the clear identification of persons

sonen and cross-register identification management. With it

data of a natural person in an administrative procedure

92

General administration, municipalities

assigned and the quality of the data can be improved as well

the renewed provision of already existing data is no longer necessary

according to the RegMoG, the tax ID should be used as a cross-register

identifier are used. In the case of an application for grant

a driver's license, the tax ID could be used for inquiries about driving

registration register or the central driver's license register.

The topic is not only national, but also European

Dimension. Selected administrative procedures are to be carried out online across borders

can be processed progressively and completely without media discontinuity

(Regulation (EU) 2018/1724 of the European Parliament and of the Council

of October 2, 2018 on the establishment of a uniform digital

gangstors to information, procedures, assistance and problem solving services

and to amend Regulation (EU) No. 1024/2012 – SDG-VO).

From a data protection perspective, the use of a registered

cross-identification feature, there is a risk that personal

gene data on a large scale easily linked and into a comprehensive

personality profile can be completed. The conference of

data protection officer of the federal and state governments already has this in their

Resolution of August 26, 2020 "Register modernization constitutional

Implement compliantly!” (https://www.datenschutzkonferenz-online.

de/resolutions.html). The risk potential is illustrated

if you consider the dimensions of register modernization

leads: 51 registers are identified by the tax ID

linked together.

So desirable and important a faster, more effective and modern

Administration is too - the task of the data protection authorities is to ensure that

to wear that despite all the euphoria and eagerness to innovate, the right to

informational self-determination does not get out of sight. Necessary

this requires transparent procedures, compliance with high data

protection standards and a technically safe design.

General administration, municipalities

8.2

Live streaming of meetings and publication of minutes

on the Internet – Participation in local politics in times of Corona

Pandemic

Participation in local political decision-making processes – for example through

keeping track of municipal council meetings or access to

Minutes of meetings – is in compliance with data protection principles

possible despite restrictions due to the pandemic.

Against the background of the corona pandemic, I received more

questions from citizens and local authorities, the question of the transfer of

Meetings and the publication of meeting minutes (transcripts)

of the municipal council on the Internet. the information

tion interest of the general public and the design of a transparent

Political decision-making and opinion-forming processes are justified here

on informational self-determination of those affected by the publication

towards people and must be balanced in an interest-based manner

to be brought. In the following I would therefore like to go into more detail on the legal

possibilities and the data protection aspects.

I. Publication of video and audio recordings of meetings of

municipal council online

For Hessian municipalities, Section 52 (3) of the Hessian Municipal

deordnung (HGO) a legal regulation for the production of image and

Sound recordings in public meetings.

§ 52 HGO

(1) The municipal council passes its resolutions in public meetings. She can for

individual matters exclude the public. Requests for exclusion

public are reasoned, discussed and decided in non-public meetings;

the decision can be made in open court if no special one

Justification or advice is required. The chairman, in agreement with

involve the mayor in the meetings that are not open to the public.

(2) Resolutions that have been passed in non-public meetings should, insofar as

this is likely to be announced after the public has been restored.

(3) The main articles of association can stipulate that film and sound recordings

media for the purpose of publication are permissible.

The regulation lays down the decision-making authority over the publication

of film and sound recordings of public meetings in the hands of the community

de-representation, which can determine in the main statute that in public

Sessions film and sound recordings by the media with the aim of

publication are permitted. This also includes the possibility

corresponding recordings on the municipal website

publish.

Insofar as the main statute contains a corresponding regulation, however

additional data protection considerations are required. So should speakers

speakers can request that their speech be recorded

or the recording is not published (right to object).

Also, before each session, a reference to the production of images and

Sound recordings are made (see also the short paper no. 10 of the DSK

on information requirements for third-party and direct collection, available at https://

datenschutz.hessen.de/infothek/kurzpapiere-der-dsk).

The city of Frankfurt am Main has in § 11 of the main statute and § 48 para. 2

the rules of procedure of the city council, for example

made the following regulation:

§ 11 Main Statute of the City of Frankfurt am Main

The public meetings of the City Council can be viewed online

audio transmission are made available. The rules of procedure regulate the details

City Council.

§ 48 paragraph 3 Rules of Procedure of the City Council

The head of the city council arranges for a simultaneous

Audio transmission of speeches on the Internet. The sound transmission is from the city

to be announced by the head of the city council at the beginning of the meeting.

Speakers who object to audio transmission have this

to notify the head of the city council. In this case

will speeches of or of the opponent, which are based on prior written

Request to speak based, not transferred.

In contrast to elected representatives, employees and meeting attendees must

not accept that they are part of picture and

sound recordings are. Here the settings are to be selected in such a way that recording

Individually identifiable persons are avoided as far as possible. Otherwise

usually the consent of the person concerned must be obtained. In

In this context, it should be noted in the case of consent that after a

Withdrawal of consent cannot be guaranteed that once in

Internet available content will be deleted globally. Only the retrieval

the municipal website can revoke the declaration of consent

prevented and thus guaranteed by those responsible.

A transparent declaration of consent should take this into account and

as concrete as possible, in an understandable and easily accessible form in one

be formulated in clear and simple language. In addition, the characteristic

sufficient account is taken of the voluntary nature of the declaration of consent

(see also brief paper no. 20 of the DSK on consent

according to the GDPR, available at https://datenschutz.hessen.de/infothek/

brief-papers-of-dsk).

II. Publication of Minutes of Meetings

In addition to virtual participation in public meetings, the

Online provision of meeting minutes against the background

of the pandemic-related contact restrictions is becoming increasingly greater

Role. A regulation on minutes can be found in § 61 HGO:

§ 61 HGO

(1) About the essential content of the negotiations of the municipal council is one

to prepare transcript. The minutes must show who is present at the meeting

was present, which items were negotiated, which resolutions were passed and which ones

elections have been held. The voting and election results must be recorded.

Any member of the municipal council can demand that their vote be taken in the

transcript is recorded.

(2) The minutes are to be signed by the chairman and the secretary.

Municipal representatives or municipal employees can be secretaries – and that too

those who do not reside in the municipality - or are elected citizens.

(3) A copy of the minutes must be included within a period of time to be specified in the rules of procedure

period of time to all community representatives in writing or electronically. Over

The municipal council decides on objections to the minutes.

Addressees of the minutes are the community board and the community

deprecation. In this way, the committees are to be given information and control

be made possible. In principle, the general public has no claim

to look at the transcripts. However, there is nothing to prevent that

Minutes relating to the public part of a meeting,

also be made available to other people.

When publishing, however, care should be taken to ensure that the

contain such personal or personally identifiable data.

An indirect personal reference has already been the subject of several times

Citizen complaints posing as complainants, buyers or sellers

97

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

of plots of land according to relevant, only relevant publications

ments, saw identified. Especially in small communities

comprehensible weighing up of local political transparency,

the citizens' need for information and individual rights

informational self-determination is important. Note in this

context also that the general public is not entitled in principle

to the publication of transcripts.

Since the circle of addressees in an Internet publication is not limited

bar is, the content must be adapted according to the requirement or

to be blackened. A data-saving handling of personal data

Data is also against the background of any assertion of

Data subject rights make sense: Does a data subject e.g. B. of his right

on deletion according to Art. 17 DS-GVO use, this can result in

that the relevant transcript is removed or extensively revised

must be made in order to process the individual personal data of the

to clean up those affected.

98

schools, colleges

9. Schools, colleges

schools, colleges

9.1

Improvements through the amendment of the Hessian school law

The 12th amendment to the Hessian School Act (HSchG) is intended to

achieve improvements in data protection law. So become schools for the

digital data processing no consent of the students

and teachers need more. A new legal regulation (§ 83a

Para. 1 No. 2 HSchG) should enable the schools to

to determine their digitization processes. become at the same time

schools, however, are also required to protect privacy and security

to ensure data processing. However, it is expected to

last until autumn 2022 before the law is passed after a wide range of consultations

can be dismissed.

The legal basis for school data processing before the

amendment

So far, schools that use a digital tool in the pedagogical

wanted to use the area of their activity, the consent of the persons concerned

serve as there is no legal requirement for this type of data processing

basis there.

School data processing is based on the legal basis of the

Article 6 paragraph 1 subparagraph 1 lit. a and e GDPR and the currently valid § 83

Para. 1 HSchG.

Article 6 paragraph 1 subparagraph 1 lit. a and e GDPR

The processing is only lawful if at least one of the following conditions

conditions are met:

a) the data subject has given their consent to the processing of data concerning them

personal data given for one or more specific purposes, ...

(...)

e) the processing is necessary for the performance of a task carried out in the public domain

interest or in the exercise of official authority, which the person responsible

was transferred.

Section 83 (1) HSchG:

Schools may collect personal information from students, their parents,

Children who will be of school age in the future or who have been deferred from attending school and their children

Parents and teachers process, insofar as this is for lawful fulfillment

of the school's educational mission and for one associated with it

purpose or to carry out school organizational measures. (...)

The need to obtain the consent of those affected applies in particular

special for pictures and videos of students who are in the

school context. The legal basis for this is Art. 6

Paragraph 1 subparagraph 1 lit. a GDPR.

Digital data processing has also been subject to the reservation of the

consent of those concerned. However, the state data processing

education (school = state) are fundamentally based on legal regulations

and the legal institution of consent only in exceptional cases

(e.g. for taking pictures).

Recital 43 GDPR

In order to ensure that the consent has been given voluntarily, it should, in special cases,

when there is a clear imbalance between the data subject and the controller

exists, especially if the person responsible is an authority,

and therefore unlikely given all the circumstances in the particular case

is that the consent was given voluntarily do not provide a valid legal basis.

EG 43 considers the voluntary nature of consent to be an actual one

or presumed subordination of parents or students

and students to school and school administration, so that an unequivocal

Consent based on a free decision of the persons concerned

is in question.

The new regulation of § 83a HSchG

Periodically I have repeated in the past

noted the need for digital processing of personal data

Data by the schools on the basis of legal legitimation

make possible. The Hessian Ministry of Culture (HKM) wants to take this into account

carry and rewrite § 83a.

100

schools, colleges

§ 83a HSchG

(1) The processing of personal data in the context of the task

of schools according to § 83 paragraph 1 is permitted, also in the context of digital applications

take place when

1. These are checked by the Ministry of Education or a body commissioned by it

and made available to schools for use, or

2. the school independently as part of its assignment of digital applications

introduces and, as the person responsible, compliance with data protection regulations

ments and the security of data processing is guaranteed.

(2) The schools can use central state-owned electronic school administration procedures

to be provided. The use of individual procedures can be declared mandatory.

(3) Further details are regulated by statutory order.

The school is to be authorized by Section 83a, Paragraph 1, Item 2 of the HSchG to

constantly as part of their task as responsible for digital applications

to introduce A proviso applies to compliance with data protection law

Provisions and ensuring the security of data processing.

The schools are thus enabled as part of their pedagogical mission

Type and scope of digital data processing both for educational purposes

as well as for school administration purposes. Also here will

In the future, the consent of those affected to data processing will be obsolete.

However, the schools also have a special obligation to

clearly the data protection conformity of the data processing. This represents

represents an enduring and challenging task that schools cannot do without

additional resources will be able to lift. That's why they have to

Ministry, the state education authorities and the teachers' academy and

the media centers have sufficient resources to support the

provide schools.

The possibility of providing the schools with state-specific electronic procedures (§ 83a

Para. 2 HSchG) and their use in individual cases

making it mandatory is to be welcomed in principle. These procedures

of the HKM and others must be checked for data protection compliance

have been.

If this is ensured, it seems more than logical to carry it through

establish mandatory use in schools. The teachers and

Pupil database by the schools according to § 1 paragraph 2 of the regulation

on the processing of personal data in schools and statistical

School surveys of 4 February 2009 (OJ 2009, p. 131) mandatory

can be used as an example.

Insofar as the school portal Hessen (SPH) will also be subject to this provision in the future

or the planned nationwide and unified video conferencing system

should, this is also an added value in terms of data protection law, insofar as their data

data protection compliance can be determined by examining the HBDI.

9.2 Electronic distance exams at universities

Electronic distance exams are a proven alternative to face-to-face exams

functions. However, legal, technical and organizational

rical framework conditions are created in order to meet the demands of the

Comparability of the test circumstances and controls as well as the protection of

To do justice to the fundamental rights of the students concerned.

Legal basis

The Hessian state government has amended the Hessian Higher Education Act

lled. In this context, in the new Section 23, a legal

Regulation created for the possibility of remote electronic examinations as well

to be able to carry out independently of the current pandemic. With this

The legislature has succeeded in creating “a permanent, viable legal basis

for electronic remote examinations".

According to § 23 Para. 6 HHG, the regulations in § 23 Para. 1 to 5 HHG

not by an ordinance, but by the statutes of the universities

be specified, in which they provide details in particular

- for the design of the electronic remote examination,

– for the processing of personal data as well

– to deal with technical faults and attempts at deception

rules.

The universities are not in their statutes on these three facts

limited. Rather, § 23 HHG provides in its regulations that the

Universities in their statutes self-contained systematic complete

can make regulations on questions relating to electronic remote examinations.

Content regulations

Remote electronic exams can make things easier for everyone involved

bring. But you have to strike a difficult balance between the

equality of those to be examined and the protection of their personal rights and

comply with their informational self-determination.

102

schools, colleges

In order to achieve this, the regulatory concept of § 23 HHG provides that

Electronic remote examinations only "in addition to the corresponding presence examinations

be offered" (§ 23 Para. 1 Sentence 2 HHG). Electronic

Distance exams are always an additional offer, which is also rejected

can be.

In order to be able to decide which form of examination you should choose

the students "are given the opportunity to relate to the exam situation

on the technology, the equipment and the spatial environment in advance

to test the exam" (§ 23 Para. 1 Clause 2 HHG).

Participation in an electronic remote examination should therefore always be

based on the principle of voluntariness. Based on the expression of

§ 23 HHG provides for a two-stage procedure for voluntary use:

– Participation is usually voluntary

Expression that those to be examined are taking part, although at the same time

an on-site examination is offered, which they could have chosen

(§ 23 Para. 5 HHG).

– Do you want to take part in an electronic remote examination with automated recording

participate, this may only take place if they are expressly included in this

have consented in writing.

The data processing in electronic remote examinations is therefore fundamentally

additionally on a legal permit. This sets the condition for a

voluntary participation through an alternative offer. The more intense

Intervention in fundamental rights on the basis of permission for automated evaluation

tion is provided by comprehensive information and an express written agreement

Consent of the participating students is taken into account.

The problem addressed by recital 43 sentence 1 GDPR,

that consent cannot provide a valid legal basis if "it

the person responsible is an authority and it is therefore in

Given all the circumstances in the particular case, it is unlikely that

the consent was given voluntarily", does not exist here.

On the one hand, data processing is based on remote electronic examinations

and the supervision provided for in principle is not based on consent,

but a legal basis, which, however, the voluntariness of

Participation ensured by a simultaneous alternative offer.

On the other hand, this alternative offer applies to an automated evaluation

tion, which is made dependent on express written consent

becomes. For this consent therefore exists despite the imbalance of power

between the university and the person to be examined “taking into account all the circumstances

in the specific case" a reasonable presumption that the consent

was given voluntarily.

This basic concept of the Hessian legislature and its legal

According to Article 6 Paragraphs 2 and 3 in conjunction with Article 6 Paragraph 1 Subparagraph 1

lit. e GDPR and Article 6 Paragraph 1 Subsection 1 lit.

casual. § 23 HHG-new regulates according to the principle of materiality

encroachments on fundamental rights by law. It contains a constitutional

permissible balance between the principle of equal opportunities and the

Protection of the liberties of the data subjects.

When conducting the electronic remote examinations, the basic

Data processing according to Art. 5 DS-GVO such as transparency, purpose

binding, data minimization, data correctness, storage limitation and

system data protection must be observed. The regulations of § 23 HHG take

see this or do not stand in the way of the fulfillment of these principles.

The principle of proportionate

moderation. This particular requires that for different

Examination objects differentiated examination modalities implemented and

adapt the monitoring measures to the respective examination modalities

to be fitted.

In the case of open-book works in which the use of

aids is largely permissible, significantly fewer monitoring measures

tests are carried out than with strictly regulated tests

aids.

Therefore, depending on the examination material, it is necessary to change the examination modalities

to adapt to the respective context of the test, which is a differentiated

extent of surveillance measures.

The principle of proportionality also applies to the differentiated

tion of technical and organizational examination conditions, e.g

Selection of a software that is as intrusive as possible or in differentiation

between carried out in the private home or at the university

remote electronic exams.

9.3

Impermissible data collection by a school when lending a

mobile device

Parents must be able to borrow a school device such as e.g. B. a lap

make an application. Many schools have for the process of borrowing

and returning the devices to their own templates developed by the parents

104

schools, colleges

were to sign. However, the school authorities are responsible for this. In the case

At one school, however, this was completely wrong in terms of data protection law. The

School collected a wealth of data from parents that was not legally requested

were still suitable in terms of content for the purpose of the loan.

Data collection by the school

I became aware of this when parents complained

made that the school collected a wealth of personal data, such as

it is classic in the area of application for social benefits.

The original application was as follows:

Application for loan of a loan laptop

for students

_____

Applicant (surname, first name)

_____

Address (zip code, place of residence, street, house number)

A

I am requesting a loaner laptop for my daughter/son:

Surname student:

First name student:

Class:

_____

Tel. (available during the day)

B.

The following siblings attend the Alexander von Humboldt School:

Surname student:

First name student:

Class:

1.

2.

3.

4.

All of the following information must be documented in writing.

Receive ongoing subsistence benefits after the twelfth book

Social Code (“Social Assistance”, “New Ways”).

□ no

□ yes* in the amount of: _____ €

(* if so, the further details C – G are omitted)

C

I have gross monthly income: _____€, net: _____€

□ my spouse or my registered partner has

monthly income of net: _____€

D

The total monthly housing costs are _____€. I pay _____€ of it.

E

Which relatives you provide maintenance?

Maintenance can be in the form of cash payments, but also through

Accommodation, food, etc. are granted. Please

state the last name, first name of these relatives (address,

only if it differs from your address in front).

If you receive maintenance solely through payment

afford.

I pay monthly Euro

Status: 10.11.2020

Legal Assessment

School data processing is based on Article 6 Paragraph 1 Subparagraph 1 lit. e

DS-GVO and § 83 HSchG (see also article under Section 9.1 - Amendment

of the Hessian School Act). The school is authorized to

to process related data of students who

Fulfillment of the education and training mandate are required.

There is no doubt that the school initially collected data that was associated with the

actual purpose, namely authorized persons a laptop over a

to borrow for a specific period of time, are not related. ask for

e.g. B. Income or bank balances are far above the target

shot out.

Also with regard to Art. 5 Para. 1 lit. b (purpose limitation) and c (data mini-

registration), the use of the application form was not permitted. Besides

the Hessian Ministry of Education had a model form for the school authorities

(It was about devices of the school authority) developed and these for

made available: contract for the loan of a mobile device for pupils

students, available at https://digitale-schule.hessen.de/sites/

digital school.hessen.de/files/Endger%C3%A4te_Leihvertrag_SAMPLE.docx.

In their statement to me, the school management informed me that

relied on the expertise of parents. The unreflected and uncritical

The school must be held responsible for the fact that these suggestions are not accepted.

Withdrawal of the application form and deletion of the data

After my intervention towards the school, which is also the competent

called the state education authority on the plan and also caused a press echo,

the school withdrew the form. The data already collected have been

deleted by the school, as the school management assured me in writing.

9.4

Privacy issues in the Padlet software application

During the year I had to deal with the use of the software application

Employ "Padlet" in the school area. I am to the conclusion

nis come that the use in or for the school, as far as private

Terminals are used, can not be done in compliance with data protection. I

I then asked the schools to continue using it until the end of the

to be discontinued for the 2020/21 school year. At the same time I have on data protection

forme alternatives pointed out.

106

schools, colleges

Use of digital tools

In times of the corona pandemic, schools are relying more than ever on the

Use of digital tools to facilitate distance learning

can. The so-called “padlet” is also a tool that comes in the form of a

digital bulletin board is used. In real time, a class can e.g. B. common

sam watch videos, write texts, send voice messages or

exchange other information.

When using digital instruments, however, data protection law

common issues to be taken into account. The same applies to use

by Padlet. First of all, it can be positively stated that users

Wall users do not have to register; you can get along with one

Sign up guest account. This eliminates the possible creation of a profile

avoided.

The Padlet platform

Padlet is operated by a US company. Since in the United

States where the GDPR does not apply, personal data can pass through

stored and processed by the company itself or by third parties

become. In addition to the shared content, this can also include the IP addresses of the

Be users or movement profiles, since Padlet at

the use of data with third parties such as B. Google shares. The exact
The content of this data is largely unknown to date.
The data protection regulations on which the platform is based
do not comply with the requirements of the GDPR, as these are only in English
are drafted and also imprecise.
Padlet can be used both mobile on devices with Android and iOS
app as well as in the browser as a web app. use schools
Padlet exclusively on school computers without an account
the computer for the respective child, the children and you remain
Usage behavior anonymous. However, it is not clear which data from
Platform operators are charged when using a school device
Padlet is accessed through the home internet connection. But as soon as
Children, teachers or parents use their private devices, they are
basically identifiable because the data is personalized by the provider
can be saved.
A use of Padlet without any problems under data protection law can only be
achieved if the use is exclusively on school computers
takes place. If private devices are used, one is data protection compliant
Application hardly possible. Even with the consent of those affected

and sufficient information on data processing, insofar as this
can be given at all is a data protection compliant use of the
Padlet platform not possible in a school context.
There are privacy-compliant alternatives

The use of digital tools and applications in the school context

is helpful considering the data protection requirements

and educationally required. My house has had many cases in the past

through advice and active support, the implementation of digital projects

allows. Digitization and data protection are not mutually exclusive;

rather, data protection enables the security of data processing

in the digital world and creates the necessary trust for the general public

Use of digital offers. This is one of the reasons why my employees

supports and promotes the search for alternatives. There was contact

admitted to the Schwyz University of Education in Switzerland

has developed a similarly designed application and for use

offers. In addition, the Technical University of Central Hesse has a digital

Product developed based on open source and at first glance

made a sufficiently data protection-compliant impression. First

Test applications are running successfully at some Hessian schools. Also

under the aspect of “digital sovereignty”, i.e. independence from

large, digital service providers, is the in-house development of software as well

to welcome their use, among other things, in the school sector.

9.5

Data protection made easy

Pupils often perceive data protection as an obstacle

taken. The diverse legal regulations are not very appealing

prepared, not only for young people. It is important to me that young people

already create simple mechanisms at school or during training

and to convey legal regulations in dealing with data protection.

Own design options and responsible handling

your own data and the data of others are a good prerequisite

for a responsible handling of the diverse digital

Tools available to children and young people.

In the context of increasing digitization, media such as video clips motivate

young people to get involved in data protection issues. The

"Data protection goes to school" initiative of the professional association of data protection

commissioned Germany (BvD) developed in 2020 with support

schools, colleges

some supervisory authorities of the federal states digital teaching and learning materials for

Data protection for use in the classroom.

Hessen supported the project by creating three video clips.

The outdoor shots were taken with schoolchildren from imma-

Nuel Kant School (Gymnasium) in Rüsselsheim and with support

of the state school authority for the district of Groß-Gerau and the Main

Taunus circle implemented. The expert talks were recorded in Frankfurt

taken. The aim was to answer the questions when designing the script

of data protection with the help of practical scenes for the schoolgirls

and pupils of the secondary level I didactically work up.

Closely linked to the right to "informational self-determination".

Personal rights are the “right to one's own image”. The distinction

is not always immediately apparent. The students experience how

recorded with a camera or a drone in physical education class

become. The video clips are constructed in a way that respects privacy issues

(GDPR), copyright (UrhG) or drone law (EU: threat

ordinance) are taken up scenically. In expert discussions with

Employees of the supervisory authorities and the initiative “Data protection goes to School (BvD)” the scenes are discussed and with the help of simple Questions such as "my I belongs to me" or "belongs to the photo on which I am pictured, really me”. Using the example of the drone It is made clear that not everything that can be filmed can be filmed may be filmed.

Left

https://www.bvdnet.de/datenschutz-geht-zur-schule/ Lehrerhandout/

https://www.bvdnet.de/datenschutz- geht-zur-schule/

9.6

Right to information and the interests of third parties worthy of protection

The right to information according to Art. 15 DS-GVO is to be seen as comprehensive, such as the Federal Court of Justice (BGH) and some higher regional courts (OLG) in have judged in the past. However, the right to information of individual not unlimited. When granting the information z. B. according to Art. 15 Para. 4 DS-GVO the rights and freedoms of other persons get noticed. This is primarily the personal data Third parties or trade and business secrets are protected.

What does the right to information include?

With the right to information, Art. 15 DS-GVO creates a basis for the fact that other data subject rights (such as the right to rectification, erasure, restriction of processing, but also the right to object) in general can be specifically asserted.

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) 1The person responsible shall provide a copy of the personal data that is the subject

processing are available. 2For all further copies made by the data subject

requested, the person responsible can charge an appropriate fee on the basis of

require administration costs. 3If the person concerned 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.

110

schools, colleges

Recital 63 GDPR

A data subject should have a right to information regarding the personal

personal data that has been collected and have this right easily and

at reasonable intervals to be aware of the processing

and to be able to check their legality. This excludes the right of data subjects

individuals to information about their own health-related data, such as data in

their patient files, which contain information such as diagnoses, test results

Results, findings of the attending physicians and information on treatments or interventions

contain. Every data subject should therefore have a right to know and to

find out, in particular for what purposes the personal data is processed

and, if possible, how long they will be stored, who the recipients of the

personal data are, according to which logic the automatic processing of personal

personal data is carried out and what the consequences of such processing may be,

at least in cases where the processing is based on profiling. If possible should

the controller can provide remote access to a secure system that

allow the data subject direct access to their personal data

would. This right should protect the rights and freedoms of others, such as business

secrets or intellectual property rights and in particular copyright

software, do not interfere. However, this must not lead to the affected

person is denied any information. If the person responsible processes a large

ge of information about the data subject, he should be able to request that the

data subject specifies on which information or which processing operations

refers to her request for information before giving her information.

Art. 15 DS-GVO enables information about this from the person responsible

to obtain whether this data relates to your own person at all

processed and if so, which ones. From recital (ErwG) 63 results

aware that data subjects are aware by exercising their right to information

about the processing of their personal data and in the

able to be put, the lawfulness of the data processing

to be able to check.

This includes all personal data and information

(Art. 4 No. 1 DS-GVO), which are available at the person responsible. The

The right to information does not only refer to so-called master data such as

such as name, address and date of birth, but also, for example, on

the communication with them. Content and meaning often arise

of information relating to a data subject

from the processing context (example: correspondence between responsible

literal and data subject). In this case, as a rule, the

the relevant documents in full (copy) upon request.

The use of the right to information is generally free of charge. Becomes

transmits a copy of the processed data to the data subject, this applies

However, only for the first copy (Article 15 (3) sentence 2 GDPR). According to Article 12

Para. 5 GDPR may only be used in the case of manifestly unfounded or excessive

Inquiries require either a fee or the provision of information

be denied. Applications can be excessive, especially in the case of frequent

be less repetition. The characteristic "frequent repetition" is included

to set strict standards.

Limits of the right to information

The right to information under Art. 15 GDPR is also not unlimited

granted. When granting the information z. B. according to Art. 15 Para. 4

DS-GVO the rights and freedoms of other people are respected.

This primarily involves the personal data of third parties or

Trade and business secrets are protected. The person responsible may

regularly but not completely refuse the information, but must

black out the names of third parties in documents, for example

not to reveal their identity.

A legitimate interest of a third party can also limit

justify the right to information. It doesn't have to be through a

be protected by confidentiality regulations. This is particularly important to think about

in the event that the person responsible has information about the person concerned

son from one or another - possibly against a promise

confidential treatment - has received, or the z. B. official

to intervene against a grievance. The responsible

would also have to according to Art. 15 Para. 1 Clause 2 lit. g GDPR

provide "all available information about the origin of the data".

The other person's interest in keeping their identity private

"Source" prevails over the interest in information at least as long as

as evidence suggests that the revelation of the identity of

informant to legal or factual discrimination

divisions of the "source". This applies all the more so far as it is

personal information of children or young people.

A trainer's right to information has limits

In the 47th activity report (Section 4.1.1) the right to information according to Art. 15

DS-GVO and others hold the following opinion:

“Providing a structured summary is also consistent with that

The aim of the GDPR is to protect natural persons from the processing of their personal

to protect your personal data (cf. Art. 1 Para. 1 GDPR). Will the copy term of the

Art. 15 para. 3 DS-GVO is generally interpreted broadly, so there is a risk that

the right to information of Art. 15 DS-GVO as a general right of access

information or as a right to inspect files, with the result that the

112

schools, colleges

Assertion of Art. 15 GDPR not to pursue data protection goals

within the meaning of the GDPR, but is misused to achieve other goals."

However, the most recent case law of the Federal Court of Justice of June 15, 2021 (VI

ZR 576/19) very broadly defined the right to information. In the same

way, the Higher Regional Court Munich I in its judgment of April 6, 2019 (3 O

909/19) and the Cologne Higher Regional Court (judgment of July 26, 2019 – 20U 75/18).

In the case presented to me for the data protection assessment, it worked

about a gymnastics trainer who worked at a federal training center

put was. This faced allegations from the young people training there
exposed, e.g. psychological violence and medically unauthorized
Giving out medication to the trainees. The accusations
by the responsible German Gymnastics Federation (DTB) through an external one
Law firm revised. In this context, the
young people were interviewed and assured of confidentiality. A more than
100-page final report was created and handed over to the DTB
ben. As a result, the trainer's lawyer demanded the handing over of the
Report and referred to Art. 15 DS-GVO. The DTB transmitted
then the report, but blacked out the passages, the conclusions
on the identity of the young people interviewed. Against this
the lawyer lodged a complaint with me.

First of all, I was able to establish that the DTB was willing to respond to the request for information
to comply with in principle. The redactions that have taken place appear
logically, it is about the statements of the young gymnasts
Behavior of the trainer towards them and others. An anonymization
of the information, i.e. the removal of the names of the gymnasts, could not
take effect, since many of the facts and situations described by them
could be traced individually and thus personally.

On data protection when processing personal data

Unfortunately, the GDPR does not contain any general regulations for children. Only for
data processing in connection with an offer of services
of the information society towards children contains Art. 8 DS-GVO
regulations. In ErwG 38 of the DS-GVO, however, the special protective
neediness of children emphasized.

Recital 38 GDPR

Children deserve special protection when it comes to their personal data, because children
the risks, consequences and guarantees concerned and your rights in relation to the processing
may be less aware of personal data. Such a special one
Protection should include the use of children's personal information for

Advertising purposes or for the creation of personality or user profiles and the
Collection of personal information from children when using services that
offered directly to children. The consent of the bearer of the parental
Responsibility should be related to prevention or counseling services that
offered directly to a child may not be required.
The trainer's right to information is in competition with the right of the trainer
affected gymnasts on the protection of their personal data,
Report in the form of interviews are included. In addition, those affected
assured the confidentiality of their statements. The interests of young people
In this case, I was against the right to information of the
Trainer classified as senior. Incidentally, the report was when
also not concerning the passages I have described, the lawyer of
trainer made available.
As a result, the request of the lawyer and his clients
tin to be able to take note of the unredacted report, none
Chance of success.

9.7 First data protection impressions of the Hessen school portal

This has been enjoyed since the start of the corona pandemic at the beginning of 2020

Schulportal Hessen (SPH) a steady increase in users

users. While before the pandemic, only a few Hessian schools participated in this

School portal were connected, it is now the majority of the

Schools in Hesse using the portal. This appears against the background

that many students in 2020 and 2021 for a long time

had to be schooled at home and that the SPH the schools from

State of Hesse is made available free of charge, more than understandable.

It is therefore all the more important that the SPH complies with data protection law

complies with regulations.

The school portal and data protection

Even before the outbreak of the pandemic, I and the Hessian Cultural

Ministry (HKM) jointly started to implement the data protection law

Discuss issues related to the SPH. From the to

Documents viewed at that time could show a cautious trend

be read out that the data protection conformity of the platform dem

appears to be guaranteed. For example, the SPH is on Open

Source systems that are hosted in Germany, so that

schools, colleges

no critical processing of students' data like

also of teachers in an insecure third country. complete a-

de data protection advice and assessment was in the reporting period

not yet possible due to the size of the project.

With the outbreak of the pandemic and the explosive growth in the number of

Users of the SPH received the question about data protection

conformity of the portal is becoming more and more important. For this reason decided

within the framework of the available resources, my advisory

further increase performance in this area. So should creating one

complete data protection concept and all data protection regulations

relevant documents to the SPH can be accelerated.

This resulted in a number of consultation appointments between the HKM and myself. This

took place at both the working and managerial level and

served to expand the existing data protection documentation

tion to the SPH to discuss together and their potential for improvement

to work out.

A look into the future

The pandemic called for a major step in the digitization of schools,

which raises important privacy issues in every aspect. To this too

solve, I have a comprehensive consulting task. Because of the fertile

Cooperation between the HKM and with is already extensive

data protection documentation for the SPH was created, to which in the year

can be built in 2022. It can therefore be assumed that I

in the near future it will be possible to give a final evaluation of the portal.

In addition to the SPH, there are other projects in the school sector that

I currently accompanied in an advisory capacity. For one thing, this is one

planned uniform access to schools. This should barriers to entry at the

Eliminate use of IT procedures. There should be a central access page

be set up, from which all applications without

new registration are available. This means, for example, that

Access to the school portal, the email for teachers and the portals of the

School authorities should be made possible via a school ID and a password.

On the other hand, the state of Hesse would like to establish a state-wide video con-

implement reference system for schools. This is intended to give schools a

data protection-compliant handling of video conferences.

115

Advice to the Hessian state parliament

10th consultation of the Hessian state parliament

Advice to the Hessian state parliament

An important task of the data protection supervisory authority is

Article 57(1)(c) GDPR, "in accordance with the law of the Member State

the national parliament … on legislative and administrative measures

to protect the rights and freedoms of natural persons in relation to

(to) advise the processing". There were three consultations during the reporting period

of the Hessian state parliament of particular importance: for the validity of the

DS-GVO for data processing in the state parliament (section 10.1), to a new one

Petition Act for the State Parliament (Section 10.2) and for the revision of the data

data protection regulations of the state parliament (section 10.3).

10.1

Does the GDPR apply to the Hessian state parliament?

The GDPR applies to the processing of personal data

in the Hessian state parliament only for the administrative area. To this counts

also the administrative processing of petitions, but not the processing

processing of a petition by a member of the Landtag as rapporteur

and also not the consultation in the Petitions Committee and the final one

Decision on the petition by the Landtag plenum. No validity

has the DS-GVO for the legislative and parliamentary activities of the

Parliament, the parliamentary groups and the members of parliament.

Since the GDPR came into force, it has been disputed whether it also includes processing

personal data collected in the parliaments of the Member States.

The ECJ (C-272/19) ruled on July 9, 2020 that

the Petitions Committee of the Hessian State Parliament (HLT) of the DS-GVO

lies and regards him as responsible according to Art. 4 No. 7 DS-GVO. With

However, in this judgment he has not decided the crucial question of whether this

also applies to the parliamentary activities of the Landtag. To this question

the President of the Hessian State Parliament asked me for a legal opinion

(see also Roßnagel/Rost, Is the General Data Protection Regulation also in the

Landtag applicable? Democratic sovereignty and Union data protection,

NVwZ 2021, 1641).

I. Scope of application of the GDPR

Crucial to the question of whether the scope of the GDPR

parliamentary activity of the state parliaments, through which the state parliament members

primarily pursue, record or exclude political and legislative objectives,

is the provision of Article 2 (1) and (2) (a) GDPR.

Art. 2 GDPR

(1) This Ordinance applies to the fully or partially automated processing of personal

of personal data as well as for the non-automated processing of personal data

Data stored or intended to be stored in a file system.

(2) This regulation does not apply to the processing of personal data

a)

in the context of an activity that does not fall within the scope of Union law,

(...)

Art. 2 para. 1 determines the material scope of application of the GDPR very much
far. Insofar as the HLT processes personal data, this also applies
them this fact. According to Art. 2 Para. 2 lit. a DS-GVO, the regulation
However, the statement “does not apply to the processing of personal data
Data … in the context of an activity not within the scope
of Union law falls".
On the question of whether data processing within the framework of parliamentary-legislative
active activity of a democratically elected representative body in Germany
within the scope of Union law and thus also of the GDPR
falls, there was no case law until the judgment of the ECJ. In the literature
the answer was controversial.
II. Decision of the ECJ of July 9, 2020
On a request for a preliminary ruling from the VG Wiesbaden under Art. 267
Para. 1 TFEU, the ECJ ruled in its judgment (C-272/19) of July 9, 2020
stated “that the Petitions Committee … to the extent that this Committee
alone or jointly with others about the purposes and means of processing
tion decides, as 'responsible' within the meaning (of Art. 4 Para. 7 DSGVO)
is to be classified, so that the made by such a committee
Processing of personal data within the scope of this
Ordinance … falls”.
In its reasoning, the ECJ focuses strongly on the activities of the petitioner
committee and does not make any fundamental statements on the parliamentary
cal activity of the LDS. He instructs the Petitions Committee in relation to
HLT a "special role". From the point of view of the ECJ, it is a body that only
"contributes indirectly to parliamentary activity" and its activities
are "political and administrative in nature". For him he takes no original

parliamentary task true, but is an "administrative control body",

118

Advice to the Hessian state parliament

which is more like a Board of Appeal or an Ombudsperson. A

Precedent for the applicability of the GDPR for general parliamentary

The verdict therefore does not result directly from the technical tasks of the HLT.

III. Exception of Art. 2 lit. a GDPR

The question of the scope of the GDPR is therefore direct

Art. 2 Para. 2 lit. a GDPR to answer. After that, it is crucial whether the

parliamentary activities of the LDS and the political-legislative activities

Members of Parliament fall within the scope of Union law.

Since the treaties of the European Union only certain sovereign rights of

transferred from the Member States to the Union is the scope

of Union law to be positively determined in each case. According to the principle of

limited individual authorization according to Art. 5 para. 2 TEU, the Union

act only within the limits of the competences that the member

States her in the contracts for the realization of the laid down therein

transferred goals. According to this, the "scope of application of the

onsrechts" with the areas for which the Union has legislative powers

zen have been granted. This is for the area of

parliamentary-legislative activities of the member states is not the case.

But even if it were argued that the "scope of the

Union law" is to be understood more broadly than the area for which legislative

competences of the Union, this area of application could only

be understood in such a way that it includes all matters regulated by Union law

includes, for which the Member States to observe Union law requirements

have. This is to be assumed if the Member State in the respective

sphere of activity of Union law or has to be carried out

enforcement or implementation of Union law, the exercise or actual

the realization of the fundamental freedoms of Union citizens must be observed.

The scope of application of Union law would then be opened up if the

field of activity is the subject of a secondary law regulation. For

the parliamentary activities of the LDS there are no specific union

legal requirements. The fundamental freedoms also cover this limited

field of activity not.

In addition, Union law protects the national sovereignty of the member

States has to consider. The legal

obligation of the Union, the respective national identity of each Member State

to be respected in their basic political and constitutional

structures including regional and local self-government

expression comes. These basic political and constitutional

gene structures and the areas of activity in which these are reflected

come, determine the national identity, which is an "ultimate limit for

action by the Union'. In Germany, after the

jurisprudence of the Federal Constitutional Court, the concept of constitutional structure

tures in Art. 4 Para. 2 Sentence 1 TEU with the constitutional identity, which over

Art. 23 para. 1 sentence 3 i. V. m. Art. 79 Abs. 3 GG is defined. The identity

of the Federal Republic of Germany, the BVerfG determines above all in its

Lisbon decision of June 30, 2009 (BVerfGE 123, 267). to the union

legally inviolable constitutional identity belong to the “political

Decisions that have a special impact on cultural, historical and

linguistic pre-understandings are dependent, which are partisan and political

parliamentary organized space of a political public discursive

unfold" (para. 247). Union law must therefore regulate the functioning of the

political-parliamentary democracy in Hesse according to Art. 4 Para. 2 Sentence 1

EUV as part of national identity, in its fundamental political

and constitutional structures.

The parliamentary areas of activity of the HLT are thus outside

the regulatory competence of Union law and its application and

thus also outside the scope of the GDPR.

On the one hand, this applies to the activities of the representative body and its tasks

as legislator. Data processing within the framework of the legislative

procedural in the narrower sense are only determined by national data protection

regulations allowed and regulated. This also includes the

operation-regulating activity of the Presidium and the Council of Elders of the HLT

and the committee secretariats. On the other hand, Union law

nor does LDS election to public office. Third fall though

also the parliamentary-political decision-making of the LDS and the following

related activities of the members of parliament and the parliamentary groups in the

advertised by the government and the opposition does not fall within the scope of the

union law. These parliamentary-political decision-making processes

also include the development of one's own political positions and initiatives

and concepts, cooperation with other parliaments, contacts

other policy makers and stakeholders as well

the public relations of the LDS, the parliamentary groups and the MPs. Not

Fourthly, the political control of the government falls under the GDPR
the LDS, particularly through its regular committees and through
exercises temporary committees of inquiry. These enable in particular
of the political opposition to examine the actions of the government
and to evaluate and to present political alternatives. Finally falls
the approval of the state budget does not fall within the scope of the
union law.

120

Advice to the Hessian state parliament

The fact that the LDS, as a state organ, adheres to the fundamental right to data
protection according to Art. 8 GRCh does not mean that for him too
the GDPR is applicable. Because the GDPR is just one of many
legal specifications of the protection of fundamental rights, which are mutually
compete, so that the fundamental rights are not directly binding on the
applicability of the GDPR can be concluded. Rather concrete
the LDS establishes this bond itself within the framework of its parliamentary autonomy,
by taking a position that corresponds to his constitutional status
data protection regulations (see Section 10.3).

IV. Application of the GDPR to the administrative area

The special importance of the LDS for the political-democratic process
and for the formation of the identity of the State of Hesse, however, only applies to theirs
political-legislative-parliamentary field of activity. It does not apply to
its administrative functions. As an organization with personal, material
and financial resources is the LDS managing authority. Therefore will
his administrative activity is covered by the scope of the GDPR.

Accordingly, § 30 HDSIG (about the opening clause of the

Art. 6 Para. 2 DS-GVO) the data processing of the HLT as administrative

hear and place them under my control.

10.2

Data protection in the Petition Act

During the reporting period, the LDS discussed a parliamentary group bill

the CDU, BÜNDNIS 90/DIE GREEN, the SPD and the FDP

May 11, 2021 on a law on the handling of petitions to the

Hessian state parliament (LT-Drs. 20/5734) and a draft of the parliamentary group DIE

LINKE for a law regulating the petition procedure in Hesse

State Parliament (Hessian Petitions Act) (LT-Drs. 20/5743) and led to both

Drafts through a public hearing on September 9, 2021. To the

I have the data protection regulations of these draft laws with the representatives

all parliamentary groups discussed a proposal for a new version and

drafted a regulation together with the state parliament administration

and presented at the public hearing. This was largely

HTL in the Hessian Petitions Act of December 19, 2021 (GVBl. 2021,

926) taken over.

121

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

For the regulation of data protection in the context of the petition process

the judgment of the ECJ of July 9, 2020 on the Petitions Committee of the

HLT are observed. Since the Petitions Committee "Tä-

activities ... of an official nature", the DS-GVO applies to him and he is as

Responsible according to Art. 4 No. 7 DS-GVO. At this judgment is

bound to the HLT as a party to the ECJ proceedings. However, after the

Results of my expert opinion on the validity of the GDPR for the HLT (s.

Section 10.1) between the administrative processing of petitions by the

Landtag administration and its processing by a member of the HLT as

Rapporteur and by the Landtag plenary to distinguish. only so far

the Petitions Committee performs administrative functions, the GDPR applies.

Insofar as the HLT exercises parliamentary activities, the Hessian ones apply

Constitution as well as the Rules of Procedure and the Data Protection Regulation (DSO)

of the LDS. For the control of data processing for administrative activities

I am responsible for the control of data processing for parliamentary

The data protection committee is responsible for activities according to § 11 DSO.

Data protection is regulated in Section 10 of the Hessian Petitions Act. This

The regulation reads as follows

§ 10 HPetG

(1) Personal data of the petitioner and the subject of the petition

may only be processed for the purpose of conducting petition procedures.

(2) Within the scope of exercising its rights, the committee is authorized to

to transmit gene data to the state government and other public bodies.

(3) There is no entitlement to inspect Parliament's petition files. The right to

15 of Regulation (EU) 2016/679

of the European Parliament and of the Council of April 27, 2016 for the protection of natural

persons in the processing of personal data, the free movement of data and

to repeal Directive 95/46/EC (General Data Protection Regulation) (OJ EU No. L 119

S. 1, No. L 314 S. 72, 2018 No. L S. 2, 2021 No. L 74 S. 35) is restricted insofar as

1. the protection of other important objectives of general public interest in the country

of Hesse the interest of the data subject in information and a copy outweighs

2. by providing information or a copy of the protection of the data subject or

the rights and freedoms of other persons are impaired or

3. the information or copy would reveal information which, according to a legal

regulation or its nature, in particular because of the overriding legitimate

interests of a third party must be kept secret.

(4) From the moment the petition is referred to the committee, supervision is incumbent

about the processing of personal data to the data protection committee of the Hessian

national parliament.

122

Advice to the Hessian state parliament

Paragraph 1 permits the processing of personal data insofar as it is necessary for

the implementation of petition procedures are required. This permission

Despite the validity of the GDPR and its application

primarily permissible because the state of Hesse has violated the opening clause of Art. 6

Paragraph 1 subparagraph 1 lit. e and paragraph 3 DS-GVO and the legal basis

can and must specify for the processing. The determination of purpose “only

for the purpose of the petition" establishes a strict earmarking and provides

indirectly clear when the data will be deleted in accordance with Article 17(1)(a) of the GDPR

Need to become.

The same applies to the permission of paragraph 2, according to which the petitioner

tion committee is authorized, within the framework of exercising its hearing

and investigation rights personal data to the state government

and other public bodies affected by the petition

are. This data is also subject to a corresponding earmarking.

Paragraph 3 excludes the administrative right to inspect files

out of. However, it also restricts the right to information and a copy of personal

related data according to Art. 15 DS-GVO for the three reasons mentioned

a. These restrictions on the rights provided for by the GDPR

affected person are objectively necessary and permissible under Art. 23 DS-GVO.

Paragraph 4 takes into account the differentiation required above between the

I have control over the administrative processing of the petitions and

the parliamentary treatment of the petitions by the deputies as

Rapporteur, by the committee in its parliamentary political

function and by the Landtag plenary session as a final political

important and decisive point.

The protection of the fundamental rights of the petitioners requires a fundamentally strong

Supervision of the processing of your data. As far as the state parliament administration

carries out the data processing and is therefore subject to the DS-GVO

Supervision by me with the help of the powers according to Art. 58 DS-GVO and § 14

given HDSIG. This essentially concerns the managerial activity

of the Petitions Committee, especially the preparation of the treatment

of the petition and the execution of the decisions of the petitions. This

Supervision does not have to be regulated in the Petitions Act, but arises

already from the HDSIG.

I have no supervision, however, over the members of parliament as reporting

officials, whose free decision is constitutionally protected by Art. 77, 95, 96

and 97 Hessian constitution is guaranteed. The data processing by

Rather, members of parliament are subject to the self-control of the state parliament, which he

data protection committee according to § 11 DSO. This body and

the Council of Elders have the task and have the necessary

opportunities to find suitable solutions to problems in parliamentary procedures

to get. This exception for MPs, the Petitions Committee and

the plenum is governed by paragraph 4. He transfers the supervision of the

Processing of personal data from the moment of transfer

of the petition to the Committee of the Data Protection Board of the LDS.

10.3

New version of the data protection regulations of the Hessian state parliament

As far as the GDPR does not apply to the parliamentary activities of the state parliament

applies, the LDS must guarantee the fundamental right to data protection

regulate themselves according to Art. 8 GRCh and the supervision of compliance with them

organize their own data protection regulations. This is done by the

HLT Privacy Policy (DSO) as Annex 4 to Rules of Procedure

of the state parliament, so far still in the version of January 18, 2014. Even if

the GDPR does not apply to parliamentary activities is the DSO

to adapt to the terms and structures of the GDPR in order to

to be connectable. Here are the findings from my report

to take into account the non-validity of the GDPR.

Together with the state parliament administration I have the new version of the DSO

supported by a draft of the regulations. This takes into account the

scope of application restricted to parliamentary activities of the HLT

rich of the DSO. Although the GDPR does not apply to this area of application

applies, the draft adopts definitions from the GDPR in order to

to be compatible with them. In a general permit

will be the processing of personal data upon perception

parliamentary tasks as admissible, insofar as they are necessary for the fulfillment of parliamentary

of lamentary interests is required and overriding ones worthy of protection

not conflict with the interests of those affected. special regulations exist

for the transmission of personal data for non-parliamentary

purposes, for data use for the purpose of joint parliamentary

rical activity of MEPs and parliamentary groups, for the electronic

Data processing for petitions and parliamentary documentation. Egg-

General regulations also set out the rights of the data subjects

Information, correction, deletion and storage limitation of

Data. Cooperation with processors was based on Art. 28

DS-GVO based detailed regulation. were newly added

also regulations on a list of processing activities and

to necessary technical and organizational measures to

adequately protect personal data. Eventually became

Advice to the Hessian state parliament

in the draft the previous regulation on the data protection committee of the HLT as

independent data protection supervisory body.

A new DSO of the HLT was not yet available at the end of the reporting period

decided but was passed by the LDS on February 23, 2022.

Employee data protection

11. Employee data protection

Employee data protection

The conditions of data protection of employees are massive

through the digitization of working life, the virtualization of work con-

clocks and workflows (see Home Office, Section 11.2) and dissemination

smart devices as work equipment or in the work environment (see GPS

Section 11.3) change. This enables the behavior and performance of

Employ easier to grasp more deeply and comprehensively. This development

has received an additional boost from the corona pandemic because

the work performance often only using information and

communication technology could be provided.

11.1

Current developments in employee data protection

Access controls, contact tracing, compulsory testing and working in the

Home office – the corona pan-

Demie but also new, independent data protection issues

caused. As topical and important as the topic is - the progressive

Digitization of the world of work and the problems connected with it

Employee data protection must not be forgotten.

Corona and employee data protection

With the expansion of testing capacities, the possibility of vaccination and

with the special regulations for vaccinated, tested and recovered people

In the spring of 2021, the interest of female employers also grew, understandably

and employers, the vaccination, recovery and test dates of their employees

to process.

This inevitably led to the question of the legal basis on which

Processing of health data in the employment relationship

could. The Conference of Data Protection Commissioners of the Independent

The supervisory authorities of the federal and state governments (DSK) had

Closing date of March 29, 2021 "Corona virus: proof of vaccination, proof

negative test result and proof of recovery in the private sector

and in the employment relationship are regulated by law!" (https://www.

datenschutzkonferenz-online.de) at an early stage of the necessity
advised to make legal regulations. There – against the background
the forthcoming federal elections – no corresponding legislative
be recognizable and at the same time inquiries from companies and
employees, I will have a handout on the subject in the summer

"Is the processing of the vaccination and recovery status of employees
permitted by employers?".
On November 24, 2021, the provision of Section 28b IfSG finally came into force.
She makes access to workplaces where physical contacts are not
can be excluded from complying with the 3 G rule (query
of vaccination, recovered or test status) and thus allows - at
Compliance with certain conditions – the processing of the under
health data arising from the 3-G check. I have this development
welcomed, since hereby the demands of the data protection supervisory authorities
was taken into account. Since my authority for concrete implementation
received many inquiries in everyday work, on November 25th I
vember 2021 on my website recommendations for data protection compliant
Implementation of the 3G rule published in the workplace (https://datenschutz.
hessen.de/datenschutz/arbeitgeber-und-bewerkte/empfehlun-
gene-for-data-protection-compliant-implementation-of-3-g).
The DSK also saw the need to clarify these and other issues
data protection issues in connection with the Corona Pandemic
my. Therefore, on December 20, 2021, the application help “Frequent

Questions and answers on the processing of employee data

in connection with the corona pandemic" (https://www.datenschutz-

konferenz-online.de/orientation aids.html).

In addition to the question of what data on the vaccination, convalescent or test status of the

Employees the employer is allowed to query and process, presented themselves

also questions about the extent to which he may communicate this data. Because the

Vaccination, recovered or test status of the employees is possible

a basis for trust in the company in personal

External contacts or visits to the company. This is before

Above all, it should be noted that the data on the vaccination, recovered or test status

of the employees' health data according to Art. 4 No. 15 DS-GVO, which

require special protection. Therefore, the publication of such

Data by the employer via the Internet is not permitted (see Section 2.6).

Due to the dynamic developments related to the

Corona pandemic, it can be assumed that in 2022 data

intellectual property issues relating to this complex of topics

will go out.

Digitization of the working world

Even if the corona pandemic is not the cause of the digitization of the

world of work, it has accelerated the process in some respects. The

Contact avoidance as the most effective means of combating infection has increased

a significant increase in working from home, for example, and

use of video conferencing systems and collaboration platforms.

Because from the employer's perspective, the control of work performance is often not

is considered equivalent to the possibilities in face-to-face operation,

new instruments for employee monitoring are increasingly establishing themselves.

The topics mentioned already show a large number of data protection

legal issues, here are some examples:

– How can a secure handling of personal data, the

process employees in the home office, be guaranteed? (see clause 11.2)

– What are the requirements for data protection-compliant use

of video conferencing systems and collaboration platforms, too

the background of any transfers of personal data

to third countries? (see section 4.2)

– To what extent is the monitoring of the work performance of employees

permitted using electronic systems in the home office and where

are here the limits?

As a special form of monitoring work performance

me in the reporting period the topics of video technology, geolocation and

Evaluation of driving behavior data in the logistics industry. The

have employees from several logistics companies

contacted us with the following questions (see Section 11.3):

– Is it permissible if the technology installed in a vehicle

traffic is monitored and additional image and sound recordings from

interior of the vehicle cabin be manufactured?

– May the GPS data processed for route planning also be used for other

other purposes (e.g. to record working hours or to prove a

working time fraud) can be used?

– Is the processing of driving behavior and vehicle data by employees

employers permitted?

Overall, the example of the logistics industry shows that

the digital transformation of the working world is already evident in some sectors

progressed. This involves the use of video technology and GPS

by no means reached the “end of the road”: the rising one

Use of information and communication technology across all types of

employment relationships leads to an ever-increasing

the amount of employee data. At the same time, the possibilities

of data analysis further improved and the use of algorithm-based

Decision support systems - for example in the application process - is

already a reality today.

The old federal government already had the resulting regulatory

recognized the need and commissioned the Advisory Board on Employee Data Protection to do so

to check whether there is an independent law on employee data

need protection. In January 2022, the Advisory Board will have its report with theses

and recommendations at https://www.denkfabrik-bmas.de/focus/

employee data protection published.

In its coalition agreement, the new federal government intends to

urgent to make new regulations on employee data protection, and

will certainly also take into account the results of the Advisory Board. With a view

to a new legislative process could also include the assessment

of the ECJ to the question submitted by the VG Wiesbaden, whether

the Hessian regulation on employee data protection in § 23 HDSIG den

The requirements of Art. 88 DS-GVO are met (Wiesbaden Administrative Court, decision of

December 21, 2020 – 23 K 1360/20.WI.PV, ZD 2021, 393).

The need to further develop employee data protection law

is not a new topic. Even with the amendment of the Federal Data Protection

Act 2009 and the regulation of individual issues of employee data

data protection in § 32 BDSG-old was determined in the legislative process:

“Section 32 contains a general regulation for the protection of personal data

Data of employees who compiled the data from the judiciary

do not change the principles of data protection in the employment relationship,

but only summarize and an employee data protection law

should neither make it superfluous nor prejudice the content.” (Printed matter

16/13657, page 20) A first attempt was made in 2010 with the “Draft

of a law to regulate employee data protection". The

However, the project failed – after much criticism – in 2013.

The steps taken to regulate employee data protection

I expressly support. As the report of the Advisory Council on

data protection has worked out aptly, is the responsibility of the legislature

thereby the challenging task of “the tension between

the human dignity and the constitutionally protected person

personal rights and interests of the employees as well as the

fundamentally protected rights and interests of employers

balanced requirements to regulate the mandatory protection

of employees through an effective data protection law

and also with a continuing dynamic digitization of the

work environment to bring about a fair balance of interests” (report of the

Advisory Board on Employee Data Protection, page 4 number II).

Employee data protection

11.2

Use of digital tools for employee monitoring

In the year under review, I received complaints in which employees stated

ben, through software applications on their business devices from their

being monitored by employers. Such applications are usually

not permitted under data protection law.

At least since the beginning of the corona pandemic, working in the "home

Office" widespread. Many people go to avoid contact

their office work from home. This enables the employees

to reduce their contacts and avoid infections. For employer

Women and employers can ask themselves whether their employees

carry out assigned tasks in the home office or the working hours

also use for private matters.

Against this background, there is a growing market for digital

monitoring of employees e.g. B. means of software applications for this

purposes to be installed on service computers. To improve performance and behavior

to enable employees to be checked, use such applications

a range of possible data that can be generated during the normal use of

IT devices are created. Starting with information that is easy to collect

– such as when an employee logged in on a device or

the screen saver was activated due to inactivity – the

number of keystrokes, the duration of those in focus,

applications used, the websites accessed in the web browser

to be recorded regular screenshots. On mobile devices

such as smartphones can also use GPS positions

and transaction data are processed.

When using Software-as-a-Service offers (SaaS), the

determined data is often transferred directly to the IT systems of the providers,

aggregated and evaluated there. Employers will then often

direct access to employee performance and behavior data

allows. In cases where employees also use their private devices

use for official tasks, or if private use

of e-mail and other Internet services using company devices

is approved, it is also not unlikely that the private

Communication and activity of employees is recorded and evaluated.

Against the background of the technical possibilities and the legitimate

Interests of employers, taking into account the personal rights of the

to be able to carry out employee performance and behavior checks,

The question therefore arises to what extent the monitoring of the work performance of

Employees using electronic systems under data protection law

is allowed.

The use of any tools to monitor employees is on

the data protection requirements of § 26 paragraph 1 sentence 1 BDSG

to eat.

§ 26 paragraph 1 sentence 1 BDSG

1Personal data of employees may be used for employment

relationship are processed if this is necessary for the decision on the justification

of an employment relationship or after establishing the employment relationship

niss for its implementation or termination or for the exercise or performance of

arise from a law or a collective agreement, a company or service agreement

(Collective agreement) resulting rights and obligations of the representation of interests

employees is required.

According to this, the processing of personal data in the employee

Permitted if they are used to carry out the employment relationship

is required. Such a requirement is stated, for example, for working hours

accepted. According to Section 16 (2) ArbZG, employers are required to

is obliged to record the working hours of its employees if they have the

working hours of eight hours per day stipulated in § 3 ArbZG.

An application that enables time tracking in the home office

and beyond that no personal data of the employees

processed, is therefore to be regarded as permissible under data protection law.

The legal situation is to be assessed differently if software goes further

operates data processing operations. Some products that come as software for

work time recording are advertised, determine the number of keyboard

punches or take screenshots of the screen on a regular basis. This is

generally inadmissible under data protection law, since such data processing

processing operations constitute a significant encroachment on the rights of employees

to informational self-determination, which is

purpose cannot be justified (BAG, judgment of 07/27/2017,

2 AZR 681/16, paragraph 21 ff).

As far as monitoring measures to uncover in the employment

criminal offenses committed in relation to the employment relationship, the strict preconditions

§ 26 Section 1 Clause 2 BDSG must be observed.

Employee data protection

§ 26 paragraph 1 sentence 2 BDSG

2Personal data from employees may only be used to uncover criminal offences

be processed if there are actual indications to be documented

justify the suspicion that the person concerned committed a criminal offense in the employment relationship

has committed, the processing is necessary and the interest in need of protection of the or

of the employee does not outweigh the exclusion of processing, in particular Art

and extent are not disproportionate to the occasion.

The monitoring of employees must then be used to detect

offenses are required. It applies that no so-called investigation

"into the blue" may take place, but already actual clues

for committing a criminal offense in the employment relationship.

These must be documented. In addition, data processing must also

actually be necessary for the detection of the offense and it is one

carry out a balancing of interests.

Under no circumstances is it permissible under data protection law to

general suspicion and to monitor preventively from the outset.

Exactly such a suspicion-independent and complete data processing

however, depending on the configuration, this is done using the most commonly available software

Employee monitoring, so that their use also according to § 26 paragraph 1 sentence

2 BDSG should only be permissible in rare cases. The mere suspicion that

Employees in the home office take care of private matters, legitimized

not their complete monitoring. Even if cases of labor

time fraud is to be assumed, the use of the described digital

Monitoring instruments are not always the mildest means,

to substantiate the suspicion of the crime.

Do employers use employee monitoring products that protect privacy
carry out legally impermissible processing operations, the
Imposition of measures according to Art. 58 Para. 2 DS-GVO can be expected.
Depending on the severity of the violation, a warning, an instruction that
Data processing in accordance with the provisions of data protection law
to bring, or a ban on the use of the software used in
come into consideration.
In addition, in such cases, the initiation of a fine procedure
consider, with employers not in the context of fine proceedings
can exculpate by the objection that the product used with
is advertised with the addition "GDPR-compliant". As responsible in mind
of Art. 4 No. 7 DS-GVO are employers according to Art. 5 Para. 2 DS-GVO for
responsible and accountable for compliance with the principles of processing
compulsory. Applications that are suitable for seamless monitoring

to enable the employees to be monitored must therefore be configured in such a way that
impermissible surveillance measures are ruled out from the outset.
Finally, it should be noted that works councils during the introduction
and use of technical facilities that are suitable for
monitor employee behavior and performance
§ 87 Section 1 No. 6 BetrVG have a right of co-determination. Also, the
processing of personal data, including special categories
personal data of employees for employment purposes
ment relationship, according to § 26 Para. 4 BDSG on the basis of collective

tive agreements permitted. In companies in which a company or

Staff council exists, should therefore prior to the introduction of such applications

operating agreements are concluded.

11.3

GPS tracking in employment

Employers are increasingly using GPS to track company vehicles

and thus also used by employees. Where are the data protection

legal limits of such surveillance? How can a localization of

employees are made data protection compliant by means of GPS tracking? It

may be permissible under data protection law, insofar as the interests of the employer

bers and the personal rights of employees in an appropriate manner

compensated and it is limited to what is necessary.

During the reporting period, I received several inquiries and complaints

dealing with the lawfulness of the processing of personal data

deal with GPS tracking.

GPS means Global Positioning System

tem). The technology is based on a global navigation satellite system

and is used for precise navigation or location determination. In here

context considered, a GPS transmitter is attached to vehicles

brought and serves to determine their exact location.

At the beginning of the year, a complaint was filed against an international

submitted to the transport company. The complainant reported

that GPS trackers were installed in the vehicles used there.

The reason given to the employees was that

the installation of the GPS tracker of the anti-theft device, the increase in efficiency,

the improvement of the service, the control of unauthorized private use

tion and the safety of drivers and vehicles

134

Employee data protection

serve. According to the complainant, the GPS data of the

Vehicles saved for six months.

As a result of my hearing on the categories of personal data

ten, the purposes and legal bases of the data processing procedure

the situation was as follows:

The company processed the following data: Name of vehicle user

Zers, the current location of the vehicle, the current speed

of the vehicle and the current Can-Bus data (i.e. ignition, mileage

counter, fuel consumption, fill level, engine revolutions).

For the purposes of processing, the transport company

led that the GPS tracking:

– Fast troubleshooting and increased efficiency in the routing

planning,

– ensuring compliance with tax regulations,

– driver safety (accident/breakdown assistance),

– the safety of the vehicles (anti-theft protection),

- the increase in efficiency in vehicle procurement (quality/wear

of vehicles) and

- Ensuring compliance with labor law requirements (abuse

the fuel card)

serve.

The responsible party set the legal basis for the processing

literal § 26 paragraphs 1 and 2 BDSG and Article 6 paragraph 1 subparagraph 1 lit. f GDPR

called. The storage period for the collected GPS data was set at six

months specified. In addition, the responsible company announced that

that the private use of company vehicles is prohibited.

My legal assessment found the following:

During the test procedure it became apparent that the use of the GPS tracker

in the described form violates the provisions of the GDPR

violates. I have my doubts about the legality of the company

informed of the data processing and pointed out in particular that

GPS tracking of company vehicles must be permissible under data protection law

can, insofar as it can be based on operational requirements. Before

against the background that GPS positioning improves the general conditions for our

permissible performance and behavior controls of the employees created

can be and for the employees a permanent performance and

Control pressure can arise is included in the review of necessity

set a high standard.

In detail, for the stated purposes of data processing by means

Capture GPS tracking:

Fast troubleshooting and increased efficiency in the

route planning

The processing of personal data is generally permitted if

if you are on one of the points in Article 6 Paragraph 1 Subsection 1 lit. a to f DS-GVO

Permission facts can be supported. Because of the opening clause

of Art. 88 DS-GVO is data processing in the employment relationship

to be measured against § 26 BDSG (its conformity with Union law is currently being reviewed by the ECJ in a preliminary ruling procedure).

With regard to GPS tracking and the associated storage of the personal data of the drivers come as a possible legal Basics in particular Article 6 Paragraph 1 Subparagraph 1 lit. b GDPR, specified by § 26 paragraph 1 sentence 1 BDSG (“Execution of the employment nisses"), into consideration.

Both regulations require that data processing be carried out in order to achieve pursued purpose is necessary. Especially when it comes to processing of employee data 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 Bring the interests of the employees and the employer as possible largely taken into account (BT-Drs. 18/11325, 98). One is required for this Examination on the basis of the principle of proportionality, which in turn requires that the controller pursues a legitimate purpose, that processing method is suitable for the realization of this purpose and it is the mildest of all equally effective available funds (cf. BAG, decision of April 9, 2019 - 1 ABR 51/17, para. 39, NZA 2019, 1055 (1059)). In addition, it must also be under consideration be appropriate to the circumstances of the individual case.

In the underlying case, I have found that the interference rectification and increase efficiency in route planning a legitimate Purpose according to § 26 paragraph 1 BDSG. To achieve the above Purpose is a fleeting snapshot (i.e. only current GPS tracking data available) but sufficient. A storage of

However, data is not required to fulfill the purposes pursued, so that

storage for a period of six months is not required

and is therefore inadmissible.

Compliance with tax regulations

According to general life experience, official vehicles are also used

are available for private purposes are actually used privately.

This is supported by the evidence of the first appearance (BFH, judgment of 4 December

2012 – VIII R 42/09). A private usage share for a company car

is not recognized by the financial administration if the person responsible

proves that the car is not used privately. As proof

contractually fixed usage bans apply. Also introducing one

GPS tracking tools can be an effective means of providing evidence

to tax authorities. Since the private use of company

but witnessing was forbidden from the outset, it was not clear why that was

GPS tracking to ensure compliance with tax regulations

should have been necessary. The person in charge couldn't either

explain that there is a corresponding requirement on the part of the tax authorities

would have given to the company. For data protection reasons

The storage was therefore not proportionate and therefore inadmissible.

The proportionality test related to the information interest of the

Employer's and the employee's personality rights therefore fell to

at the employer's expense.

Driver safety (accident/roadside assistance)

The collection and storage of GPS tracking data in order to

Accident or breakdown to ensure quick help is a measure

of occupational safety and according to § 26 paragraph 1 sentence 1 BDSG in

to be assessed in connection with the provisions of the Occupational Safety and Health Act.

The principle of necessity also applies here. In the specific case, it has already been

I doubt the suitability of the measure, since in the event of a

Accident available tools (roadside assistance, emergency call) for the

Safety of the drivers are likely to be more appropriate. In any case, the permanent memory

It is not necessary to save the GPS data of the vehicles for this purpose.

Vehicle security (anti-theft)

As far as it has been stated that GPS tracking (also) serves the purpose of

Theft protection and vehicle retrieval, I have

no need for constant detection of the vehicle position and a

Storage determined for this. For finding a stolen one

company vehicle, the event-related survey of the location of the

vehicle in the event of a determined vehicle loss (also

VG Lüneburg 4th chamber, partial judgment of March 19, 2019, 4 A 12/19, marginal note 39 f.).

Increased efficiency in procurement (quality, wear and tear of

Vehicles)

Data processing using GPS tracking enables efficient and

suitable vehicle types are identified. Enabled in procurement

vehicle tracking has potential for optimization, which is reflected, for example, in cost savings

savings could be made. By collecting and storing the Live

Can Bus data (ignition, odometer, fuel consumption, fuel level

and engine revolutions) the performance of the vehicles can be evaluated

and thus it can also be decided whether the vehicle type is suitable for the

is suitable for the intended purpose: data can be used for consumption,

to purchase vehicles that have lower fuel consumption.

In addition, it can also be relevant whether there are maximum kilometer specifications

are complied with, in accordance with the applicable lease agreements

must be taken into account.

In relation to the data collected for this purpose, however, the personal

employee protection interests outweigh, since it is a

storage of data collected in bulk from those affected.

I therefore suggested pseudonymising the Live Can Bus data

and to limit their storage to three months. After three months

the data can be aggregated, in which the average

Efficiency of the vehicles used is determined.

Furthermore, I have the submission of a voluntary self-commitment

demanded that the collected data not be mixed up with other employee data

merged and not used for performance and behavior controls

be turned. This request is the responsible company

complied.

Ensuring compliance with labor law requirements

(misuse of the fuel card)

A distinction must be made between preventive control measures for over-

checking compliance with existing labor law obligations and

Cause-related repressive employee controls in the case of a specific

cumulative initial suspicion.

Employee data protection

Unprovoked preventive control measures to check the

Compliance with existing employment law obligations

Preventive compliance controls that are not based on a personal

simple initial suspicion of a breach of duty or a criminal offense

hen, can under certain conditions according to case law

of the Federal Labor Court based on § 26 paragraph 1 sentence 1 or 2 BDSG

(BAG, decision of July 9, 2013 - 1 ABR 2/13, para. 20 et seq.). this applies

especially for those carried out according to abstract criteria, not an employee

particularly suspect, open, temporary and random

Monitoring measures aimed at preventing breaches of duty

or criminal offenses and without the implementation of which no

tens-directing effect can be unfolded. One such measure is

to announce.

Cause-related repressive employee control with concrete

documented initial suspicion

Thus a positioning system for the detection of a criminal offense is used permissible

can be, it is necessary according to § 26 paragraph 1 sentence 2 BDSG that a

concrete initial suspicion of a crime. The repressive employees

ter control has a significant impact on the personality sphere, since a targeted

monitoring takes place.

The admissibility requirement of a concrete suspicion prevents

This means that targeted surveillance can be used without restrictions.

In order for there to be concrete suspicion, there must be facts

which may serve as evidence of the existence of a criminal offence. It must be in

from a personal and spatial point of view, the objectively justified initial

suspected of committing a criminal offence.

Since § 26 paragraph 1 sentence 2 BDSG only criminal offenses in the employment relationship

regulates, the employer has an obligation to prove that a crime has been committed in

employment relationship was committed and the use of a tracking system

tems is the most effective means of reconnaissance. In addition, must

the specific suspicion of a definable group of employees

relate. It is not necessary that the suspicion arises exclusively

directed against a person. A driver pool would be conceivable, which is closer to

would investigate. On the other hand, it would not be permissible to have all employees under one

to raise general suspicion.

Even in the case of a repressive localization, a legitimate interest of the

employer at the control measure. As part of a

suitability test must reflect the employer's interest in the

uncovering the criminal offense to protect employee interests

outweigh the protection of privacy. As part of the

Interests are weighed up, above all, the type and severity of the crime,

the degree of suspicion and the severity of the interference with

personal rights taken into account. It can be due to proportionality

the significant encroachment on personal rights in the case of petty crimes

miss. In addition, the positioning for repressive purposes is to be limited in time.

As soon as the suspicion has been clarified or it becomes apparent that the crime has not been committed

can be uncovered and the measure thus remains ineffective

set the location of employees. Otherwise the action is taken

disproportionate and therefore inadmissible (see also Byers in Weth/Herberger/

Guardian/care, data and privacy protection in the employment relationship,

2nd edition 2019, paragraph 11 et seq.).

Both preventive and repressive measures do not allow for a permanent one

and comprehensive tracking of employees. Have limited storage

I consider admissible in the case of the above-mentioned constellations.

The company showed its full willingness to

to behave in accordance with data protection regulations, namely as explained in more detail above

procedure. The fact that a com-

complete documentation including a data protection impact assessment

was submitted for GPS tracking and the deletion of the stored

GPS tracking data after knowledge of the inadmissibility of their storage

has been confirmed. It should also be noted that the data stored during the violation period

cherated data were not used for employee checks. The employees

were comprehensively informed about the implemented measures.

In exercising my discretion, I have therefore abstained from submitting the

proceeding to the legal department of my company to initiate fine proceedings

apart from driving.

11.4

Conflicts of interest for data protection officers

The compatibility of the work as a data protection officer with others

Activities in the company or in the public body is always

Subject of inquiries or complaints to my authority. successor

some relevant constellations are shown.

The DS-GVO contains conflicts of interest for data protection officers in

Art. 38 Para. 6 DS-GVO only a short regulation. Further stipulations

does not contain the regulation. Accordingly, the practical application

of the standard with some uncertainties.

Employee data protection

Art. 38 GDPR

(...)

(6) 1The data protection officer may perform other tasks and duties. 2The

Responsible or the processor ensures that such tasks and

duties do not lead to a conflict of interest.

In principle, data protection officers can, in addition to those with the designation

associated tasks, cf. Art. 39 (1) GDPR, also other tasks

perform duties and duties, provided that these other activities are not allowed

lead to a conflict of interest. The absence of conflicts of interest

is closely related to the requirement of an independent

Activity, see Article 38 (3) sentence 1 GDPR. It is both about

a designation requirement as well as – after the designation – a

Organizational obligation of the person responsible and the processor.

Art. 38 GDPR

(...)

(3) 1The person responsible and the processor ensure that the data protection

in the performance of his duties, did not commission any instructions regarding the exercise

of these tasks. 2The data protection officer may from the person responsible

or not dismiss the processor for the fulfillment of his duties or

be disadvantaged. 3The data protection officer reports directly to the highest

Management level of the controller or processor.

(...)

Data protection officers may not have any position within the company
hold, in which they are informed about the purposes and means of the processing
personal data. To ensure this is due to the
structural differences of the respective company or the respective
Always make a case-by-case assessment for the industry. Nevertheless leave
work out some guidelines.
Conflicts of interest can regularly arise from the position in the company
arise (owners, members of management or the board of directors).
These individuals are original to the lawfulness of data processing
responsible for the person responsible or the processor and can
cannot effectively control themselves (see also Art. 38 Para. 3 Sentence 3

DS-GVO, according to which the data protection officer is directly responsible for the highest
reported to management level). Furthermore, the naming of
Managers not permitted: This applies in particular to the management of the
HR department (due to the associated responsibility for
the handling of employee data), the management of the IT department (due to
the responsibility associated with this function for the technical
organizational measures) as well as the management of the marketing or
operations department (because of the responsibility for handling customer data).
A designation for hierarchically subordinate positions such as
such as IT employees (in particular with administrator rights) or
Human resources department regularly inadmissible, provided that they are able
to determine or significantly influence data processing processes.

Furthermore, the appointment of a data protection officer is regular

inadmissible if this has a special economic interest in the

company is successful (e.g. shareholders and family members

the management).

For an IT security officer, the designation as

Data protection officer to accept conflict of interest.

IT security is comprehensive in order to detect misuse

Collections of personal data interested. A conflict of interest

is even more obvious if the IT security officer is responsible for the

implementation (with budget responsibility).

Even with compliance officers and the heads of the legal departments

a conflict of interest is often to be assumed. These are often in the

company's internal business processes in such a way that they

due to this more far-reaching task performance

the necessary independence in the evaluation of individual data processing

management processes. Furthermore, their activity with the collection is possible

a lot of personal data. However, this may vary depending on

the performance of the task may also have to be evaluated differently in individual cases (see

on this Bergt, in: Kühling/Buchner, Art. 38 para. 42; as well as deliberative Heberlein,

in: Ehmann/Selmayr, Art. 38 para. 23).

The appointment of a data protection officer is to be assessed rather critically,

who is at the same time a member or even chairman or chairman of the

rate is. The control authority of the data protection officer also includes

the data processing by the works council, cf. Art. 39 Para. 1 lit. b DS-

GMOs, which also apply within the framework of the participation and co-determination rights

may include employee data (see Heberlein, in: Ehmann/

Selmayr, Art. 38 para. 24; Bergt, in: Kühling/Buchner, Art. 38 para. 45: “Not

142

Employee data protection

recommended"). As a result of a submission by the BAG (ZD 2021, 701, 703 f.).

the ECJ will soon decide on this disputed issue.

Furthermore, conflicts of interest can even occur with external data protection authorities

appear. In this respect, the person responsible or the order

processor contractually regulate with the external service provider that this

does not engage in other activities that create a conflict of interest

the tasks of the data protection officer for this person responsible

or lead processors. This is particularly relevant if

far the data protection officer in addition to his work for the concerned

company is professionally active in the same line of business.

An impermissible conflict of interest would also exist if the external data

data protection officer provides IT services at the same time or the

Responsible or the processor in data protection relevant

represents litigation in court.

In order to avoid conflicts of interest, depending on the activities,

Size and structure of the facility some stipulations by those responsible

and processors are taken into account. Especially with larger ones

Company is the structural organization with the respective tasks

and competences within an internal guideline,

so that awareness of any conflicts of interest is increased

and these are as obvious as possible from the outset (see Ar-

tikel-29 Working Party Working Paper 243 – Guidance in relation to

Data Protection Officer (“DSB”), p. 19 f.).

In the event of a conflict of interest, I have various supervisory rights

measures available. In addition to the notice of a violation

against the DS-GVO towards the person responsible or the order

Processor according to Art. 58 Para. 1 lit. d DS-GVO I can according to § 40 Para. 6

Sentence 2 BDSG demand the dismissal of the data protection officer if

there is a "serious conflict of interest", cf. Art. 58 Para. 6 DS-

GMO. However, not every conflict of interest justifies the dismissal,

Rather, it must be obvious (e.g. to the head of the IT department)

(see Dix, in: Kühling/Buchner, § 40 marginal number 17 with w. N. also on the question of

compliance of the regulation with European law). Furthermore, violations of

the avoidance of conflicts of interest in accordance with Article 83 (4) (a) GDPR

fined.

143

Art. 58 GDPR

Each supervisory authority has all of the following investigative powers that

allow her

(...)

d) the controller or the processor of an alleged violation

to point out against this regulation,

(...)

(6) 1Each Member State may provide by law that its supervisory

have additional powers in addition to those listed in paragraphs 1, 2 and 3

powers. 2The exercise of these powers may not affect the effective implementation

of Chapter VII.

§ 40 BDSG

(...)

(6) 1The supervisory authorities advise and support the data protection officers

Consideration of their typical needs. 2You can request the dismissal of the

data protection officer request if she or he to fulfill her or his

does not have the specialist knowledge required for the tasks or, in the case of Article 38 paragraph 6, the

Regulation (EU) 2016/679 there is a serious conflict of interest.

(...)

Art. 83 GDPR

(...)

(4) In the event of violations of the following provisions, in accordance with paragraph 2

Fines of up to EUR 10 000 000 or in the case of a company up to 2%

of its total worldwide annual sales of the previous financial year

imposed, whichever of the amounts is greater:

a) the obligations of controllers and processors pursuant to Article 8,

11, 25 to 39, 42 and 43;

(...)

Section 7 (2) HDSIG takes over the regulation for Hessian public bodies

of Art. 38 Para. 6 GDPR.

§ 7 HDSIG

(...)

(2) 1The data protection officer may perform other tasks and duties.

2The public body ensures that such tasks and duties do not become one

create a conflict of interest.

(...)

Employee data protection

There is a conflict of interest with official data protection officers

similar to the non-public area regularly with the management of the authorities,

with the mayor of a municipality as well as with prominent management

activities (in particular in the management of the human resources department and in the

management of the IT department). The appointment of members of the staff council

is due to the control obligations of the official data protection officer

to evaluate critically towards the staff council. Basically allowed

is the activity in the legal department without a management function as well as the management of the

Audit Office.

The sanction options of my authority are in the case of official data

protection officers noticeably restricted. In this respect, according to Art. 58

Paragraph 1 lit. d GDPR i. V. m. § 14 paragraph 1 HDSIG the public body on one

indicate violation. In the event of an unresolvable conflict of interest

to be dismissed, cf. Section 6 (3) sentence 3 HDSIG.

§ 14 HDSIG

(1) 1The Hessian data protection officer shall take within the scope of the

Regulation (EU) No. 2016/679 the powers according to Art. 58 of Regulation (EU) No. 2016/679

true. 2If the Hessian data protection officer comes to the conclusion that

Violations of the regulations on data protection or other deficiencies in the

processing of personal data, he or she shall notify the public

Provide and give this prior to exercising the powers of Art. 58 Para. 2 Letter b

to g, i and j of Regulation (EU) No. 2016/679 Opportunity to comment within

a reasonable period of time. 3From the granting of the opportunity to comment

be waived if an immediate decision is required due to imminent danger or

public interest appears necessary or a compelling public interest

opposes. 4The statement should also contain a description of the measures

made on the basis of the notification by the Hessian data protection officer

have been. 5The exercise of the powers according to Art. 58 Para. 2 Letters b to g, i and j of

Regulation (EU) No. 2016/679 informs the Hessian data protection officer

relevant legal and technical supervisory authority.

(...)

§ 6 HDSIG

(...)

(3) 1The public body ensures that the data protection officer at the

performance of her or his duties, no instructions regarding the performance of these

receives tasks. 2The data protection officer reports directly

the highest management level of the public body. 3The data protection officer

may not withdraw from the public body because of the fulfillment of his or her tasks

appointed or disadvantaged.

(...)

Should there be any uncertainties about any conflicts of interest,

my authority can be contacted for further discussion.

Finally, it should be pointed out once again that the contact details of the

are to be communicated to the data protection officer of my authority, Art. 37 Para. 7

GDPR. A registration form is available on my website for this purpose.

Art. 37 GDPR

(...)

(7) The person responsible or the processor publishes the contact details of the

data protection officer and communicates this data to the supervisory authority.

146

web, advertising

12. Internet, Advertising

web, advertising

12.1

It's human in the network - From the colorful everyday life of

complaint handling

As a supervisory authority, I stand in the protection of personal rights in the

first row and fulfill a variety of important ones assigned by law

Tasks. It is precisely because of this that I am not only associated with important and

confronted with fundamental questions of data protection law, but also frequently

with all too human, smaller and larger worries of digital everyday life.

As an independent data protection supervisory authority, I have an extensive

Catalog of tasks assigned, e.g. in Art. 57 GDPR, § 40 BDSG

and Section 13 HDSIG. The processing of complaints takes a

particular importance and a significant part of the daily work

the authority (item 1).

The legislator has the right to lodge a complaint with a data protection

authority has been accorded great importance. According to Art. 57 Para. 1 lit. f

DS-GVO, the supervisory authorities have to deal with complaints, especially from

concerned persons deal with, the subject of the respective complaint

investigate to a reasonable extent and the respective Complaints

and complainants within a reasonable period of time about the

report the progress and outcome of the investigation. The complaint

is possible without any form or deadline requirements and without incurring any costs

arise for those who complain. Also should them because of their

Complaint accrued no disadvantages by the responsible body.

In fact, the complaint is a well-suited means by which those affected

the competent supervisory authority on a specific data protection law

Draw attention to the problem and thus receive individual help in individual cases

can. At the same time, the supervisory authority can use this method to systematically

uncover and remedy physical deficiencies in those responsible.

Unfortunately, not every complaint lives up to these lofty claims

and goals fair. Again and again my employees are

also with questionable content, whimsical, abusive and occasionally

very amusing cases that we as a regulator face

nevertheless have to deal with the content.

It is inherent in the right of personality that in the case of (supposed)

recently there is an individual and personal concern or

at least perceived subjectively. In this respect, not a few

complainants when writing the complaint

en clearly emotionally agitated. Especially when it comes to data protection

Problems related to the Internet is the e-mail program

or the complaint form on my website just a few clicks from the

Removed website or app that gave rise to the complaint. Not

Rarely do such complaints give the impression that the

the complainant felt the need

with a short-term satisfaction with a complaint against a just

create perceived injury or disadvantage.

However, this is not always originally related to the

Processing of personal data. It is not uncommon for

obviously used to create a "secondary theater of war"

for already existing, other disputes and with the

to report alleged violations by the other party to the supervisory authority. So

I often get complaints, e.g. B. from dissatisfied customers,

who share their anger about an unfortunate business relationship

a complaint about cookies or data protection notices on the company

mens website vent. Complaints are always being made

the websites of business competitors or against private individuals

one with which the complainant has other personal or family ties

has disputes.

For example, during the reporting period I had to respond to a complaint

father against his own adult son, who on his pri-

vaten website as a hobby genealogist the family tree and thus also

had published the biographical data of his parents. The data protection law

fought family quarrel produced in addition to the usual, preparatory

Correspondence two formal notices, one urgent and one main

ren before the administrative court, a petition to the Hessian state parliament

father's and another of the son's as well as a supervisory complaint

against the case worker. However, the website is now offline.

Especially shortly after the GDPR came into force, but occasionally still today,

can also be the misunderstood reference to the right to complain to the

supervisory authority make their work more difficult. data protection information

Art. 13 DS-GVO, which must be granted for every data processing

always also a reference to the right of appeal to the supervisory authority

contain. The contact details of the HBDI frequently given therein are

again and again with the contact details of the actually responsible office

changes. Occasionally, the right to complain under data protection law is even

as a general right of appeal against any decision of the responsible

literal misunderstood, whether or not related to processing

148

web, advertising

related to personal data. So reached me

For example, numerous objections to fines due to

speeding violations or complaints against the arrest

of broadcasts without any reference to data protection law.

Unexpected legal hurdles can also arise when processing requests

hard to show up. For example, data protection law does not provide for responsibility

literal, who decide on the respective data processing operations

and therefore also have to be legally responsible for them, must be of legal age.

An 11-year-old child who discloses someone else's personal information in a

social network spread worldwide, is therefore also responsible.

Exactly this case was brought to me by way of a complaint.

Even the determination of a legal guardian or the wording

a cover letter that an 11-year-old could understand would be in this case

become difficult. Fortunately, the background of the case turned out

but as a misunderstanding on the part of the complainant, so that the latter

Complaint withdrew and deeper research into protection of minors

controller in data protection law became superfluous.

Occasionally they reveal themselves in complaints and complaints brought to my attention

Concerns also completely wrong and often amusing ideas of the
data protection and the tasks and powers of a supervisory authority
en. Thus, the HBDI is neither technically able nor legally authorized to all
to compile data stored worldwide about a specific person
bear and to provide information or even to delete. The HBDI also does not carry any
intelligence operations out, can not feel persecution
help through supposedly bugged household items, inquirers
obtain personal data from third parties, unwanted apps on
delete the mobile phone of a complainant, a fee for the
Introduce the sending of e-mails or the obligation to pay the broadcasting
expose trags as a feathered pet with its excretions
rendered the television unusable.
Complaints about data protection stem from the full life and their
Processing often requires expertise in data protection law as well
Humour, empathy or dealing with websites that otherwise
should not be accessed by business computers. At legitimate
Complaints can be good for the complainants
helped and data processing methods improved and made more secure
become. On the other hand, unfortunately, a large number of unpleasant,
querulous or apparently abusive complaints
lifted. Since the complainants just at
such complaints often particularly emphatically on the legal

owed processing of their request, these must also

sometimes with a lot of work and time and deferring others

tasks to be processed.

12.2

The cookie consent - curse and blessing at the same time

Countless complaints concern the use of cookies and the

binding of services relevant to data protection law on websites. In the

In most cases, the website operators require the consent of the users,

to set cookies and thus be able to process tracking data. often

However, the users cannot or do not want to log in before each visit

deal with this topic in detail on a website.

Cookies are ubiquitous when using the internet. While some Coo-

are technically necessary for the respective basic function of a website

to make available, others are used to provide user data

collect and create user profiles, the web analysis and in particular

serve the marketing of target group-oriented advertising. Above all

the latter entails considerable risks for the personal rights of the users, since

it with the creation and processing of extensive personality profiles

(see also Section 13.2. in the 48th TB and Section 13.1 in the 49th TB).

Since 2009 there have been European legal requirements for the setting of

Cookies and for the use of similar technologies in December

2021 in the new Telecommunications Telemedia Data Protection Act (TTDSG)

were implemented. Section 25 TTDSG stipulates that cookies are fundamentally

only with the consent of the user on his end device (PC, smartphone

etc.) can be stored and read from there. exceptions apply

only if it is absolutely necessary to set and read the cookie

is required to provide a service expressly requested by the user

To make available. However, this regulation primarily serves the purpose of integrity

the end device used with which a specific service is accessed,

and only indirectly the protection of personal rights. That's the way it should be

be prevented that service providers without knowledge and without consent

users store cookies or other data on their devices and

read out and thus use the end devices for your own data processing.

However, the TTDSG does not regulate what can be done with set cookies and comparable

ble technologies may be made and for what purposes and in

the extent to which user data may be collected and processed.

This is to be regulated in a European ePrivacy regulation

was originally intended to come into force together with the GDPR in 2018.

150

web, advertising

However, since the legislative process for this is still not

sen, currently also apply to data processing using cookies

general rules of the GDPR. According to this, certain data

processing related to cookies that have little impact on

have personal rights (e.g. in the case of technically necessary

First-party cookies), exceptionally without the consent of the user

be allowed. As a rule, however, especially when it comes to tracking

or other service providers are involved for the collection and processing

of data by means of cookies, a consent according to Article 6 Paragraph 1 Subparagraph 1 lit

GDPR required. This can be done with the required according to § 25 TTDSG

consent to the setting of cookies.

Ultimately, providers therefore need in all cases in which cookies and

comparable technologies not only for technically necessary ones by the user

desired purposes that are at the same time unobjectionable in terms of personal rights

are used, the user's consent to the setting of cookies

as well as in the subsequent data processing with them. In order to

fetch, most website operators use a so-called cookie banner

the first time the website is used, this is superimposed optically

and more or less detailed information about cookies and buttons

contains with which the consent can be given.

However, experience shows that most users have little interest

have and often cannot or do not want to take the time before the

Visiting a website for detailed information on an abstract topic

to read and based on this a conscious and differentiated decision

about the use of sometimes dozens of cookies. aggravating

on top of that, it is in layman's terms, even if the providers are detailed and

inform transparently about it is hardly possible, the complex legal

and technical background of data processing with cookies

carry out and assess their impact on personal rights.

For these understandable reasons, most users try the

"Processing" of cookie banners towards the fastest possible variant

complete. The website operators knowingly offer one as a rule

prominent option to give consent with a single click

grant and at the same time hide the cookie banner, since this

also corresponds to their business interests.

Against this background, it is particularly important that the providers

Obtaining consent at least the legal requirements

meet and allow users to have a real, unbiased

and to make voluntary decisions. For example, next to a

simple way to give consent an equally convenient

be offered the opportunity not to give consent and the set-

zen of cookies and the associated data processing.

With regard to the design of data protection-compliant cookie consent

In view of the few concrete legal regulations, there are many

ambiguities. This is one of the reasons why the practice of the providers is very correct

many cases do not yet comply with the applicable legal requirements

match. In order to make this more understandable, the data protection conference in

December 2021 the guidance of the supervisory authorities for providers

and providers of telemedia from December 1, 2021 (OH Telemedien

2021) (https://datenschutz.hessen.de/sites/datenschutz.hessen.

de/files/DSK102_OH-Telemedien_20.12.2021.pdf), with which the same-named

Orientation guide from 2019 has been updated. In it are found

detailed and precise information, which exact data protection law

Requirements when obtaining cookie consent apply.

The federal legislator has a possible new system in § 26 TTDSG

created, with which the obtaining and granting of cookie consents in

be simplified in the future for both providers and users

should. For this purpose, neutral bodies (so-called PIMS – Personal Information Ma-

Management Services) on a fiduciary basis for the management of consents

take over and mediate between users and providers. That's how it should be

Users are enabled to make decisions at a central point in each case

to meet the desired scope of data processing, to which the various

which providers are equally bound. The decision will thus

brought forward in time and both users and providers would be relieved of the burden

exempted, immediately before each use of a new website consent

to demand or to grant. Before the possible establishment of PIMS

However, a more specific legal ordinance is required first

by the federal government. So it will be some time before

shows whether PIMS actually brings the hoped-for simplification when granting

will entail consents. Given the different

interests of those involved and a lack of economic incentives to

However, there are certain doubts about this.

Until the legislator special rules for data processing with cookies

and comparable technologies creates and/or through the establishment

PIMS result in at least simplifications in practice is everyone's responsibility

individual providers of telemedia when using devices that require consent

Services the task of obtaining legally effective consent from users.

In doing so, all legal requirements must be observed and the users informed in detail

and to provide information in a comprehensible manner, without overtaxing them at the same time

deterring is a challenging and difficult task.

152

web, advertising

However, it must not be forgotten that the providers themselves

have at hand, about the services integrated in their offers and

to decide the number and quality of the cookies used. je

fewer services that are problematic under data protection law are used, the

less effort has to be made by the provider when obtaining the necessary information

operate consents. Not least for this reason, the providers should

of telemedia the services integrated into their websites and apps

question and check whether they are actually needed or not much

are easily dispensable or at least through more data protection friendly

Alternatives can be substituted.

13. Social affairs, video surveillance

social affairs, video surveillance

13.1

Federal Participation Act: Working aid “Data protection in the Rehabilitation"

After a project "Data protection in carrier-transmitted

comprehensive rehabilitation process" at the federal working group for rehabilitation

tation (BAR) in Frankfurt am Main was successfully completed, I was again

as representatives of the federal states in a follow-up project based on this

Member of a project group for the development of a working aid

above topic. Legal background for seeking

Another such work aid that could be used throughout Germany was the

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

This project was also completed in summer 2021 with good results

be terminated.

In autumn 2019, after the successful completion of a (first)

project, the creation of a work aid on the subject of “data protection

in the cross-carrier rehabilitation process" (cf. my contribution in the 48th TB,

6.4) approached the members of this project group again to explain the complex

Topic "Data protection in rehabilitation" in another (follow-up) project

take up and deepen.

It was the common goal of the project group here, not yet deepened

considered data protection aspects in the practical cooperation in the

engage in the rehabilitation process. Specifically, it should be about the

Cooperation of the rehab provider with service providers, the process

sen “needs identification”, “service implementation” and “activities for and

after the end of a service" as well as the cross-sectional topics "expert opinion"

and go to "discharge reports".

In addition to the BfDI, HBDI and representatives of the BAR, these were also participants

Project group again representatives e.g. from

- Federal Ministry of Labour and Social Affairs,

– Federal Ministry of Health,

- German Federal Pension Insurance,

– German statutory accident insurance (DGUV),

- Federal Employment Agency,

– National Association of Statutory Health Insurance Funds,

– for the federal states: Ministry of Labour, Health and Social Affairs

NRW,

- for the integration offices: Center for Family and Social Affairs Bavaria.

The group of actors involved was also asked about their perspective

to be able to involve, in addition to representatives from

the practical provision of rehabilitation services. This included

e.g. B. the areas of service providers or associations of people

disabilities.

At a total of nine events organized by the BAR in Frankfurt am Main

deokonferenz dates in the period from December 2019 to July 2021 was announced in

all-day working sessions the project topic by the participants

and participants elaborated. There were also numerous bi- or

multilateral specialist exchanges, topic processing or coordination

between different project participants. As in the previous project

the discussions between the representatives of the various

Institutions always considerate with regard to the respective concerns and were

constructively and pragmatically oriented. That's how it was for everyone to work together

participants, both professionally and interpersonally, once again pleasant and fruitful.

In the last meeting of the project group in summer 2021, the working

help "Data protection in rehabilitation" were passed unanimously.

From my perspective, the jointly developed result can be good

let see:

- On more than 60 pages, the topic is presented in all its facets (not

most recently also from the perspective of data protection),

presented and explained in terms of content and classified legally.

- Then in illustrative representations on more than 20 pages

ten examples of permissible data collection and transfers in the

rehabilitation listed.

– Finally, the work aid contains numerous sample forms that

were integrated into more than ten pages.

In total, this resulted in a work aid with over 100 pages.

In autumn 2021, the BAR initially published it in its final status

sent to the project group and subsequently made public. she stands

now available on the BAR website for download at https://

www.bar-frankfurt.de/fileadmin/FILE-LIST/_publikationen/reha_basisn/

pdfs/AH_Datenschutz_II_final_barrierearm.pdf and can also be saved as

bound brochure can be obtained there.

social affairs, video surveillance

For the concerns of data protection I can, as in the previous project

balance again that BfDI and HBDI help shape in a positive sense

were able to influence and have now helped to achieve a result that

the data protection perspectives in the challenging and difficult

factual connections between the different rehabilitation phases

taken into account.

13.2

Video surveillance in shopping arcades

Irrespective of the ownership structure, it is a

shopping arcade around a publicly accessible space. A surveillance

must be measured against the relevant legality requirements

permit.

In 2019, I received several complaints about video surveillance

development in and around a shopping arcade with adjoining residential buildings

a property in a downtown location. The complaints were made independently

from each other by two private individuals as well as a civil rights group.

Presentation of the location

In detail, the shopping arcade consisted of ten shops,

three restaurants and a theater. The basement offered

Parking in a public underground car park. The adjoining residential

complex (with over 200 apartments) consisted of several buildings, with

14 mainly publicly accessible entrances and stairwells.

There was a park in the immediate vicinity of the facility

and a drug substitution facility, which is part of a federal

wide heroin study was set up.

I asked the camera operator for information in accordance with Art. 31 GDPR

asked. The participation was initially delayed, but this gradually changed

threat of fines changed.

The camera operator reported that in the past there had been

numerous cases of drug-related crime, drug consumption, property

termination, burglaries in apartments and basements, theft and physical

Attacks against passers-by and employees, some with serious

would have suffered ultimate consequences. Also due to those in the neighborhood

lying drug substitution facility consider itself a “problematic

Milieu" in the passage and the adjacent residential building complex.

Staircases and alcoves would be used for sleeping, drug dealing and

-consumption used. By exercising the domiciliary rights, the

Surveillance for security, deterrence and security

carried out on evidence.

Review of video surveillance

The subject of the test was the video surveillance of the public

and private space, the technical and organizational design of the

Monitoring and compliance with transparency obligations. During the exam

a distinction was made between video surveillance in residential

complex and surveillance in and around the shopping arcade.

residential complex

The video surveillance in the residential complex was

administrative investigation civil court ruled that a claim

on removal of the camera according to § 823 Abs. 1 BGB i. V. m. § 1004 paragraph 1

BGB i. In conjunction with the right of personality derived from Article 2(1) of the Basic Law

exist. The lawsuit filed by a former resident of the condominium against the

operator of the camera, who was also the owner of the residential complex,

was therefore unsuccessful in this matter. A claim for the removal of

disputed cameras existed - taking into account all the circumstances

of the individual case and after a comprehensive weighing of goods and interests

involved – so not.

During an on-site inspection, it was also found that

no private areas (such as apartments or balconies) from the surveillance

were included. The monitoring took place outside, in the

Commonly used, hard-to-see stairways and

Niches in which criminal offenses occurred repeatedly.

Adjustments were only necessary here insofar as the tenants

were to be fully informed about the surveillance. This was done using

a circular.

passage

Within the shopping arcade, video surveillance was implemented using in

test criteria common to test practice. This included currency

the legitimate interests, the need for monitoring and

a balancing of interests. When checking legitimate interests

it had to be taken into account that a third-party interest according to Art. 4 No. 10 DS-GVO

came into consideration, since this is a typical constellation in shopping centers

158

social affairs, video surveillance

existed, in which the landlord carried out the monitoring also in the interest of his

Shop tenant operation.

The camera operator stated that the surveillance of the passage

finally within the property of the operator, i.e. in private

area. Therefore, the first thing to check was whether the shopping arcade

considered public space.

Rooms are publicly accessible if they are dedicated to public transport.

are met or according to the recognizable will of the entitled person by anyone

can be used or accessed.

In the case of a shopping arcade, the operator wants it to be

rich (e.g. in shop windows) can be used or entered by anyone

can. The ownership of the observed object is first

irrelevant. Only the one opened by the entitled person is decisive

Actual possibility of use by the general public, d. H. an un-

certain group of people. This includes e.g. B. Showrooms of a

museum, sales rooms of a department store, a

ter staircase to a doctor's office or law firm, counter halls

of a train station as well as the platform or the station forecourt. Also

the prior purchase of an admission ticket or the need for an

melde does not stand in the way of this if the opportunity is open to everyone.

It was the same with this shopping arcade. certain access

there were no prerequisites, so that here from a publicly

accessible space was to go out.

The use of video surveillance equipment in the interior areas of the

passage, at the delivery entrances, in the underground car park and the

access to the garage and the garbage dump was mostly not objectionable.

The camera operator was able to obtain far-reaching information and specific

Submit documentation on administrative offenses and criminal offenses that

an increased need to protect property from damage caused by vandalism

justified. In weighing up the concerns, interests prevailed here

of the camera operator to the general personal rights of the

passage visitors.

surveillance of the environment

The cameras mounted outside the passage were so

directed that they from the outer skin of the property in the public

pointing into the room (street / sidewalk). The property line was there

unmarked and seamlessly paved. For outsiders

was not clear where monitored areas are located and whether

if image areas are blackened. All passers-by at the passage

walking along, as well as people walking the adjacent railway underpass and

used the adjacent traffic space, had to be protected by a far-reaching

go out video surveillance.

As part of the necessity test, it had to be clarified whether the video surveillance

tion was suitable for achieving the purpose and whether alternative measures that

do not intervene or intervene less deeply in the right of personality, in concrete terms

were preferable in individual cases. Various purposes were presented (danger

defense, deterrence, preservation of evidence, security of

employees). For those installed on the outer skin of the passage and in

video cameras aimed at the public space, however, could not

reasonableness and no adequate justification for the purpose are presented,

so that eight cameras were dismantled.

information signage

On the basis of Art. 13 Para. 1 and 2 DS-GVO, a Vi-

deomonitoring of publicly accessible rooms on the upstream

sign to point out the following:

– circumstance of observation – pictogram, camera symbol,

– Identity of the person responsible and, if applicable, his representative

(according to Art. 27 DS-GVO), name including contact details,

- Contact details of the company data protection officer - as far as

called, but then mandatory,

– Processing purposes and legal basis in keywords,

- Indication of the legitimate interest (insofar as the processing is based on Art. 6

Paragraph 1 subparagraph 1 lit. f GDPR is based),

- if necessary, duration of storage,

– Reference to the other mandatory information (in particular information

right, right of appeal, recipient of the data if applicable) and the

access to this.

The signage was applied in the process in accordance with the

fits.

14. Economy, banks, self-employed

Economy, banks, self-employed

14.1

Self-disclosures are also in the case of encryption of stored data

granted

Personal data is often encrypted for security reasons

saved. If these are decrypted for processing and the

Responsible hereby access to the data, the encryption is available

not object to the provision of information.

On January 13, 2018, the new EU payment services

implemented the Payment Services Directive 2 (PSD2) into national law.

As a result of the implementation, various improvements are in force for consumers

kicked. Above all, however, two new services were established, the consumers

independent of credit institutes. In these services

these are payment initiation services and account information services.

A payment initiation service can be commissioned by a payer to

initiate a transfer from his bank account, e.g. B. around in

to carry out a payment transaction online. Account Information Services

provide an account holder with consolidated information on one or more

reren bank accounts available and third parties can gain from it

Provide credit rating information. Both services can

Execution of payments can also be combined with each other.

Both services require access to the bank account and thereby

recognizable postings in the form of payments and incoming payments.

The use of these services therefore also creates a comprehensive insight

the service provider in the financial situation as well as in the consumer and

Payment habits of the user and account holder.

However, all services are subject to the PSD2 and thus also the

Services of the aforementioned service providers of the DS-GVO. You must therefore

be provided in accordance with data protection. Above all, this requires a limitation

adjustment of the data processing to the commissioned purpose of the service. One

Data processing without the appropriate authorization may not take place.

However, if a correspondingly extensive order is placed, a

correspondingly extensive data processing permitted. That's why

I recommend careful consideration of the scope of such a service

before placing an order and using these services sparingly. The

benefits and the losses associated with the use of the service

Privacy should be carefully balanced.

Due to the application of the GDPR to these services, regardless

of their admissibility under data protection law, is also an observance of the

Rights of data subjects required by the service provider. In

In one case of a complaint, a self-assessment pursuant to Art. 15

DS-GVO not carried out. The service provider relied on the

Data encrypted for security reasons. The encryption of the data

lead to their anonymization. A processing of personal

Data about which information could be given is therefore not available. To the

partially corresponded to the data protection declaration used. In this

was also pointed out to the encryption and that the

Data only from the person concerned and using the necessary

such key could be retrieved. This key would lie with him

service provider not before. He could therefore neither access the data nor

provide information in accordance with Art. 15 GDPR.

However, the content of the service contradicted this. He saw an extensive

rich processing and evaluation of the stored personal data

data before. Such processing without prior decryption

of the data was not plausible. The service provider recognized this after mine

also pointed out and then changed its data protection declaration. This

now explicitly refers to the processes through which the service provider also

personal data decrypted processed and this also through

employees can be read. All processes were of the purpose of

Processing included so that there was no unlawful processing. The

The scope of the processing was only incorrect in the data protection declaration

shown what is happening with affected persons and employees of the service provider

had led to misunderstandings and a refusal to provide information.

The requested information was also given on my references. Additionally

the internal processes were redesigned in such a way that later information

requests are granted in accordance with data protection regulations. In the future he intends to

Service providers the automated provision of information according to Art. 15 DS-GVO.

14.2

Right to information vs. tipping-off ban

Despite the existence of a right to information according to Art. 15 DS-GVO

Personal data stored by banks under certain conditions

not provide information to those affected.

The topic "Scope of the right to information according to Art. 15 DS-GVO" in

connection with account terminations or refusals of contractual

conclusions is always the subject of complaints that reach me.

162

Economy, banks, self-employed

The subject of these complaints is often that a bank

relationship with the complainant without giving reasons

unilaterally terminated. When asked about the reason for the cancellation

The bank then often appeals, at least rightly so under civil law

to the provisions of the terms and conditions, the contractual relationship without specifying

reasons to terminate.

In terms of data protection law, the scope is important when evaluating such matters

of the right to information according to Art. 15 DS-GVO. After

Art. 15 GDPR, data subjects must be given information as to which

Personal data is stored. This means that one in the system of

Bank customer-specific stored reason for the cancellation

must also be included in information according to Art. 15 DS-GVO if

under civil law, a statement of reasons is not required. civil

termination may be effective without giving reasons. This

however, does not change the scope of the obligation to provide information under Art. 15 GDPR.

However, the right to information is fundamental to the

responsible to claim. The mere request for termination,

The reasons for which the bank terminated the contractual relationship are

usually not as a request for information according to Art. 15 DS-GVO or even as

Specification of an already existing request for information in the sense

of sentence 7 of recital 63 DS-GVO to be interpreted, provided that these

Demand made without reference to the right to information.

Recital 63 sentence 7 GDPR

The controller processes a large amount of information about the data subject
person, he should be able to request that the data subject specify which
Information or which processing operations your request for information relates to before
he gives her information.
If, however, as part of the specification of the request for information
according to Art. 15 DS-GVO, the reason for the termination is explicitly asked,
this is usually through the bank to the person concerned, provided
saved, also to be informed. The reason for termination would
thus brought to the attention of the person concerned. Reasons for a unilateral
Termination by the bank is often the lack of profitability of the
business relationship or a sustained disruption of the relationship of trust
between bank and customer.
However, there are in connection with the fulfillment of the right to information
also case constellations in which the reason for termination, even if this

is stored, not be part of the information according to Art. 15 DS-GVO
may. This is the case, for example, when there are legal regulations
are, which prohibit the responsible persons certain information to the
to be communicated to those affected.
A norm that often comes into play in this case constellation is found
in Section 47 of the Money Laundering Act (GWG), the so-called "tipping-off ban".
§ 47 GWG
(1) An obligated party may the contractual partner, the customer of the transaction and
not inform other third parties of

1. an intended or submitted report pursuant to Section 43 (1),

2. an investigation that is initiated on the basis of a report pursuant to Section 43 (1)

has been directed, and

3. a request for information pursuant to Section 30 (3) sentence 1.

The "tipping-off ban" prohibits an obligated party under Section 2 GWG, among other things, from

the contractual partner (here the terminated, former customer) about it

to inform that according to § 43 Abs. 1 GWG a report about a

Facts to the Central Office for Financial Transaction Investigations (FIU)

has taken place. Such reports are usually

“Suspicious Money Laundering Reports”.

If, by stating the reason for termination, the person concerned

fenen would be disclosed that such a report by the bank to the

FIU has been deposed, the provisions of Section 47 GWG apply accordingly

to note. According to § 47 GWG i. V. m. Art. 23 (1) lit. e GDPR and § 29

Paragraph 1 sentence 2 BDSG would be the disclosure of the stored date

"Reason for termination" in this case is therefore expressly prohibited.

In order to make such national regulations possible, the legislator has

an opening clause was created with Art. 23 GDPR. Article 23 paragraph 1

DS-GVO allows the member states, under certain conditions

etc. to limit the right to information according to Art. 15 DS-GVO.

Art. 23 GDPR

(1) By legal provisions of the Union or the Member States to which the responsible

che or the processor is subject to, the obligations and rights under the

Articles 12 to 22 and Article 34 and Article 5, insofar as the provisions of

comply with the rights and obligations provided for in Articles 12 to 22, by way of

Legislative measures are limited, provided that such a limitation

respects the essence of fundamental rights and freedoms and in a democratic

society constitutes a necessary and proportionate measure that:

ensures:

a) national security;

b) national defence;

c) public security;

d) the prevention, investigation, detection or prosecution of criminal offenses or criminal

enforcement, including protection against and defense against threats to the

public safety;

e) the protection of other important objectives of general public interest

of the Union or a Member State, in particular a major economic

civil or financial interest of the Union or a Member State, e.g

in the currency, budget and tax area as well as in the public sector

health and social security;

the protection of the independence of the judiciary and the protection of judicial processes;

f)

g) the prevention, detection, investigation and prosecution of violations of the

professional rules of regulated professions;

h) Control, monitoring and regulatory functions that are permanently or temporarily associated with the

Exercise of public authority for those mentioned under letters a to e and g

purposes are connected;

the protection of the data subject or the rights and freedoms of others;

the enforcement of civil claims.

i)

j)

According to Recital 73 DS-GVO, a restriction can then occur, for example

follow if this is necessary for the detection and prosecution of criminal offenses

and is proportionate. According to § 261 StGB it is money laundering

for such a crime.

Recital 73 GDPR

1Union or Member State law may restrict certain

Principles and regarding the right to information, access to and rectification

or deletion of personal data, the right to data portability and

consent, decisions based on profiling, and communications

of a personal data breach to a data subject

and certain related obligations of those responsible

as far as this is necessary and proportionate in a democratic society

is to maintain public safety, including the protection of

Human lives, especially in natural or man-made disasters

disasters, the prevention, detection and prosecution of criminal offenses or the criminal

Enforcement – which includes protection against and averting of threats to the public

Security includes - or the prevention, detection and prosecution of violations

against professional rules for regulated professions, the keeping of public registers

for reasons of general public interest and the further processing of

archived personal data to provide specific information in the

related to political behavior under former totalitarian regimes,

and to protect other important objectives of general public interest of the Union

or a Member State, such as important economic or financial interests, or the

data subject and the rights and freedoms of others, including in the

areas of social security, public health and humanitarian aid.

2These limitations should be consistent with the Charter and with the European Convention on

protection of human rights and fundamental freedoms.

The legislature has therefore made use of the opening clause and

in § 29 para. 1 sentence 2 BDSG a corresponding restrictive regulation

regarding the right to information according to Art. 15 DS-GVO.

§ 29 BDSG

(1) 2The data subject's right to information pursuant to Article 15 of the Regulation (EU)

2016/679 does not exist insofar as the information would disclose information that is

of a legal provision or its essence, in particular because of the overriding

legitimate interests of a third party must be kept secret.

The obligation to provide information according to Art. 15 DS-GVO does not exist,

if the information in question is based on a legal regulation

must be kept secret. Consequently, they find the right to information

restrictive regulations of § 47 GWG i. In conjunction with Art. 23 (1) lit. e GDPR

GVO and § 29 para. 1 sentence 2 BDSG apply to the reason for termination,

provided that the Bank hereby submits a suspicious activity report

the FIU would be revealed.

In such cases, the bank is consequently obliged to provide the information

appropriately restricted, even if the suspected money laundering

display represents the reason for termination and this in the systems of

Bank is stored personally. The information is then nevertheless as

to be considered in full, even if the reason for termination is not stated

becomes. Exists in addition to the issued suspected money laundering report, however

there is another reason for termination, this must be included in the information.

14.3

Misdelivery of customer letters

Missing customer letters is one of the most common

data protection violations reported to the supervisory authority.

The incorrect dispatch does not always trigger the obligation to report according to Art. 33 DS-GVO.

166

Economy, banks, self-employed

In order to be able to decide on the reporting obligation according to Art. 33 DS-GVO,

However, an appropriate risk assessment must be carried out in each individual case.

If there are any uncertainties, it is advisable to contact the supervisory authority

in Hesse, the HBDI, to ask.

An incorrect dispatch of customer letters can be caused by the incorrect address

ment of a letter. In this case, the further

Content of the letter the actually intended addressee and this

assignable facts arise. But a wrong shipment can also happen

resulting in adding pages to a properly addressed letter

were not intended for the customer to whom the letter was sent

was addressed. Again, depending on the content of the incorrectly assigned

Pages may contain information about an individual, not the recipient

of writing concern. Even if it is the wrong shipment

a serial letter can be derived from the naming of another

Person give an indication of an existing customer relationship. Also

this is personal data. The wrong shipment of

Customer correspondence therefore basically constitutes a data protection violation

However, not every wrong delivery is reportable within the meaning of Art. 33

GDPR. An exception exists if the data breach

not expected to pose a risk to the rights and freedoms of the

affected person.

Art. 33 GDPR

(1) 1In the event of a breach of the protection of personal data, the

respond promptly and where possible within 72 hours after reporting the breach

became known to the competent supervisory authority pursuant to Article 55, unless

that the personal data breach is not likely to result in a

risk to the rights and freedoms of individuals. 2If the notification is sent to the

If the supervisory authority does not respond within 72 hours, it shall be given a reason for the delay

to add.

Decisive for the question of whether a notification according to Art. 33 DS-GVO is made

must, therefore, is the assessment of the risk arising from the data breach

can be expected to arise. This means that a responsible person

appropriate risk assessment must be carried out in each individual case.

If documents are sent incorrectly, this risk assessment

In particular, the following parameters must be taken into account:

– content of the letter,

– recipient of the letter,

- affected person.

When evaluating the content of the letter is primarily based on it

to turn off data to be extracted. This is how a risk assessment at a

incorrectly sent appointment confirmation, from the z. B. only the name of the

data subject and the existing or prospective business

relationship to the responsible body is disclosed, turn out differently than

if this letter also includes data such as IBAN, date and place of birth and

Address data or even lists of assets or health data

contained. These circumstances would certainly lead to an obligation to report.

Just like the content of the letter is the person of the recipient

of great importance when assessing the risk. logs example-

the recipient himself at the responsible office and hands over the

wrongly received documents and ideally also confirms

not having made any copies may result in the waiver of a notification

Art. 33 DS-GVO are well represented. But the recipient is not

to determine or not respond to inquiries and may therefore be a risk

cannot be excluded for the person concerned, has a message

to the supervisory authority according to Art. 33 DS-GVO.

In addition to the content and the recipient, there is also the person concerned

to be taken into account when assessing the risk. If for example

a person is in the public eye and wrongly transmitted

If data becomes known, this may have negative effects, such as e.g. B.

on the public perception of the person, should this

also included in the risk assessment.

168

credit bureaus, collection agencies

15. Credit bureaus, collection agencies

credit bureaus, collection agencies

15.1

Disclosure of address data by credit agencies and

collection agency

Conducting an address search on the part of a creditor and

a mandated collection agency (IKU) as part of a debt

recovery and the information provided in this context by

updated address data of the debtor

a credit agency to these are fundamental from a data protection perspective.

additionally permitted. However, in individual cases, a separate

Verification before providing information may be required.

In the present case was a debtor during the debt collection process

moved and had the creditor or the collection agency (IKU)

not given their current address. In addition, the debtor had

the responsible registration authorities of your former and new place of residence

an information block according to § 51 Federal Registration Act (BMG) in the registration register

register. In order to inform the debtor as part of receivables management

ments by post, the mandated IKU conducted a

Address research at SCHUFA Holding AG (SCHUFA). Thereupon

SCHUFA sent this the new address data of the debtor

no. However, the SCHUFA had no knowledge of the existence of one

Blocking of information according to § 51 BMG; she did not have the debtor about this

informed. The debtor did not dispute the existence of the

Financial support. However, she took the view that the available data

lungs (request from IKU and information from SCHUFA)

were inadmissible due to the information block entered.

Concrete explanations of the reasons for the registered blocking of information

the debtor did not do to me.

However, the present data processing is in cases in which the believer

bigerin or the IKU no longer has the current address of the debtor

is known (e.g. due to

ser, already outdated address data or due to a move of the

Debtor during the ongoing debt collection process), on the basis of

Article 6 (1) subparagraph 1 lit. b GDPR to enforce the debtor's

Fulfillment of the contract with the creditor and on the basis of Art. 6

Paragraph 1 subparagraph 1 lit. f GDPR to safeguard the legitimate interests of the IKU

generally permissible.

169

Article 6 paragraph 1 subparagraph 1 DS-GVO reads with regard to the two permissions

inventory as follows:

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following

conditions are met:

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;

(...)

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.

With regard to the details regarding the basic admissibility of the

Data processing by IKU I refer first to my explanations

as part of my 49th activity report (section 12.3).

A credit agency may therefore, if there is a necessary

legitimate interest of their contractual partner (here: creditor or IKU)

Information about the address data of the debtor within the framework

of claims management. The realization of the owed

In principle, claims against the debtor are made

a legitimate interest. Any conflicting overriding

Interests of the debtor in an omission of this

Provision of information is generally not initially apparent.

Are there facts that justify the assumption that the affected

or another person through information from the population register

for life, health, personal freedom or similar things worthy of protection

Interests can arise, the registration authority has at their request or

ex officio according to § 51 BMG an information block in the population register

to enter.

§ 51 BMG reads as follows:

170

credit bureaus, collection agencies

§ 51 BMG

(1) If there are facts that justify the assumption that the person concerned or a

a danger to life, health,

personal freedom or similar interests worthy of protection can arise, the

the authority on request or ex officio free of charge a blocking of information in the registration

to register. A similar interest worthy of protection is in particular the protection of

concerned or another person from threats, insults and unauthorized persons

reenactments. When determining whether there are facts within the meaning of sentence 1

also to consider whether the person concerned or another person belongs to a group of people

belongs to, who because of his professional or honorary activity

generally sees hostilities or other attacks to a greater extent.

(2) If, after hearing the data subject, a risk pursuant to subsection 1 is not

can be closed, information from the population register is not permitted. Is the affected

person cannot be reached in cases where an information block is initiated

an official authority named in Section 34 subsection 4 sentence 1 numbers 1 to 4, 6 to 9 and 11

was registered because of hearing the initiating body. Unless information

is granted, the requesting person or body receives a communication that does not allow any inferences

allow to determine whether there is no data available for the person concerned or whether there is one

Blocking of information exists.

(3) If an information block has been entered, the data subject and, if the

Entry at the instigation of an in § 34 paragraph 4 sentence 1 numbers 1 to 4, 6 to 9 and

11 named authority was carried out ex officio, in addition to the initiating body

to inform immediately of any request for information from the population register.

(4) The blocking of information is limited to two years. It can be done on request or ex officio

due to be extended. The data subject must be informed before the block is lifted

ten, as far as it is reachable. Was the blocking of a number in § 34 paragraph 4 sentence 1

1 to 4, 6 to 9 and 11, this authority must be informed if the

data subject cannot be reached.

(5) Information from the population register is also not permitted

1.

as far as the inspection of a civil status register according to § 63 of the civil status

set must not be permitted and

in the cases of § 1758 of the Civil Code.

2.

However, this blocking of information according to § 51 BMG extends exclusively

based on information from the registration authority. The registration authority informs the

Credit bureaus in Germany also do not preventively about the entry of

Blocking of information in the population register for the persons concerned. a sol

che data transmission would already be inadmissible because there is no

legal basis exists.

Consequently, a credit agency has no knowledge of this at first - unless

the credit agency was informed by the debtor

informed of this matter.

If the credit agency is not aware of the establishment of an

has a freeze on the future of the debtor is a

Provision of information on the current address data for this person to a

Creditor not objectionable.

Even in the event that the person concerned has informed the credit agency about the

worn information block according to § 51 BMG informed, would be in the case of

Request from the creditor or an IKU, which obviously exclusively

the realization of an open claim serves to provide information to you

current address data is generally permissible. Finally serves the

Entry of an information block in the population register not for the purpose that

a debtor thereby submits to the assertion

evade legitimate civil claims.

Nevertheless, the credit agency has in such a case - through implementation
appropriate processes - to ensure that through such
provision of information indicates a hazardous situation for the person concerned
can be closed. Such a process can be individual, for example
Queries to the data subject include whether an information
delivery to the requesting contractual partner is safe for them (e.g. because
the endangering person does not work for them). Alternatively, a
note to be included in the data subject's record
which contractual partner may not be able to be informed, or with
a similar note. In principle, SCHUFA can assume that
that their contractual partners are reputable and of them through the knowledge
me the current address of the person concerned no danger for this
runs out Only with this assumption contradicting indications
should a credit agency possibly have a conflicting predominate
the interest of the person concerned in the provision of information regarding
accept their address data and refrain from providing information.

15.2

inadmissibility of poste restante delivery of a data copy

Art. 15 GDPR

The provision of information according to Art. 15 DS-GVO with the address "post-
in stock" to a branch of Deutsche Post AG is due to data protection law
fundamentally inadmissible. The correct and complete information
With a corresponding application for a self-disclosure for the
Credit agency be so difficult that the omission of a disclosure of information
is nothing to complain about.

credit bureaus, collection agencies

In the present case, the complainant criticized SCHUFA Holding

AG refuses to provide information in accordance with Art. 15 GDPR.

To this end, he stated that he would be planning some trips and sailing trips in the near future

to do business or to stay abroad in general. Therefore he desires

the provision of information poste restante to a person specifically named by him

Branch of Deutsche Post AG in Germany. A current address in

abroad or a possible previous address in Germany informed the complainant

defuhrer not with.

In principle, a credit agency according to Art. 15 DS-GVO has the data subject

person to provide information about the data stored there about their person:

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:

(...)

The credit agency, as the responsible body, must ensure that

Information according to Art. 15 DS-GVO exclusively to the person concerned, to whom

the credit agency keeps a credit agency data record. A negligent

Significant transmission of the personal data of the person requesting information

Person to an incorrect third person would be out of data protection law

view not allowed.

In order to comply with this obligation to provide information according to Art. 15 DS-GVO

However, in order to be able to comply with the requirements, the credit agency must

be put in a position, the person requesting information is initially beyond a doubt

to identify and then the corresponding credit agency data record

(if such exists) to be able to correctly assign this person. There-

for further details on the manner of this identification

as part of the process of providing information by credit bureaus

I refer to the explanations on this in the context of my 45th activity

report (Section 4.2.2.1.1). Admittedly, the statements made there refer to

the legal situation applicable at the time (information according to § 34 BDSG old version), however

the principles explained in this regard and the corresponding

Procedure due to the entry into force of the GDPR on May 25, 2018

changed; rather, they continue to exist unchanged.

In principle, a person requesting information is identified

based on the personal details you have provided: first name(s), surname, address

and date of birth.

If the person requesting the information fails to do so, the credit reporting agency will do so

It is the responsibility of the credit agency to provide an address when a request for information is made

already due to this incomplete personal data in actual terms

not possible to identify the person or to

th data record can be assigned without a doubt. In addition, it is the credit reporting agency

also not possible in such a case constellation, corresponding

to make inquiries to the person requesting information in order to

to determine the data in this case. In this respect, if necessary

a query means the omission of information on the part of a

Credit agency already due to the actual impossibility of correct

and complete provision of information from a data protection point of view

to be objectionable.

Even if, as part of the information request from the credit agency, the

last applicable (previous) address of the person concerned in Germany

would have been and thereby an eligible record on the part of

credit agency would have been able to determine, would come a poste restante delivery

the corresponding data copy according to Art. 15 DS-GVO due to the

The risk of misuse associated with the type of delivery is not considered. closing

With this form of delivery, the credit agency cannot rule out

that the information provided does not fall into the hands of an unauthorized third party

arrives, which may be abusive, naming the applicable ones

Personal details of the person concerned, a provision of information to one of them

designated branch of Deutsche Post AG.

The poste restante delivery of a single specific letter (here:

Data copy according to Art. 15 DS-GVO) - according to the Germans

Post AG - in such a way that the sender (here: the credit agency) in the address field

of the letter only the name of the addressee,

the addition "poste restante" and the address of the selected post office.

As an alternative to the name of the recipient, a

between the sender (in this case credit agency) and the recipient or

password agreed upon by the recipient. Therefore

the address field would contain the following data, for example: Max

Mustermann or password: "Fliege32", poste restante, Poststraße 1, 12345

wishhouse. The one sent to this branch of Deutsche Post AG

Documents are kept there for a period of seven days.

Within this period, the recipient or recipients

low the possibility of the document upon presentation of an ID card or

174

credit bureaus, collection agencies

receive notification of the agreed password. As part of

the delivery of this document takes place on the part of the employee or

the employee of Deutsche Post AG only compares the data of the

sender, which the recipient has communicated, as well as

the specified name of the recipient or

alternatively the agreed password. Here it is the handing over

Employees of Deutsche Post AG not possible, a

unequivocal identification of the recipient as the correct data subject

of the corresponding credit agency data record based on the address field

specified data. Besides, this isn't theirs either

Task. Rather, the actual recipient or the actual remains

Recipient when using a password for the employee or

the employee of Deutsche Post AG was ultimately anonymous.

Consequently, even in such a case, the omission of an information

issued by means of poste restante transmission by a credit agency

Not only not objectionable from a data protection point of view, but

more offered.

175

transportation

16. Transportation

transportation

Vehicle owner query to enforce contractual penalties

private parking

The collection of vehicle owner data by means of a simple register

coming from operators of private parking lots or commissioned by them

Company is allowed if a legal claim related to

the operation of the vehicle can be plausibly asserted. It is

however, it is neither my job nor my area of responsibility

to check whether the business model pursued by the car park operator

or the company commissioned by him is legal.

Business owners of customer parking spaces and also

Operators of private parking spaces are increasingly hiring private parking

monitoring companies that ensure the proper use of the parking

control places. In this context, you can reach me regularly

Complaints from citizens requesting payment

received because they apparently parked illegally in a parking lot.

For the complainants, the

Ask where the company got their contact information from and if the

data collection is lawful.

At the one sent by the private parking surveillance companies

It is not a question of requests for payment, as is often assumed

about fines, but rather about contractual penalties. Fines for "false

parker" are used exclusively by authorities (e.g. the local regulatory

offices) raised while the present requests for payment

are only sent by private companies.

By parking the vehicle, the driver enters into a contract with which

he accepts the general terms and conditions of use. This

are usually printed on signs in the parking lot and

also regulate the payment of contractual penalties in the event of corresponding

tion. The question of whether the company's claim is justified can

not clarified by way of a complaint to my authority, but must

be decided in civil courts if necessary. My authority can

only check the legality of the data collection.

In this regard, there is for the owner of the parking space or that of him

commissioned companies the possibility of the vehicle owner data on the

regulatory authorities or the Federal Motor Transport Authority. Because these

are obliged according to § 31 StVG as responsible registration authorities, that

local vehicle register (at the registration authorities) or the head office

Vehicle register (at the Federal Motor Transport Authority).

It should be noted that the vehicle registers pursue the purpose that

vehicles registered on public roads and their owners

to collect and use this data for traffic-related matters

to make available (see § 32 StVG).

According to Article 6 Paragraph 1 Subparagraph 1 lit. c GDPR i. V. m. § 39 Abs. 1 StVG has the

Approval authority or the Federal Motor Transport Authority is therefore a simple one

to transmit register information to the person who, stating the relevant

the registration number or the relevant vehicle identification number

states that he uses the data for assertion, security or enforcement

or for the satisfaction or defense of legal claims in connection

with participation in road traffic or to bring a private lawsuit

required for traffic violations.

It is sufficient if the legal right to information by the interested

senten is presented plausibly (see Bundestag printed paper 10/5343 of April 17, 1986, p. 74).

If the requirements of § 39 paragraph 1 StVG are met, the

Requesters from the authorities a simple register information about the

Owner of the named vehicle and thus also their contact details.

The simple register information according to § 39 Abs. 1 StVG is one of the

most common forms of register information (see BT-Drs. 10/5343 from 17.

April 1986, p. 74).

§ 39 Road Traffic Act

(1) Of the vehicle data and owner data stored in accordance with Section 33 (1).

1. Surname (for legal persons, authorities or associations: name or

Designation),

2nd first names,

3. Order and artist name,

4. address,

5. type, manufacturer and type of vehicle,

6. name and address of the insurer,

7. Number of the insurance policy, or if this is not yet saved, number

mer of the insurance confirmation,

8. if applicable, date of termination of the insurance relationship,

9. possibly exemption from the statutory insurance obligation,

10. Time of allocation or issue of the number plate for the holder as well as

11. Vehicle registration number

178

transportation

to be transmitted by the registration authority or by the Federal Motor Transport Authority if

the recipient, stating the relevant registration number or the relevant vehicle

zeug identification number states that he is asserting the data, backup
or enforcement or for the satisfaction or defense of legal claims in connection
related to participation in road traffic or to bring a private lawsuit
offenses committed in road traffic (simple register information).
If the parking violation was not caused by the owner himself, but
from another driver, is obtaining simple register information
nevertheless permissible under data protection law, since the parking lot operator has the
must have the ability to determine the contractual partner. Parking on a
However, private parking is regularly anonymous, without the operator
via contact with his contractual partner. The current jurisprudence
of the Federal Court of Justice speaks to the vehicle owner therefore a secondary
Burden of proof with regard to driver status (see BGH, judgment of 18
December 2019 – XII ZR 13/19). The Federal Court of Justice ruled that
the operator of private parking spaces also requires an increased parking fee from the vehicle owner
may demand a fee if the latter only claims his driver status as a lump sum
denies without disclosing who is the driver and thus the contractual partner
considered at the time in question.

179

17. Healthcare

healthcare

Also the data protection issues in the areas of healthcare
and health research were strong in the reporting period
shaped by the corona virus. Examples of this are e.g. B. data protection law
che information on the use of the Luca app in Hesse (https://datenschutz.
hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/

data-protection-legal-notes-on-use) on the Hessian vaccination campaign

(https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/ge-

healthcare/frequently-asked-questions-related-to) or

on SARS-CoV-2 quick tests (https://datenschutz.hessen.de/datenschutz/

health-and-social-care/health-care/privacy-at-sars-cov-

2 rapid tests). But there are also many known privacy issues

Especially in these areas there are still many uncertainties, the consultations and

have made interventions by me necessary.

17.1

Transparency of data processing

Unfortunately, in the last reporting period there were again more and more submissions

on the subject of non-granted access to files in accordance with § 630g BGB and

15 DS-GVO by therapists. This

affected both medical practices and hospitals. Unfortunately is

here often an intervention is necessary to treat patients

to help them to obtain the rights to access and information to which they are entitled.

Frequently, there were also requests for advice from doctors,

who support me in fulfilling the right to information in accordance with Art. 15 DS-GVO

have asked for help. The right to information according to Art. 15 DS-GVO is

a claim that is independent of the right to inspect the files in accordance with Section 630g of the German Civil Code

with different content and purpose. The request for data disclosure must

cannot be justified, nor is it bound to a specific form. At

Manifestly unfounded or excessive requests can the doctor's office

either demand a reasonable fee or refuse to provide information.

The patient must be given the information immediately, in every

However, the case is available within one month of receipt of the application

be asked. This period can be extended by a further two months

den if this is taking into account the complexity and number of

applications is required. About this is the person concerned within a

to be informed monthly.

The provision of information can in principle depend on the wishes of the persons concerned

person in writing, electronically or verbally. The increased Si

security requirements when transmitting the specially protected

However, health data must be fulfilled (see Section 17.2). The affected

Person can also receive a copy of the stored data concerning them

demand. The information is to be provided free of charge. Just for more about that

Copies that go beyond the initial information may be provided by the doctor's office

demand payment.

If there are doubts about the identity of the person making the request (e.g

Change of residence), the doctor’s office must protect those who are worthy of protection

health data request further information for legitimacy, e.g. B.

the sending of a copy of the identity card. The ones not required

personal information on the copy of the ID (such as eye color, height,

ID card number) may be blacked out by the patient.

According to § 29 paragraph 1 sentence 2 BDSG, the information is based on the data of the requesting party

limit person. Data of third parties, in particular of family members,

may in principle only with their consent and release from the duty of confidentiality

be notified.

To support medical practices, I have a corresponding template for

Information according to Art. 15 DS-GVO made available on my homepage:

https://datenschutz.hessen.de/datenschutz/ gesundheits-und-sozialwesen/

healthcare/information-according to-art-15-ds-gvo-for-doctors-practices.

17.2

Invoices from the pharmacy by mail?

When sending pharmacy bills by email, it is for protection

of the health data concerned here a content encryption (“end

end-to-end encryption”) required. As privacy-compliant solutions

come encryption standards S/MIME or OpenPGP, portal solutions

or possibly password-protected ZIP files.

The Hessen State Chamber of Pharmacists asked me for an assessment of how

principle when sending invoices by e-mail

may be. This was preceded by an entry regarding the unencrypted

Emailing pharmacy bills to a nursing home. here had

I managed to get the pharmacy to stop this practice.

According to Art. 5 Para. 1 lit. f GDPR, personal data must be in

processed in a way that ensures adequate security of the

personal data guaranteed. With appropriate technical and

organizational measures is protection against unauthorized or unlawful

moderate processing and against accidental loss, unintentional

destruction or accidental damage ("Integrity

and confidentiality").

According to Art. 32 DS-GVO, the person responsible, taking into account the

state of the art, the implementation costs and the type, scope,

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

Likelihood of occurrence and severity of risk to rights and

Freedoms of natural persons appropriate technical and organizational

to take measures to ensure a level of protection appropriate to the risk

to ensure.

The more sensitive the personal data is, the bigger it is

Protection requirement, which is the basis for the selection of the measures to be taken

is to be laid.

Pharmacy bills regularly contain information that

Conclusions about the state of health of the customers

to permit. Especially with prescription drugs

the expected intake of a drug also a specific one

be assigned to a person. They are therefore those according to Art. 9 Para. 1 DS-GVO

specially protected health data.

When sending e-mails with health data, a transport

Encryption is generally not sufficient. Rather, here is to

Protection of health data taking into account the state of the art

content encryption in addition to transport encryption

("End-to-end encryption") required.

By using the common encryption standards S/MIME or

OpenPGP can e.g. B. content encryption of e-mails can be achieved.

However, the recipients of the invoices would have to

have the appropriate knowledge and technical capabilities.

Another data protection-compliant variant can be found in the provision of the

Invoices exist via an external IT provider (portal solution). here

the customers will be informed by e-mail that

their invoice via a personalized and password-protected login

can download from a server of the IT provider. With this variant

it must be ensured that the IT provider meets the increased requirements

to IT security when handling health data. The data

must also be stored in encrypted form on the provider's server

so that he does not have access to the data.

Alternatively, pharmacy invoices may be submitted under the following conditions:

also as a password-protected ZIP or PDF file as an attachment

E-mail to be sent:

– The e-mail itself may be in the subject, in the text and in the name of the attachment

no health data included.

– The password must be sufficiently complex and must not vary

can be derived from the communication relationship (e.g. date of birth or

customer number).

– When encrypting, appropriate settings must be made under

adequate level of protection considering the state of the art

be achieved (Article 25 GDPR). This includes, for example, that the

software used supports secure encryption algorithms

(e.g. AES-256) and no access options (so-called "backdoors") for

the provider of the software.

– The password must be transmitted via an alternative communication path

communicated (e.g. in person, by telephone, SMS) and should not be exceeded

be used for a longer period of time.

A prerequisite for these data protection-compliant solutions for electronic
Transmission of the bills is that the recipient is actually in the
Are able to open the encrypted messages. Therefore is regular
in advance of the transmission, a vote on suitable solutions and
formats required.
The routine unencrypted sending of invoices by e-mail
on the basis of the consent of the customer is not permitted.
The legal requirements of Art. 5 Para. 1 lit. f and 32 GDPR apply
against this and oblige the pharmacies, regardless of their will
appropriate precautions for customer notifications
to protect personal data.
The Conference of Independent Data Protection Authorities of the
The federal and state governments (DSK) decided on November 24, 2021
clarified that a waiver of the data to be held by the person responsible
technical and organizational measures or the reduction of the
legally required standards on the basis of consent
is generally not permitted (see Annex 1, Item 2.4).
As a result, I informed the Hessian Chamber of Pharmacists that
that the above requirements for sending invoices
apply by email.
186
healthcare
The Hessen Chamber of Pharmacists can now legally
safely advised and these the mentioned, data protection compliant solution
show approaches.
17.3

Discretion restored in doctor's office

Medical practices must ensure that the necessary discretion is maintained in the

realities of practice are preserved. Confidential conversations at reception

must not be audible in the waiting room. possibly has

the medical practice protective measures of a technical or organizational nature,

e.g. B. structural measures to ensure discretion in the practice rooms

to ensure.

Through an anonymous submission, I was made aware that

the necessary confidentiality and discretion in a Hessian medical practice

given. The photos of the practice provided by the doctor's office showed

the following situation on site:

The doctor's office was structurally open. There was a partition between

Waiting room and reception area with an open passageway without one

lockable door. The premises were not upstairs either

ceiling, but they were open to the very high ceiling of the building

leave. Confidential conversations at reception could therefore by patients

be heard in the waiting room.

In conversations at reception, patients place special emphasis

sensitive health information. These are regularly

sonal in the patient file as a file system according to Art. 2 Para. 1 Alt. 2 DS-GVO

stored so that the scope of application of the GDPR is opened up.

According to Art. 5 Para. 1 lit. f GDPR, the medical practice is legally obliged to

to process personal data in a manner that ensures a reasonable

ensures the security of this data, including protection against

unauthorized or unlawful processing (“Integrity and Confidentiality”).

Therefore, the practice must ensure that the acknowledgment and

authorized third parties is prevented as far as possible. Also the medical one
Confidentiality according to § 203 Section 1 No. 1 StGB requires a special one
Discretion in the premises of the practice.
I pointed out the lack of discretion to the doctor's office and
suffices that they take appropriate technical and organizational measures,
such as, in particular, structural changes and additional soundproofing
measures, meets.
187
The Hessian Commissioner for Data Protection and Freedom of Information
50th activity report on data protection
Various measures have been tested in practice. So became the paste
an additional noise protection wall and hanging down the ceiling
richly planned with sound-absorbing sails. In the end decided
the practice for a spatial separation of waiting room and reception
rich. Structurally, the reception area became a closed room
redesigned so that the discussions there between employees of
Practice and patients no longer overheard in the waiting area
can become.
17.4
Duration of retention of patient records in dental practice
A retention of a dental practice's patient records after expiration
the statutory ten-year retention period (§ 630f Para. 3 BGB).
generally not permitted. The civil law statute of limitations
of claims for damages do not justify any longer ones
Storage of the data by the dental practice.
Rather, longer storage is only permitted in individual cases, insofar as

there are special medical reasons for this or concrete indications

available for a legal dispute. In these cases, the

Dental practice to document the reason for the longer storage.

On the occasion of a submission I have the procedure directory of a dental

medical practice checked. The directory of procedures provided that the

Patient data even after the ten-year retention period has expired

be archived.

The dental practice informed me that the patient data was up to 30 years

would be kept after the end of the treatment relationship. This

long storage is more appropriate due to the late limitation period

claims for damages required. According to § 199 paragraph 2 BGB

the maximum period of limitation for claims for damages due to

Injury to life, body or health 30 years.

In principle, personal data is based on the principles of

data minimization (Art. 5 Para. 1 lit. c DS-GVO) and storage limitation (Art. 5

Paragraph 1 lit. e GDPR) to be deleted if the purposes of data processing

have been reached (Art. 17 Para. 1 lit. a DS-GVO) and no legal storage

storage obligations pursuant to Article 17 (3) (b) GDPR

demand. As a rule, therefore, the patient data are with the end of the

to be deleted after ten years for the following retention periods.

188

healthcare

According to 630f paragraph 3 BGB and § 12 paragraph 1 of the professional code for Hessian

Dentists are the patient files for a period of ten

years after completion of treatment, unless later

other regulations, other retention periods exist.

The start of the retention period sets the completion of the treatment

in advance. It must be differentiated whether it is a single

closed treatment process because of a specific ailment

or a long-term treatment z. B. because of a chronic illness.

In the case of individual illnesses, the retention period begins at the end of the

specific treatment process.

In the case of a permanent or extended treatment, it comes down to the

Day on which the patient was last treated for this disease process

(Rehborn/Kern in: Laufs/Kern/Rehborn Handbuch des Ärzterechts,

5th edition 2019, § 61, para. 31). This is the first day of the 10 year period.

The last patient contact that occurs for any other reason is

not relevant to (Spickhoff in: Spickhoff, Medizinrecht, 3rd ed.

2018, BGB § 630f para. 7).

According to § 85 para. 2 sentence 1 no. 2 Radiation Protection Act (StrlSchG)

drawings as well as X-ray images, digital image data and other investigations

data for a person of legal age for a period of ten years

(a) and in the case of a minor, up to the age of 28.

Age (b) to keep. A 30-year retention period applies to

these documents only in the case of treatments with ionizing radiation

or radioactive substances (§ 85 Para. 2 Sentence 1 No. 1 StrlSchG).

In individual cases, further special statutory regulations may apply to dental practices

data protection obligations apply, which must then be taken into account for the data in question

are sighted.

Should be necessary to achieve the purpose for which the patient data was collected

were still necessary to be retained, they do not have to be deleted

(cf. Art. 17 Para. 1 lit. a GDPR). In particular, this can

be the case if the health data contain important information,

with regard to which it can be assumed that even after expiration

statutory retention periods the interest of the patient in the

storage outweighs the interest in erasure (e.g. if it is

in the course of treatment it becomes apparent that the longer storage of the

Patient records for future treatment of a patient in particular

important is).

However, this is not the norm, but can only be used in the case of special medical

financial reasons apply in individual cases. In a deletion concept are over

deletion periods that go beyond the retention periods

justify and document.

A flat-rate storage of the personal patient data via

the period of § 630f paragraph 3 BGB due to the 30-year statute of limitations

199 Para. 2 BGB is not permitted.

According to Article 17 Paragraph 3 lit. e GDPR, the obligation to delete according to Article 17 Paragraph 1 applies

DS-GVO not if the processing of the data for the assertion,

exercise or defense of legal claims is required. This sets

provided that a dispute already exists or is specifically foreseeable.

A general precautionary application in the event that theoretically still

a claim could be asserted against the treating person,

is not permitted.

Storage of patient data after the ten-year storage

A period of grace may therefore be permissible in individual cases if the dental practice

After weighing the conflicting interests (probability

the assertion of legal claims against the continuing

encroachment on fundamental rights through storage) to the corresponding result

comes.

The reversal of the burden of proof according to § 630h paragraph 3 BGB does not lead to any other

Evaluation. This reversal of the burden of proof in the case of missing treatment

mentation no longer applies if the ten-year retention obligation of the

§ 630f Para. 3 BGB has expired (cf. explanatory memorandum “Draft of a

Law to Improve the Rights of Patients” dated

August 15, 2012, Bundestag printed paper 17/10488, p. 30).

In this respect, the treating person meets after the expiry of the ten-year period of § 630f

Para. 3 BGB from the non-existence of the documentation is not a disadvantage.

He deletes or destroys the documentation of the treatment after the expiration

of the deadline, the burden of proof regulation of § 630h Para. 3 BGB no longer applies.

Due to regular inquiries on this subject, I have the

Federal Chamber of Dentists and the State Chamber of Dentists of Hesse to

lung requested. Both chambers also see no dentists

Requirement for retention beyond ten years. The

The Hessen Chamber of Dentists has made it clear that in individual cases,

in the case of corresponding treatment relevance, a longer storage period

medical reasons as admissible.

I have informed the dental practice about the legal situation and to adjust

solution of the deletion processes. Then I got the dental practice

informed that they will comply with their deletion deadlines with regard to patient data

appropriately.

healthcare

17.5

TeleCOVID Hesse

Using the TeleCOVID Hessen app, hospitals with smaller

Intensive capacity for a COVID treatment a second opinion of a

Intensive care physician or an intensive care physician of larger hospitals

catch up. The hospitals can network via video telephony and

Transmit findings and treatment data in encrypted form. so can

important information before transferring to another hospital

be replaced.

The use of the app can affect the previous exchange of information between

the intensive care units via telephone, fax and e-mail simplify and technically

improve. Around 80 hospitals in Hesse are already connected

and can use the app.

During the development and introduction of the TeleCOVID Hessen app

I involved from the beginning. In regular conversations, everyone

stakeholders worked together constructively. My hints and comments

ments to design the system were implemented and those involved

Hospitals were included in this discussion. through the early

Numerous concepts relevant to data protection could be included at an early stage

and documents are coordinated in advance.

Here it was shown again that my involvement before the start of the project

the right course can be set regularly and in good time

project-delayed improvements to establish the data protection

formality will not be required.

17.6

Data protection issues in theses and doctorates

Personal data is collected as part of research projects

processed, there must always be a legal basis for this processing. The

As a rule, data processing will be based on consent.

According to Section 24 (1) sentence 1 HDSIG, processing is also permitted without consent

special categories of personal data, these are in particular

Health data, within the meaning of Art. 9 Para. 1 DS-GVO for scientific

Research purposes permitted when processing for these purposes

is necessary and the interests of the person responsible for the processing

the interests of the data subject in the exclusion of processing

predominate.

191

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

§ 24 para. 1 sentence 1 HDSIG is only for public bodies in Hesse, i.e. in

special universities, applicable and therefore only applies to research projects

be under the responsibility of a university of the state of Hesse. For

private universities, not the HDSIG, but § 27 BDSG is applicable.

The concept of scientific research purposes is

reason 159 sentence 2 of the DS-GVO to be interpreted broadly. Also research projects

in the context of academic theses (e.g. bachelor or

Master's thesis) or doctoral projects are regularly included.

Is the data processing based on the legal basis of Section 24 Paragraph 1

Clause 1 HDSIG is before the start of the research project according to § 24

Para. 1 sentence 3 HDSIG to create a data protection concept that

must be presented to the competent supervisory authority upon request.

If only anonymous data is used, there are no personal

related data, the DS-GVO is according to Art. 2 Para. 1 DS-GVO then

not applicable. However, a data protection concept is also recommended here

to create, in which primarily the anonymity of the data and the protection of their

anonymity is shown. However, it is only anonymous

Data, if the data - even with additional knowledge that can be reached - is not

assigned to identified or identifiable natural persons

can.

I have a template for such a data protection concept on my website

provided that is particularly related to research projects

with academic theses (e.g. bachelor's or master's theses)

ten) or doctoral projects in Hesse (https://

datenschutz.hessen.de/datenschutz/statistics-and-science/science/

data protection concepts-for%C3%BCr-academic).

Especially in the "smaller" research projects mentioned above

the danger that the creation of a complete data protection concept

the project came to a standstill due to a lack of personnel and technical resources

brings. With this pattern I would like students and PhD students

assistance in fulfilling data protection obligations

ben, so that these research projects do not interfere with data protection law

Expenses for testing and documentation fail.

18. Technology and organization

technology and organization

Important topics in which the technical and organizational

planning competence was required in the supervisory authority, e.g. B.

Video conferencing systems (item 4), management systems (item 8) and large

IT applications in schools (item 10). But also the increase in

Cybercrime and failures and upgrades in network components

required a lot of attention. A high base load caused the additional

Increasing reports of data breaches to review and grow

were manageable. Another important task is the technological one

observing developments and recognizing where new risks arise,

but also where old protection mechanisms no longer offer data protection. A

vivid example of this is the need to replace the fax with digital

to replace alternatives that comply with data protection law.

18.1

Data Breach Notifications

The number of reports of data breaches reached in the year under review

a new record. Responsible bodies continue to have advice

need for information on fundamental questions in the context of data protection incidents

as well as the requirements for reporting.

Overview and Developments

In the reporting period, my authority received a total of 2,016 reports

of data protection violations according to Art. 33 DS-GVO, § 65 BDSG i. V. m.

§ 500 StPO and § 60 HDSIG from the public and non-public

area one. Compared to the previous year, the number of data

protection incidents by 571 reports and thus increased by more than 40%.

The figure below represents an overall development of the reported

Data breach at HBDI since GDPR came into effect

on May 25, 2018.

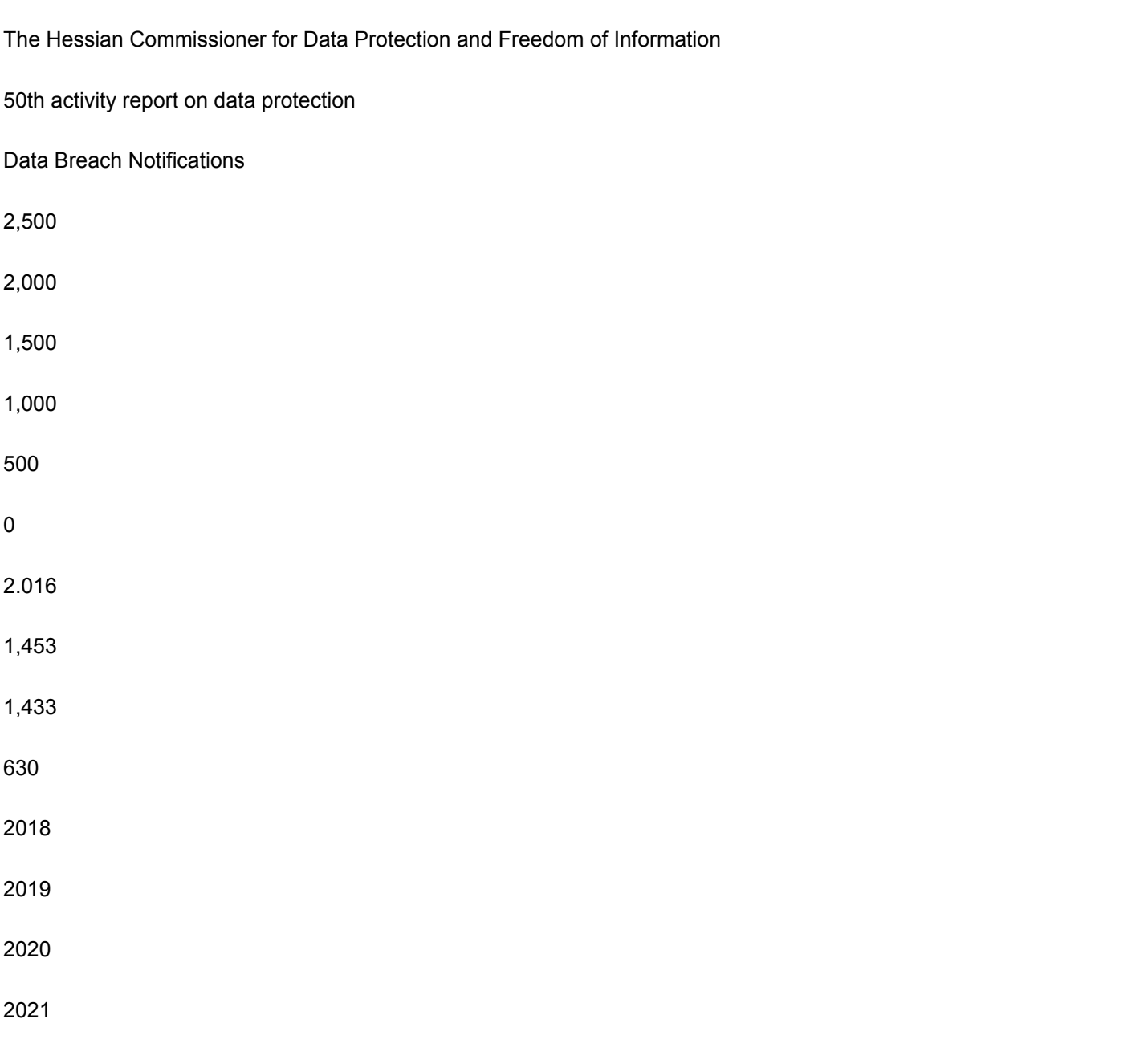

Fig. 1 Development of the number of data breach notifications

HBDI since the GDPR came into effect

The obligation of the responsible bodies, breaches of protection

to report personal data to the data protection supervisory authority,

arises from Art. 33 GDPR.

Art. 33 GDPR

1In the event of a breach of the protection of personal data, the responsible

immediately and if possible within 72 hours after becoming aware of the violation

was, this to the competent supervisory authority pursuant to Article 55, unless the

Personal data breach is unlikely to pose a risk

for the rights and freedoms of natural persons. 2If the message is sent to the

supervisory authority within 72 hours, it shall be given a reason for the delay

to add.

If the processor has a personal data breach

becomes known, he reports this to the person responsible immediately.

The notification according to paragraph 1 contains at least the following information:

a) a description of the nature of the personal data breach,

as far as possible, specifying the categories and the approximate number of those affected

persons, the affected categories and the approximate number of affected personal

son-related datasets;

b) the name and contact details of the data protection officer or another

contact point for further information;

194

technology and organization

c) a description of the likely consequences of the violation of the protection of personal

personal data;

d) a description of those taken or proposed by the controller

Measures taken to address the personal data breach

and, where appropriate, measures to mitigate their possible adverse effects

effects.

(1) If and to the extent that the information cannot be provided at the same time,

the Controller may receive this information without further undue delay

make available gradually.

(2) 1The person responsible documents violations of the protection of personal data

including all related to personal data breaches

Data standing facts, their effects and the remedial measures taken.

2This documentation must be used by the supervisory authority to verify compliance with the

enable provisions of this article.

The personal data breaches reported to me

are based on a wide variety of circumstances and causes. As already in

In recent years, however, data breaches have also dominated in 2021,

the punishable hacker attacks, incorrect shipment (see also Section 14.3) and loss

(see also Sections 2 and 18.4) or theft of data.

The banking, trade and commerce sectors, the subject area

Employee data protection and the health sector were again on the agenda

most affected.

Rise in cybercrime

It is particularly negative that in 2021 the reports in

connection with criminal cyber attacks have increased significantly. In the

Compared to the previous year, the number of reported attacks tripled

from 184 to 628 incidents. This development, which must be taken very seriously,

from my point of view, among other things, on several in the course of the year

major events that have occurred or become known.

On the one hand, the news about the destruction of the Emotet botnet caused concern

by internationally cooperating law enforcement agencies for numerous

Reports from companies, municipalities and other organizations

to my authority. In this context it was found that

that previously several systems - including some in Hesse

resident responsible person – had been compromised. the respective

Those responsible have been identified by the relevant law enforcement agencies

informed me about this and reported the data that had become known to me

data protection violations.

195

On the other hand, there were critical ones that were heavily discussed in public

Vulnerabilities in Microsoft Exchange servers and how they are exploited

the group called "Hafnium" also numerous Hessian companies

and other institutions affected. Alone on this matter went on

260 reports according to Art. 33 DS-GVO within a very short time at my

authorities, which led to an enormous amount of additional work and

due to a considerable amount of time and human resources

tape. In order to make the processing of these cases as efficient as possible,

existing practices when processing data breach reports

and additional new forms and catalogs of questions were developed. The

The majority of these reports have already been checked and completed

(see Section 18.3).

In addition, I received numerous reports over the course of the year

via so-called ransomware attacks. "Ransomware" is in expert circles

for "ransomware". These are malicious programs

by criminal attackers on the systems of responsible authorities

be played. As a rule, the data is then encrypted

and blackmails the victims of the attack with a demand for money (see Section 18.2). As

In this context, it is particularly critical to observe that

more often smaller companies or e.g. B. Medical practices victims of such

attacks.

Another incident that contributed to the negative statistics occurred-
contacted a Hessian contract processor. This offers for various
Cities and municipalities offer a platform on which citizens can register with a
Register your email address to receive an up-to-date waste calendar
can. When sending the annual waste calendar, cybercriminals
len intercepted a four-digit number of e-mail addresses and partly for
Phishing emails used. A total of 51 were Hessians from the incident
communities affected. The processor responded to a first
Suspected data leakage quickly and informed both those concerned
municipalities as well as the supervisory authority. All concerned citizens
Citizens were also notified immediately. Overall they were
measures initiated by the processor are required and
measure to minimize the damage and the risks of a recurrence
to minimize the occurrence of this situation.

Pandemic notifications

As in the previous year, the ongoing pandemic in the
some data protection violations in the reporting year. During the year
2020 tends to be about disclosures of an existing Covid-19 disease

technology and organization

kung as well as various home office problems (see 49. TB, No. 15.1),
this year I received more and more reports in connection with this
with the corona vaccination, but also with confused test results and
vaccination certificates.

At the end of 2021, individual data breach reports came in
Connection with the implementation of the so-called "3G regulation" on

Add workspace. For example, B. several responsible bodies in the

Lists of employee data as part of the organization of 3G controls

to (internal) wrong addressees. health information such as B. the vaccination status,

were usually not directly affected in these case constellations. Out of

however, relevant indications could be derived from the context.

Surprised by the high number of reported data breaches

not that responsible bodies, but also processors, agree

Extensive need for advice and support in dealing with data

security incidents and regularly bring questions to my authority.

During the reporting period, I received several inquiries regarding the

timing of the report and the calculation of the reporting period.

How exactly is the 72-hour period calculated?

Some essential questions that have often been put to me and for those

practice are of enormous importance relate to calculation

the deadline for reporting personal data breaches

Data. In particular, it was questionable for those responsible whether the deadline

also continues on weekends and public holidays or until the next

working day is suspended.

It should be pointed out again at this point that the reports

of data protection violations the special urgency in the foreground

and this according to Art. 33 Para. 1 Sentence 1 DS-GVO "immediately", possibly

must be done within 72 hours.

In addition, I would like to point out in this context that the

Deadline calculation according to Regulation (EEC, Euratom) 1182/71 of

Council of June 3, 1971 laying down the rules for deadlines, dates and

Dates (FristenVO) take place. The national regulations from §§ 186 ff. BGB

cannot be used as a subordinate right. The relevant ones

Regulations are contained in Art. 3 of the Deadlines Ordinance.

Article 3 Deadlines Ordinance

(1) If a period measured in hours begins, the point in time is decisive in

which an event occurs or an action is undertaken,

Calculation of this period not counting the hour in which the event or action

falls. Is for the beginning of a period measured in days, weeks, months or years

the point in time at which an event occurs or an action is taken is decisive

, the day in which the

event or action falls.

(2) Subject to paragraphs 1 and 4, the following applies:

a) A period measured in hours begins at the beginning of the first hour and ends

at the end of the last hour of the period.

b) A period measured in days begins at the beginning of the first hour of the first

day and ends at the end of the last hour of the last day of the period.

c) A period measured in weeks, months or years begins at the beginning of the

first hour of the first day of the period and ends at the end of the last hour of the

day of the last week, month or year that is the same

designation or the same number as the day on which the period begins. One is missing

period measured in months or years in the last month for their expiration

decisive day, the period ends at the end of the last hour of the last day

this month.

d) If a period includes fractions of a month, the calculation of the fractions of a month

a month of thirty days.

(3) The deadlines include public holidays, Sundays and Saturdays, insofar as these

are not expressly excluded or the deadlines are based on working days.

(4) If the last day of a period not measured in hours falls on a public holiday,

a Sunday or a Saturday, the period ends with the expiry of the last hour

the following working day.

This provision does not apply to time limits that start from a specific date or a

specific event to be calculated retrospectively.

(5) Each period of two or more days includes at least two working days.

According to Art. 3 Para. 1 Sentence 1 of the Deadlines Ordinance, the reporting period begins with the next

full hour after positive knowledge of the data protection violation. This ends

according to Art. 3 Para. 2 lit.

For the question of whether the calculation also includes weekends and holidays

days are taken into account is the interpretation of Art. 3 Para. 5 Deadlines Ordinance

and the question of its applicability to the 72-hour period.

Art. 3 para. 5 Deadlines Ordinance contains a provision regarding all deadlines “from

two or more days". These deadlines include at least two

working days. Because the privacy breach notification period is a

72-hour and not a 3-day period, Art. 3 Para. 5 Deadline Regulation does not apply

reversible. Therefore, a strict deadline calculation is to be assumed here.

Due to an immediate data breach to be assumed

technology and organization

If action is required, an "immediate" report is required. This can't

mean that the deadline is extended by a further two days due to a weekend

can be extended. In summary, it can be stated that the

Deadline for reporting data breaches including weekends and

may expire on public holidays.

Also the notification of data subjects according to Art. 34 DS-GVO

must immediately and thus "without culpable hesitation" i. S.v. § 121 BGB

take place. The legislator did not define a fixed deadline for this.

Art. 34 para. 1 GDPR

(1) If the breach of the protection of personal data is likely to have a high

risk to the personal rights and freedoms of natural persons, so be-

the person responsible shall inform the data subject of the violation without undue delay.

In addition, it is important in this context that a notification

then has discharging effect if they are with the competent supervisory authority

he follows. Otherwise the notification could be time-barred. The supervisory

They work together and forward the reports to the if necessary

competent supervisory authority. However, it is essential that the

responsible bodies get clarity in advance about

which data protection supervisory authority is responsible for them, and not first

when a data protection incident has occurred.

When is step-by-step reporting necessary?

In the case of technically influenced case constellations in particular, the information

The information situation at the time the incident became known is often relative

poor or patchy. For those responsible, the question therefore arises

whether the notification is already made at this point in time or only when further submissions are made

knowledge has to be made.

Decisive for the determination of the beginning of the period is according to Art. 33 Para. 1

Sentence 1 DS-GVO the knowledge of the responsible person of the violation of the

protection of personal data. In the case of a notification after the expiry of

The delay must be 72 hours in accordance with Art. 33 Para. 1 Sentence 2 GDPR
be justified. In addition, Art. 33 Para. 4 DS-GVO enables the
Responsible in certain cases, the supervisory authority gradually
to inform.
However, the application of these two rules is sometimes misunderstood.
stood. Delayed notifications with a reason should be an absolute

remain exception. Art. 33 para. 4 GDPR emphasizes the need for a
immediate notification in all cases requiring notification. fall under
also situations where a qualitative message with all the necessary
contents within the period is not readily possible. The responsible
Therefore, persons must not wait with the report until the facts of the case have been resolved
fully determined and then justify the delay. Rather must
the person responsible must submit a report immediately and upon submission
further knowledge unsolicited and without unreasonable further
Delay more detailed information successively from the supervisory authority
provide.
In this context, I would like to point out once again that
Protective purpose of the obligation to report and notify under Articles 33 and 34
GDPR, which tends to be interpreted broadly. Above all, it is
around to protect the personal data of data subjects, possible
Avert or reduce damage and other disadvantages for those affected
avoid people as much as possible. The supervisory authority is informed
to provide advice and intervene if necessary.

It is therefore important at an early stage of a possible data

breach of protection to involve the supervisory authority. Affected people

are notified to these for the dangers to which they are exposed

could, to raise awareness and to give them the opportunity at an early stage

to take countermeasures.

Conclusion

Overall, there was a significant increase in reports in the year under review

of personal data breaches, in particular

caused by criminal cyber attacks. Cooperation

of the responsible bodies with the supervisory authority is designed in the

constructive in most cases. If the requirements of Art. 34 DS-GVO

are available, those affected are usually informed. In many cases

the responsible bodies inform the data subjects themselves

initiative for the purpose of transparency and better protection, too

if there is no high risk to their rights and freedoms.

Overall, I had to report relatively few violations in 2021

connection with the reporting and notification obligation of the responsible

verbatim according to Art. 33 and 34 DS-GVO. Late and

omitted reports, missing documentation of the violation as well as

Failure to notify those affected remained isolated cases. This

Processes are currently in relation to further data protection law

Checked measures and sanctions on my part.

technology and organization

18.2

Ransomware and ransomware attacks

Cyber attacks using ransomware have increased dramatically in the past few years

increased and are currently among the greatest threats from the

Area of cybercrime for organizations and companies. The

Impact on the security of personal data is significant

and demand increased attention from those responsible.

Ransomware and ransomware attacks

The term "ransomware" means "blackmail software". He sits down

from the English words "ransom" for "ransom" and "ware" as short

form for "software" together. In this context, between the

Ransomware as malware and the ransomware attack as a strategy

distinguish the attacker. While ransomware is a

Malware essentially consists of highly efficient encryption pro-

gramme are added as part of the ransomware attack

other tools used, e.g. B. for infiltrating and scouting

the victim's IT network. These vary in strength

Automated attacks in which the attacker is directly in the IT network of the

operated on the victim. In the course of a successful ransomware attack

the data is encrypted on the affected IT systems of the victim and the

original data deleted. This ensures that the victims do not

have more access to their data. Only after paying a ransom

will be the decryption and thus the restoration of availability

of the data promised. If appropriate precautions have not been taken,

the data cannot, or only with a great deal of time and money

effort to be restored. Increasingly, they exfiltrate

Attackers also collect data from the victim and threaten to publish it

or the auctioning of data. Are personal by the ransomware attack

son-related data is affected, there is at least a violation of the

according to Art. 32 Para. 1 lit. b DS-GVO to be guaranteed by the person responsible

the confidentiality and availability. Depending on the resulting

Risk to the rights and freedoms of the natural persons concerned

can this i.a. a report of violations of personal protection

related data according to Art. 33 DS-GVO at my authority as well as a

Information of the persons concerned according to Art. 34 DS-GVO required

make. In any case, documentation of the incident pursuant to Art. 33

Para. 5 DS-GVO.

201

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

The evolution of ransomware

The origins of ransomware date back to the late 1990s.

The development over time shown in Figure 2 (BSI, ransomware

ware – Threat Situation, Prevention & Response 2021, Chapter 8.1, https://

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/

Ransomware.pdf) names individual ransomware or for

Ransomware attacks additional malware used.

Fig. 2 Development of ransomware over time

By 2017, the ransomware variants were developing

come faster. A change began with WannaCry, in that more efficient

dissemination methods were used. It began an increasing

Professionalization of attackers, leading to a changed tactical

procedure led. With targeted and methodically advanced attacks

focused on companies and organizations. The associated

the greater effort was offset by a higher potential for damage and

significantly higher ransom demands. This effect is as one

of the engines of the menacingly rapidly increasing number of cases.

A survey in Germany from 2019 showed that around 30 percent

of the companies surveyed with a turnover of up to 3 billion euros

have already been affected by a ransomware attack (Statista, War Ihr

Has your organization ever been hit by a ransomware attack? https://

de.statista.com/statistics/data/studie/1038985/survey/ affected-by-

ransomware-by-sales-size-class-of-companies-in-germany/).

The Federal Office for Information Security (BSI) assumes this

anticipate that ransomware attacks will continue to increase. The technical ones

technology and organization

skills of the attackers and the tactical approach of the blackmailers

evolve and new attacker groups will appear.

An additional driver of this development is the increasing sharing of people

Knowledge between the attackers.

How to deal with ransomware attacks

From reports according to Art. 33 GDPR due to ransomware attacks

the following procedure can be derived in abstract form (BSI,

The situation of IT security in Germany 2021, chap. 1.2.2, https://www.

bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichten/

Management Report 2021.pdf).

Fig. 3 Ransomware tactics

In step 1, the victim's IT networks are

hangs, remote access such as VPN connections or maintenance access infiltrated.

Depending on the victim's compromised user accounts, the

Attackers have elevated privileges that make the attack easier. In shape

a lateral spread in the victim's network, the attacker penetrates in the second

Step with the help of extended access rights, corresponding malware

and tools into other IT systems. In the third step,

Victim's son-related data exfiltrated. This step is common though

not a mandatory part of the attack. In the fourth step, data

encrypted by the ransomware and by subsequently deleting the

Raw data made inaccessible to the victim. A contact

with the victim in the form of a ransom note with the ransom

ments and the threat that the data that may have been withdrawn

publishing or auctioning takes place in the fifth step of the attack.

From paying the ransom as shown in the sixth step

the BSI advises against it and recommends that the police be reported immediately

reimburse (BSI, The situation of IT security in Germany 2021, Chapter 1.2.2).

Necessary handling of ransomware attacks

With a view to the security of the processing of personal data

Art. 32 DS-GVO must classify ransomware attacks as a significant threat

be considered. Therefore it applies to those responsible, to them

Endangerment in terms of data protection management to prevent

to take measured technical and organizational measures. As

The result of the risk analysis required for this must be carried out together with

the information security management also about the specific area

identified overarching measures beyond the processing activity,

evaluated and implemented. As part of the process for regular

Verification, assessment and evaluation of the effectiveness of the measures taken

Measures according to Art. 32 (1) lit. d GDPR must change the

Risk situation from ransomware attacks are explicitly taken into account.

If a ransomware attack has occurred, the data protection

legal assessment of the incident does not exclusively refer to the exfiltrated

or encrypted data. Rather, everyone must first

IT systems are viewed as potentially compromised. In particular

it must be taken into account that encrypted data, despite any de-

coding e.g. B. after payment of ransoms as a general rule

must be viewed with promise. The payment of ransoms to the

organized crime in cyberspace is making further ransomware attacks

Feed and guarantees no decryption or non-disclosure.

Should personal data be affected, is risk-dependent to a

timely notification according to Art. 33 DS-GVO and to a notification

of those affected according to Art. 34 DS-GVO (BSI, The situation of the

IT security in Germany 2021, chap. 1.2.2).

204

technology and organization

Ransomware incident with disclosure of personal data

on the dark web

Under certain circumstances, a ransomware attack also publishes

disclosure of the leaked data by the attackers in order to

build up pressure to pay the “ransom”. Is it a

large amount of data, those responsible are faced with the challenge

identify which persons are affected, and these given

if to be notified immediately.

I. Attack on an insurance company

A Hessian insurance association processes personal data

its policyholders as the responsibility

literally according to Art. 4 No. 7 DS-GVO. On the night of July 9th to 10th

In 2021 there was an attack on the IT systems of the person responsible,

which also used ransomware. By this malware

was personal data of policyholders and insurers

secured and thus the access of the person responsible

withdrawn. In addition, there was a drain and a downstream one

Release of parts of the personal data. So they were

Confidentiality and the availability of the personal data concerned

data is no longer guaranteed.

II. Notification in accordance with Art. 33 GDPR

The person responsible informed my authority on July 10, 2021

first notification of this personal data breach

away. He was within 72 hours according to Art. 33 Para. 1 Sentence 1 DS-GVO

committed, as at least from a risk to the rights and freedoms of

affected persons was to be expected. In principle, such a

Report to the competent supervisory authority in accordance with the requirements of the

Art. 33 Para. 3 DS-GVO also information on the type and scope of the affected

personal data, the categories of data subjects

as well as the possible consequences for the persons concerned. Because him

at this point in time, however, the corresponding findings are not yet available

were available, this was the first report by the person responsible

an initial notification that my authority about the incident itself in

informed. In the days and weeks that followed, the person responsible

literal this first message several times for additional information that

became known in the course of his analysis of the incident. The possibility that

necessary information from the competent supervisory authority gradually

to make it available is provided for in Art. 33 Para. 4 GDPR and carries

taking into account the fact that it is precisely in incidents involving complex

IT systems are involved, often only an analysis geared towards clarity

can provide information about which processing activities and in what way

and to what extent are affected (see Section 18.1). In the present case

the person responsible for his obligation to report to my authority

both in terms of deadlines and in terms of content.

The person responsible must identify the data generated during the following analysis

Knowledge gained in connection with the violation of the protection of personal

related data are available and their impact and the taken

Remedial measures concern, in its documentation according to Art. 33 Para. 5

record sentence 1 GDPR. This also applies to cases in which it is

obviously no risk for the rights and freedoms of data subjects

has come. When processing reports in accordance with Art. 33 GDPR

and beyond that, my authority regularly mentions the possibility

33 Para. 5 Sentence 2 DS-GVO Use, this documentation

to request in full, in particular the course of an incident

understand and the adequacy and effectiveness of the

responsible remedial actions planned and taken.

III. Publication of personal data on the “dark web”

On August 6, 2021, I became aware that as part of the

Incidentally leaked personal data in the so-called "Darknet"

had been published. Corresponding messages reached me

on the same day both by the responsible person himself and by

the data protection supervisory authority of another federal state, which is

publication became aware of. Since I own an IT lab

operate in order to process information technology issues with concrete data

to be able to check the protective cover, I was able to convince myself

that among the data published in the "Darknet" actually also

personal data from the area of responsibility of this

insurance association found.

In the event of a possible, threatened or actual publication of personal

related data, all findings must be taken into account and must be

can also be found in the risk assessment of the person responsible. there is

in particular the question of whether an unauthorized publication has taken place or

to what extent this is to be assumed for the assessment of the probability of occurrence

probability of a risk for the rights and freedoms of the persons concerned

relevant. Such an assessment must be checked and

to adjust when new knowledge is available, such as when in the context

technology and organization

of an incident, the publication of personal data from the attacker

fer is threatened or such publication has actually taken place.

The assessment of the severity of the risk, in turn, is decisive

influenced by

- by which group of persons an unauthorized knowledge is presupposed-

is obviously possible

– which categories of persons are affected,

– which categories of personal data are affected, in particular

taking into account special categories of personal data

Data according to Art. 9 DS-GVO,

– what number of people and datasets are affected,

– which technical and organizational measures are taken,

to mitigate the consequences of unauthorized disclosure.

Here, too, the estimate has to be adjusted in the event of new findings

required, e.g. B. in the context of the analysis of any publications per-

son-related data by the attacker.

The large amount of leaked and published data in this incident

required that the person responsible for evaluating the publications

an external company and this one, among others, too

assigned the task, in the published data personal data

and to identify the persons concerned.

IV. Risk Assessment

The following criteria were used for the risk assessment in the present case

really important:

Possibility of knowledge by unauthorized persons

The files drained from the controller's IT systems

were posted by the perpetrators of the incident on their "Darknet" website

published freely accessible. The hurdle for further unauthorized access is

thereby to be rated as low and the group of people who are on

access to this data is almost unlimited. This will make the

Probability of damage occurring and thus the risk of

affected persons increased.

207

Categories of data subjects

In the incident described here, both were policyholders

and policyholders as well as employees and business partners

affected. Different groups of data subjects can each have one

require their own risk assessment, depending on which categories

personal data were affected in their case. Since the group of

affected policyholder was the largest of the three named,

I will focus on presenting the following aspects to this group

focus.

Categories of Personal Data

Personal data of policyholders were predominant

Address and bank details. In particular, the bank details

ten due to the peculiarities of entrepreneurial activity

of the person responsible represents a challenge. Because the person with whom a

The insurance relationship exists, in individual cases, with the person who

makes payments under this contract may deviate, bank

are not always unequivocally tied to a policyholder

or a policyholder with a known contact option

be assigned. The categories of personal data concerned

are of particular importance for assessing the severity of the risk

for the rights and freedoms of the data subjects. The responsible

must consider the possible consequences of misuse

of this data by unauthorized persons for the rights and freedoms of those concerned

evaluate people. In the case of the address data, it is possible first

to think of fraud attempts. Both would be undirected scenarios

(Mass mailing of fraudulent letters or resale

for advertising purposes) as well as a targeted approach. In the present

The case, however, was a personal visit to the persons concerned

unlikely. The same applied to any acute risk situation

for this. A concrete danger is not least due to the large

ßen number of similar data sets less likely. Related to

Bank details are initially payment and bank fraud attempts

to consider. An example of this is direct debit fraud, in whose

Frame unauthorized debits under the pretense of an approved

Direct debit could be made.

Number of records affected

The perpetrators of the incident created around 25,000 files on the "Darknet"

published. Not each of these files also contained personal information

technology and organization

Data. There were quite a few, especially with regard to the bank details

few files that contained a large part of corresponding data sets.

In the further course of the investigation, about a dozen files

searches 180,000 account details alone. So there are possible consequences

could apply to a very large number of people, was that too

to rate the associated risk accordingly high.

Consequences of unauthorized publication

The special thing about the unauthorized publication that happened here

son-related data is that it took place on the "dark web". In contrast to

usual websites that almost everyone accesses on a daily basis

the additional anonymization used for "Darknet" pages

tion infrastructure of the operators of such a site when visiting them

visible, unless he reveals himself. Accordingly

also find common law enforcement actions, which are about

Publications on certain social media channels or others

Websites can prevent, with "Darknet" sites no comparable

starting point. Those responsible must therefore reckon with the fact that one day

in the "Darknet" publication exist for a long time and for

remains accessible to unauthorized persons. In addition, published content

can be accessed, copied and redistributed. Also a successful one

Removal of the publication does not provide effective protection against a

Redistribution or republication. Accordingly works

a publication in any case increases the risk considerably in the long term.

V. Notification of data subjects in accordance with Art. 34 GDPR

In the synopsis of the relevant facts comes the person responsible

with regard to the risk to an overall assessment. Has the violation of

Protection of personal data likely to be a high risk for

the personal rights and freedoms of data subjects result, so

the controller notifies the data subjects in accordance with Art. 34

Para. 1 DS-GVO immediately from the violation.

In the incident described here, the person responsible came to the conclusion

that he must notify the data subjects. Basically

this notification must be made without undue delay, i. H. without culpable hesitation
of the person responsible. Whether a delay caused by a
Fault on the part of the person responsible must be based on the respective
circumstances are assessed. In the present case, the person responsible
the persons actually affected are only known after some time

become known because the evaluation of the large amount of data that has flowed off
took a reasonable amount of time.
In such cases, where a notification of data subjects
is directly connected with a disproportionate effort -
for example also because these persons cannot be determined exactly
-, the notification has instead according to Art. 34 Para. 3 lit. c DS-GVO in
form of a public notice or by any similar measure
to take place. Also the concept of the public of such an announcement
special attention should be paid to A notice on the
company website of the person responsible took place in the present
the case at a very early stage. The person in charge had to
however, assume that its customers usually
do not regularly visit the website of the insurance association. Therefore
he decided at a later date to include the notice in
to have two high-circulation daily newspapers published. After
the persons concerned had become known to him, finally took place
also a personal notification by post.
In certain case scenarios it is conceivable that a notification

by serial letter is not sufficient because individual cases require separate notifications

ment content necessary for the person responsible to fulfill his or her duty

from Art. 34 DS-GVO can fully comply. This is particularly

dere then to think if individual records from the rest thereby

stand out that they are interfering with the rights and freedoms of

particularly suggest to the persons concerned. An example of this

would be, for example, if, in addition to a large number of similar account data

still certain records would exist, based on details of individual

insurance relationships entered into. Affected persons would be

then inform them through appropriately customized notifications.

If necessary, the person responsible can form a group,

to distinguish certain case groups of affected persons and these

to be notified accordingly.

VI. Advice to affected person by my authority

In the aftermath, in particular the postal notifications by the

Those responsible reached my agency about 50 written submissions

of data subjects - some of them as complaints pursuant to Art. 77 Para. 1

DS-GVO - as well as a large number of telephone inquiries. The complaint-

facts were mainly aimed at the question of immediacy

the notification.

210

technology and organization

In addition, affected persons turned to me with the question

how they should behave in order to avoid possible consequences of the publication

to defend against their personal data. Against the background of

I informed the inquirers of the risks presented in such cases

about the possibility of various fraud attempts

should be aware as a result of the disclosure of their address or account data

ten. Looking at the affected account data, many of those affected found

competent help from the banks and savings banks responsible for them. This

advised them, for example, to check their bank statements regularly for

to check authorized debits and to take action in such cases.

VII. Supervision of the responsible body

I was in regular contact with the affected insurance company early on.

easy exchange. Since the focus of my work is on the data

In particular, the person responsible found that there were intellectual property issues

in questions of IT security as well as the criminal law aspects of others

Set up another competent contact point: The central contact point

Cybercrime at the Hessian State Criminal Police Office combines personnel and

professional resources for investigating criminal offenses in the digital space

and puts you in contact with bodies that are involved in improving

be able to advise and support the company's own IT security. In the country

Hessen regularly comes to the Hessen CyberCompetenceCenter

particular importance as this is for public bodies as well as for small ones

and medium-sized companies in the private sector when processing concrete

cybersecurity incidents upon request. If a contact

to my authority before support with a view to IT security

safety of the reporting body is ensured, I recommend those responsible

usually to take advantage of these offers of support.

IT emergency in the company due to a ransomware attack

A ransomware attack does not always have to result in encryption of the

maintain a victim's IT systems. Even if such attacks are discovered and

be prevented before the encryption, the management of the

Attack companies face great challenges, especially when

already through a derivation and publication of data by the

Attackers serious breaches of personal protection

data have revealed. What should a company do when nothing works anymore?

and still need to react quickly?

In the case to be reported here, I initially only saw an attack on the

company network, where data is withdrawn and

called "Darknet" were released. More details about the situation

did not contain the message. A further investigation of the facts revealed that

a known ransomware group linked to the incident

was due to data exfiltrated from the controller's IT network

published on the dark web site of this group.

The course of the attack followed the well-known procedure for ransomware

attacks. Via an initial access (probably via phishing or a

other form of social engineering) to an IT system of the victim

the attackers found their way out laterally in the IT infrastructure of the person responsible

and tried, among other things, to change their access rights to other IT systems

and expand services. Employees of the person responsible provided the

unusual behavior in the IT infrastructure during the course of the attack

and reported this to the IT department. This reacted immediately and could

deny the attackers access to the IT infrastructure before they can

IT systems and data could be encrypted. However, it was about this

At this point, data has already been exfiltrated. The attackers
then tried to ransom money for not publishing the data
blackmail. Ultimately, the threatened publication of the
Data on the ransomware group's dark web site.
Even if the attack did not encrypt the IT systems
had come and thus did not lead to an immediate operational standstill,
coping with the incident presented those responsible with great
challenges. After ensuring that the attackers of the
Access had been denied due to possible lateral
spread of the attackers all IT systems initially as potentially
should be viewed and treated accordingly. To the extent
of the attack and to be able to narrow it down were IT forensic
Investigations necessary for an external IT security service provider
was brought in. Depending on the results of the forensic
The affected IT systems were cleaned up and restored
or had to be set up completely from scratch.
Furthermore, the person responsible and the commissioned IT security
service provider the company data published on the Darknet
systematic analysis. The aim was to determine the extent of the injuries
of the protection of personal data and the persons concerned
determine in order to be able to notify them in accordance with Art. 34 DS-GVO. The
Investigation revealed that in addition to personal data from employees
authorized the person responsible also employee data from other companies

technology and organization
men, such as customers, cooperation partners, suppliers or similar. were affected.

As far as data was processed in the order, the corresponding

those responsible are informed. Due to the extraordinary

Due to the complexity of the data published on the dark web, the analysis was not short-term

possible, but was done in a reasonable time.

It came as a result of notifying the other affected companies

for further reports according to Art. 33 DS-GVO at data protection supervisory

authorities in other federal states and countries of the EEA. These provided

I then occasionally had questions about the incident.

The obligation of the person responsible to report a violation of the protection

to report solar-related data within 72 hours results from

Art. 33 para. 1 DS-GVO, if there is at least a risk to the rights

and freedoms of natural persons must be assumed. In com-

complex incidents, those responsible have the option, in accordance with Art. 33

Paragraph 4 DS-GVO to provide information step by step. This

must be active by the person responsible and without undue further

delay occur.

For the processor, Art. 33 Para. 2 DS-GVO results in the

Obligation, a personal data breach

notify the responsible person immediately after becoming aware

gen. In concrete terms, this means that the contractor is the person responsible

must inform immediately if his investigations have revealed

that personal data falling within the area of responsibility of

those responsible fall, are affected. Due to in this specific

This was only the case for the complex and therefore lengthy analysis of the data

possible after several weeks, because only then could it be determined

which responsible persons were affected.

The company concerned as the person responsible and as the

technical and organizational measures taken by the processor

Responses to the incident were appropriate and adequate to the incident

to terminate and prevent recurrence.

The incident described shows that a ransomware attack usually increases

personal data breaches. In particular

must in the case of an exfiltration of personal data by the attackers

also be checked whether from a high risk for personal rights

and freedoms of the persons concerned must be assumed. This

should often be the case. According to Art. 34 DS-GVO in such cases

Notification of those affected by the injuries required.

If the attackers publish data, increases

basically the risk significant because with the general availability the

likelihood that this data will be used or misused by third parties

will increase accordingly. In the present case, a detailed analysis

Analysis of the published data is required to both controllers and

also to identify affected persons and the specific risk for them

Being able to assess rights and freedoms individually.

A common problem with data exfiltration by attackers is that

it is difficult or impossible for those responsible to determine

ask what specific data the attackers have captured. For this would be

a fine-grained logging of events, accesses, built

Internet connections and transferred data volumes on all IT systems

and services necessary. This would also have to cover the full period of the
cover attack. However, attackers are often involved in these types of attacks
active in the victim's IT network for several days, weeks or even months,
without being discovered. For specific statements remains responsible
often only the possibility of relying at least partially on information
which the attackers reveal. That means they must both be published
Analyze data as well as evidence provided by attackers
in the form of file lists or similar. evaluate. A responsible person can
but do not conclude that further data was not exfiltrated. Also
future use of the data cannot be ruled out either
become like the use of downloaded data by other actors.
There are also tendencies for ransomware groups to store data on the dark web
offer for sale. The specific risk assessment therefore depends on each
individual case, the context and possibly also collected experiences
with certain attacker groups.
The incident also shows that high efforts of precaution against such
attacks must be made. They mostly take place through social
Engineering. Become an employee of a company or an authority
for example, tempted to click on links in e-mails or websites
click, via which the attack software then enters the system of the person responsible
chen is transmitted. Reducing this vulnerability is compared to
the possible damage of a successful attack is always profitable. This
Risk minimization repeatedly calls for targeted educational measures
and awareness raising.

18.3

Dealing with vulnerabilities in Internet services

Security-critical vulnerabilities in software can attackers

make it possible to compromise IT systems. The impact on the

data protection were impressive with the announcements made in March 2021

which vulnerabilities in the widespread software Microsoft Exchange.

vulnerabilities in software

Apparently there is no software without errors. One for the safety of

processing of personal data particularly relevant category

of errors in software are the so-called "weak points". This kind

of security-related errors can lead to IT systems or

-Services become vulnerable to threats and thus a concrete threat

arises. From a privacy perspective, the successful exploitation of

Vulnerabilities by attackers to violations of the in Art. 32 Para. 1 lit. b

DS-GVO required protection goals confidentiality, integrity, availability

and lead to resilience.

In order to be able to reference vulnerabilities uniformly, this is usually done

Common Vulnerabilities and Exposures (CVE) system (The Miter Corpora-

tion, About the CVE Program, https://www.cve.org/About/Overview) and for

the assessment of the criticality of the industry standard “Common Vulnerability

Scoring System” (CVSS) (Forum of Incident Response and Security Teams

(FIRST), Common Vulnerability Scoring System SIG, https://www.first.org/

cvss/) used.

To eliminate vulnerabilities, it is necessary for the manufacturers of the

develop and provide appropriate software security updates.

If attackers become aware of vulnerabilities in software before

speaking software updates can be developed and provided,

a particularly large risk arises for IT systems or services. Who-

exploited by these vulnerabilities is also referred to as so-called

"Zero-day" attacks, since the developers had 0 days before the attacks began

Have time to fix the vulnerabilities.

IT systems or services in which

Vulnerabilities can be exploited by attackers directly over the Internet

can. Operators of such IT systems or services must therefore

particularly protect the security of the processing of personal

To guarantee data in accordance with Art. 32 DS-GVO. This includes in particular

also the timely import of security-related software updates.

Since with the release of software updates also possible attackers

Learning about vulnerabilities is especially critical for critical vulnerabilities

Hurry. Basically, it is for the secure operation of IT systems

or services that require the supply of security updates

for the software used is ensured by the manufacturer. Also is the

Observation of trustworthy sources of information regarding the

knowledge of vulnerabilities required. Should be a vulnerability

become known and an available security update has not yet been

can be played or if an update from the manufacturer is not yet available, so

the risk caused by the vulnerability must be assessed. Dependent

If necessary, further measures are to be taken based on the result

Ensure security of processing according to Art. 32 DS-GVO

and may extend to the deactivation of affected systems. The

In any case, the person responsible should document the procedure in order to

to comply with its obligations to provide evidence in accordance with Art. 24 Para. 1 DS-GVO.

"ProxyLogon" vulnerabilities in Microsoft Exchange Server

That this type of "zero-day" attack for Internet-accessible IT services

catastrophic consequences for business and public administration

ments and citizens in Hesse can have

with those that became public knowledge on Wednesday, March 3, 2021

Serious vulnerabilities in the Exchange email server software

from Microsoft (Microsoft Exchange). The vulnerabilities with the

CVE IDs CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-

27065, also known as ProxyLogon, existed

in a variety of Microsoft Exchange versions and made it possible

Attackers, affected IT systems (exchange servers) via the Internet

compromise (BSI, "Cyber Security Alert: Multiple Vulnerabilities

in MS Exchange, CSW no. 2021-197772-11032", https://www.bsi.bund.de/

SharedDocs/CybersecurityWarnings/DE/2021/2021-197772-1132.pdf).

This made it possible for attackers to gain access to the affected IT systems

and thus in principle also to the data stored or processed there

to obtain personal data. The Federal Office for Security in the

Information technology (BSI) went from 57,000 affected in Germany alone

Exchange servers and classified the vulnerabilities with the highest possible

Criticality as "IT threat situation red". Affected responsible persons must

ten therefore of a real and immediate danger to those of them

operated Exchange server go out. As a result of the vulnerabilities was

a variety of vulnerable Exchange servers are actively attacked and very

often compromised as well. Accordingly, many people in charge

in Hessen possible or already concretely recognized violations of the

Protection of personal data according to Art. 33 DS-GVO reported to me.

The technical background includes that the ProxyLogon vulnerabilities

put in the components or functionality of the Exchange server

located that connect via Hypertext Transfer Protocol Secure

(HTTPS) enabled. This is used for example for the frequently

Web mail interface Outlook Web Access (OWA), the module Unified

Messaging (UM) or for the synchronization of mobile devices

with "ActiveSync" required. Accordingly, Exchange servers were that

these functionalities not used or for the effective additional

technical measures had been taken before successful attacks

protected.

Fig. 4 Timeline of ProxyLogon vulnerabilities

The timing of events surrounding the ProxyLogon vulnerability

len is shown in Figure 4 as a timeline. This makes the danger

through these kinds of zero-day vulnerabilities. That's how they were below

vulnerabilities summarized under the term ProxyLogon

since the Microsoft Exchange version 2010, i.e. for more than ten years

available in all versions.

In its cyber security warning, the BSI quotes IT security service providers

which since November 2020 at customers indications of exploited and so far found unknown vulnerabilities. The ProxyLogon vulnerabilities were then in December 2020 by a Taiwanese IT security company discovered, analyzed and the company Microsoft on Tuesday, January 5, 2021. Upon request, the IT security Microsoft company on Thursday, February 18, 2021, that the corresponding security updates on Tuesday, March 9th, should be made available as part of the usual “patch day”.
At the same time, in January and February, various IT security service providers Attacks on the Exchange servers of individual companies and organizations exploiting the vulnerabilities found. This was also reported to Microsoft. From February 26th or 27th In 2021, different attackers then started to actively and extensively on the Internet for exchanges affected by the vulnerabilities ge servers to search. In response to this, the company Microsoft am Wednesday March 3, 2021, the security updates ahead of the usual Patchday ready and published a security warning with the call update affected Exchange servers immediately. According to this publication Attacker groups began publicizing the vulnerable Exchange servers to attack and compromise automatically and on a broad front.
On Friday, March 5th, the BSI issued a press release warning of the chess and announced that operators of affected exchange servers to contact vern directly and point out the danger situation (BSI, Press release “BSI warns: Critical vulnerabilities in Exchange servers – Immediate action necessary!” from May 5, 2021 https://www.bsi.bund.de/ DE/Service-Navi/ Press/Press Releases/Presse2021/210305_Exchan-

ge-vulnerability.html).

In the following week, the BSI then called the "IT threat situation

4/red" because there are still tens of thousands of Exchange servers in Germany

were endangered and immediate action by the operators was necessary.

On Friday, March 12, 2021, I published a press release on the

immediate need for action by those responsible and operators of

affected Exchange servers and for these types of incidents

specifies when a report of the incident in accordance with Art. 33 DS-GVO

is necessary for me (HBDI, press release "Immediate need for action

due to vulnerabilities in Microsoft Exchange Server” dated March 12, 2021).

The implications of these critical vulnerabilities for those responsible and

Operators of affected Exchange servers were far-reaching. To my

it can be stated that the security updates by the company Microsoft

were made available at a time when a multitude

successful attacks had already been carried out. On the other hand

some complex and time-consuming preparations had to be made

so that the security updates for the ProxyLogon vulnerabilities

could be played.

Since successful connections were already made before the security updates were

attacks on affected Exchange servers had been carried out, it was

not sufficient to import only the provided updates.

First, successful attacks had to be carried out on the affected Exchange servers

be closed, in case of doubt of a compromise of the

IT systems was to be expected. Therefore, it was first necessary to concerned

Exchange servers according to the available recommendations, guides and

comprehensive review of assistance. The person in charge provided one

successful attack on an Exchange server, he had this attack

contain effectively and deny attackers access. For this was

it is also necessary to use other IT systems and services in the environment of the

to comprehensively analyze the affected Exchange server in order to establish a lateral

Prevent or counter the spread of attackers.

Privacy Assessment and Response

From the point of view of data protection, it must be stated that a successful

Attacking an exchange server in the above scenario resulted in a breach

the protection goals of confidentiality defined in Article 32 (1) (b) GDPR

reliability, integrity and availability. These aren't the only ones

email content including its attachments, but also the associated ones

Metadata of the e-mails with which the communication behavior of the users

can be analyzed. Others may be added

personal data, e.g. B. account data, entries in calendars or

Address Book Entries. Personal data breaches

Data according to Art. 33 DS-GVO was to be assumed in particular if

Instructions for access by unauthorized third parties were provided. Independent,

Art. 32 (1) obliges whether a compromise has occurred

DS-GVO responsible persons and processors for the following:

Art. 32. GDPR

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

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

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

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

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

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

a) the pseudonymization and encryption of personal data;

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

to ensure permanent equipment and services related to the processing;

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

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

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

quality of the technical and organizational measures to ensure the

security of processing.

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

to be taken into account 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.

Due to the presence of the ProxyLogon vulnerabilities, the security of the

Processing of personal data in accordance with Art. 32 Para. 1 DS-GVO

on the affected Exchange servers at risk. After becoming known

of the vulnerabilities, it was therefore necessary to reassess whether an

measured level of protection with the technical and

organizational measures could still be guaranteed. Usually was

jeopardizes the guarantee of the level of protection and therefore an immediate

reaction essential. To restore the required level of protection,

The measure was the immediate installation of the security updates
necessary but not sufficient. Since a compromise that has already
notification of the affected Exchange servers had to be assumed,
were at least those recommended by the manufacturer Microsoft or the BSI
implement further measures.
The concrete handling of the vulnerabilities caused by the ProxyLogon
resolved incidents was not only for those responsible and operators of
affected Exchange servers an exceptional situation, but also has
my authority faced challenges. Overall it came in this
Related to over 250 reports of breaches of protection
personal data according to Art. 33 DS-GVO until the end of May 2021
these accounted for around a third of all reports pursuant to Art. 33 GDPR

technology and organization
during this period. Most messages met within the first
three weeks after the vulnerabilities became known.
In this type of incident where IT systems and services may
wise were successfully attacked and compromised, usually occurs
an individual technical clarification of the facts by my employees
and employees. In this way, I make sure that the
Controllers and processors fulfill their obligations under Art. 33
GDPR compliance and those implemented in response to the incident
technical and organizational measures appropriate and effective
to end it and prevent it from happening again. Furthermore
must be ensured that at a high risk for personal
Rights and freedoms of natural persons those affected by the

responsible according to Art. 34 DS-GVO.

The large number of largely similar incidents enabled me to

the processing of the vast majority of cases by a standard

standardized procedure and to process it efficiently. to the-

For this purpose, an optimized process for

designed, coordinated and implemented these types of incidents. Through mine

A questionnaire was developed for the employees

was sent to the person responsible together with the confirmation of receipt.

This questionnaire was used to record the relevant aspects of the incidents

and evaluated in a standardized way based on the answers. Building on this

was decided in which cases of a fulfillment of the data protection

legal obligations are assumed by those responsible

could. Incidents involving even after answering the questionnaire

If there were still unanswered questions about data protection, an individual

subjected to examination. This procedure made it possible, in addition to processing

Processing of the normal volume of reports in accordance with Art. 33 DS-GVO

the operations on the ProxyLogon vulnerabilities until the end of 2021

complete as much as possible.

Summary for all reported incidents did the technical review

The following result: Based on the process described, my

Employees over 250 reports in accordance with Art. 33 GDPR

processed and the incidents checked, evaluated and the person responsible

given feedback. Nearly 30% of the reported incidents came

According to those responsible, there was no compromise of the

Exchange server. A little over half of those responsible were

a successful attack and a compromise of the affected server

established or could not be ruled out. stayed here

the respective incident, however, according to those responsible on the

221

each affected server is limited. A lateral spread to further

IT systems was reported for just over 15% of incidents. At 10% of

Reports could put those responsible at high risk for the rights

and freedoms of the persons concerned do not exclude and have

informed them in accordance with Art. 34 DS-GVO. After evaluating the

returned questionnaires resulted from about a third of the

Incidents additional queries within the framework of an individual examination

have been clarified. By the end of December, the reported incidents were up

less than 2% of operations completed.

In the following, three cases are presented as examples – in a company,

a public body and a law firm – described in

where the vulnerabilities of Exchange servers are exploited by attackers

could become.

I. Late Response to Exchange Vulnerabilities

The ProxyLogon vulnerabilities in the company's email server software

Microsoft have created tens of thousands of Exchange servers worldwide

could be compromised. A prompt and reasonable

Response by those responsible would in many cases cause greater damage

can prevent.

On March 3, 2021, Microsoft had unscheduled software updates

published dates for the Exchange server software that has critical vulnerabilities

put the software for exchange server closed. Not until March 17th

In 2021, 20 responsible persons from Hesse reported to me in accordance with Art. 33 DS-GVO

possible personal data breaches caused by

these vulnerabilities were made possible. Among these was one

IT system house, the incident of which is described here as an example.

The notification already pointed out that in addition to the Exchange

ge server also several domain controllers, i.e. IT systems for authentication

tification of other IT systems and users, has been compromised

were. Developed for processing reports in accordance with Art. 33 GDPR

my house in connection with the ProxyLogon vulnerabilities

work process with a questionnaire and sent it to all

respondents who had submitted Art. 33 notifications for response.

Based on the evaluation of the completed questionnaire and the original

I have further reports from the responsible IT system house

information requested. Relevant for the technical examination were included

the lateral spread of the attackers in the controller's IT network,

the affected IT services and those by the controller in response to

technology and organization

technical and organizational measures taken in response to the incident. The

Among other things, the person responsible sent me the final report of the

made available to the IT security service provider commissioned by him. This kind

Reports are generally for a technical review of data protection incidents

helpful and generally enable, magnitude and criticality of the incidents

better assess.

For the specific incident, it emerged from the report that the initial

Compromise of the responsible person's Exchange server already on

March 4, 2021, i.e. one day after the publication of the security

security updates by Microsoft. This was done by the attackers

set up a so-called web shell that allows them later access

the IT system enabled. Four days later, on March 8th, this was

Web shell then used by the attackers as a starting point to gain access

spread laterally in the IT network of the person responsible. Here could

the attackers also completely compromise domain controllers and

theoretically full access to all IT systems connected to it and

-Obtain services.

This information led to further queries on my part in order to

Adequacy and effectiveness of the measures taken by the person responsible

Response to the serious compromise of its IT infrastructure

and verify the personal data processed therein. The

The person responsible told me that although the attackers largely

had access to its IT systems. As part of IT forensic

However, examination did not reveal any evidence of exfiltration or

other violation of the protection of personal data found

become.

In response to the successful attack, the person responsible

determined not to restore the compromised IT systems,

but has a complete on devices procured for this purpose

set up a new IT environment. Furthermore, all suggested

and recommended measures of the IT security service provider in full

scope implemented.

Based on the information provided by the person responsible, I came to the conclusion that

the attack after the phase of lateral spread by the person responsible

chen was discovered, but even before the protection of personal data

was injured by the attackers.

As an appropriate response to becoming aware of the critical proxy log

On the one hand, gon vulnerabilities were reported by the company on March 3, 2021

Microsoft released security updates for the Exchange Server and

must be imported immediately. Because of Microsoft and the

BSI published notices was still known that importing

of security updates was not sufficient, but of successful ones

Attacks on the Exchange Server had to be assumed. Therefore was

it is necessary to check the Exchange servers in operation for a possible

mediation to investigate. The time reported to me by the person responsible

Procedure suggests that the installation of the security updates

not taken place immediately and also the necessary immediate investigation

The Exchange servers were not checked for possible compromises.

The incident was only discovered over a week later when the attackers

already had access to the IT infrastructure of the person responsible and this

used. The question therefore arises to what extent the person responsible

Obligations according to Art. 32 DS-GVO to ensure security

has complied with the processing.

This regulation requires controllers and processors to

that they have a level of protection appropriate to the risk and their ability

to guarantee the protection goals on a permanent basis. It turns out

hence the question of how and how quickly critical vulnerabilities

placed in IT systems or services. The untested and

unplanned installation of updates can occur in complex IT systems

Disturbances in the operational process or, in the worst case, a failure

to lead. Therefore, for operational reasons, there may be delays in delivery

import come. To minimize the risk would then be necessary

supporting measures are necessary to prevent the exploitation of the vulnerability

to prevent, but at least to recognize. Depending on the risk

specific vulnerabilities, especially if they are simply about the

Internet exploitable and exploited en masse may possibly

also the deactivation of affected IT services and systems

be an appropriate measure. Especially the one considered here

In the run-up to the incident, there were not only specific warnings from the BSI with

speaking recommendations for action, but also a wide range of media

Reporting on the ProxyLogon vulnerabilities.

The obligation according to Art. 33 DS-GVO within 72 hours

Personal data breaches become known

report provided at least of a risk to the rights and freedoms of

affected persons can be assumed, the person responsible has complied.

Another aspect to be checked is whether notification of the

met about the breach of the protection of their personal data

according to Art. 34 Para. 1 DS-GVO is necessary. Relevant to the question of whether a

Notification of the persons concerned according to Art. 34 Para. 1 DS-GVO

has to take place is the circumstance whether the incident is likely to result in a

there is a high risk for the rights and freedoms of the data subjects.

In its risk assessment, the responsible party came to the conclusion that

there was no violation of the protection of personal data

is, as there are no indications of a data leak or access by the attacker

personal data was available and no other violations of

protection goals could be identified.

In the final assessment of the incident and the response of the responsible

literal I came to the conclusion that its taken action

although late, but then reasonable and sufficient to the

to end the incident and prevent a repetition of the facts.

After the discovery, the person responsible reacted immediately and

external IT security service provider with the comprehensive analysis of the incident

instructed. It was also important that the compromised IT systems were not

only cleaned or restored, but a new one on new hardware

IT environment built up while doing the proposed and recommended

Measures of the IT security service provider have been implemented.

The statement by the person responsible that the incident did not lead to any high

risk and no concrete violation of the protection of personal

ner data came because no data leak could be determined

and thus no notification of those affected in accordance with Art. 34 DS-GVO

was necessary, I accepted, pointing out to him that

that he is obliged according to Art. 33 Para. 4 DS-GVO to give me a changed

communicate information or new findings.

II. Impact of Exchange vulnerabilities on a

Hessian district

The weak points also had an impact in the area of public administration

len the software for Exchange servers as a gateway for attacks and for the
Possibility of data breaches and required comprehensive
Protection and precautionary measures.
On March 10, 2021, a Hessian district reported to me on time
According to Art. 33 Para. 1 DS-GVO that a Microsoft Exchange server from
was affected by the security gaps that had become known shortly before and
the possibility of a personal data breach
duration. The affected Microsoft Exchange server may be
Become the target of an attack, as part of which the vulnerabilities with
the designations CVE-2021-26855, CVE-2021-26857, CVE-2021-27065
and CVE-2021-26858 were exploited. These vulnerabilities

are also known as "Hafnium" vulnerabilities because Microsoft suspects
that a hacker group with the same name is behind the attacks.
In the notification, the person responsible stated that up to 450 employees of
a possible breach of the protection of their personal data
could be affected. However, the notification was only made as a precaution
been because an actual breach of protection has not yet been proven
could become. In the risk assessment it carried out, the district came
assessment to the conclusion that there is probably no high risk for
rights and freedoms of the persons concerned. Accordingly
also do not have to notify the data subjects in accordance with
Art. 34 para. 1 DS-GVO. However, he might have
affected employees the day after the potential

Protection violation informed voluntarily.

In his report he also presented me with the ones he had taken and planned

technical and organizational measures (TOM) with which he

wanted to ensure that a specific further protection violation did not

could occur. As an immediate measure, he has the manufacturer Microsoft

provided security updates imported after the possibly

affected servers had been taken offline. Also planned is one

to put a web application firewall into operation, which is suitable for comparably

to counter possible attacks because of the existing security gaps

Attacks can take place via the web application "Microsoft Outlook Web App".

The district was also responsible for processing Art. 33 notifications

Questionnaires created about the Exchange vulnerabilities were sent. Of-

These questions were aimed in particular at assessing the risk for

Rights and freedoms of the persons concerned by the person responsible

as well as the TOMs he grabbed as part of the incident. I had to

but remind the county to answer my questionnaire,

because he allowed the deadline to pass without result. The provision of § 43

Paragraph 3 of the Federal Data Protection Act (BDSG) means I have public bodies like that

here responsible regional authority although not subject to fines

Remedial measures are available if they fulfill their obligation under Art. 31 DS-

GMO to cooperate with my authority. However

In these cases, I also have the option of using them in accordance with Art. 58

Paragraph 1 lit. a DS-GVO to provide the necessary information

place. However, I did not have to make use of these powers,

because the district reacted to my reminder in time and the

submitted the completed questionnaire.

The answers showed, for example, that he had at least the

Manufacturer Microsoft and information provided by the BSI

226

technology and organization

evaluated and implemented the appropriate measures. in-depth

Queries were only necessary because the person responsible

not immediately able to state that his analyzes of the

incident were sufficient. At the same time, however, he could experience a data leak

exclude. As part of the consultation with him, he was able to

answer my queries satisfactorily. Finally

I could therefore assume that the person responsible

and implemented sufficient measures to bring the incident to an end

and prevent recurrence. With an appropriate notification

I completed the process.

III. Attacks on Exchange vulnerabilities in

law firms

Hessian law firms were also the target of attacks

Exploiting vulnerabilities in Exchange Server software. attorney

Law firms, as responsible for data protection according to Art. 24

GDPR i. V. m. Art. 32 DS-GVO the security of the processing of them

entrusted data and must therefore be proactive and

deal seriously with the topic of information security.

Law firms in Hesse were also aware of the use of the

Vulnerabilities in Microsoft's Exchange Server software affected. Think

The authority contacted the Hessian bar associations at an early stage

contacted and informed about the problem. The Bar Association

Frankfurt am Main then issued a warning and advice on remedial

taken by the BSI are published on their website. As a result,

I've been following numerous personal data breaches

Art. 33 DS-GVO reported.

Law firms, as data protection officers, must

according to Art. 32 DS-GVO for the security of the processing of personal

general data. This includes “suitable technical and organizational

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

to ensure". After the discovery of security vulnerabilities in the

electronic data processing must prompt investigation and

Potentially affected systems are secured. This assumes that

the person responsible either himself or through commissioned service providers

already actively informed about developments in the field of IT security in

formed. The vague legal concept of "state of the art" is subject

a constant change that the person responsible has to follow.

227

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

After the threat was removed from the installation of the manufacturer-provided

initially provided security updates and additional measures

seemed to have been averted always reached me at the end of 2021

nor reports of the exploitation of existing or new ones

Vulnerabilities in Exchange Server software. Often they were

use compromised server to send emails with hyperlinks

det, which reload malware and thus further systems of the

can infect directional recipients. Here are practically in all cases

personal data affected, since the e-mails sent regularly
Metadata and message content of the stored correspondence
to give the recipient the appearance of authenticity. The
Downloaded malware can in turn encrypt the
Target systems make subsequent ransom payments for the encrypted ones
to extort data. Such an incident affects availability
personal data and can have serious consequences for the ongoing
have business operations of law firms.
It should also be noted that according to Art. 34 Para. 1 DS-GVO a
notification of data subjects about the violation of the protection of
personal data is required when there are high risks to their rights
and freedoms cannot be excluded. This is up to one
Outflow of personal data subject to professional secrecy
are entrusted, particularly close. Notifications have been
those responsible are mostly carried out proactively. In individual cases,
this only after a tip from my authority. According to Art. 34 (3) lit. c
DS-GVO can also notify by public notice,
such as a note on the website of the person responsible, if
it would otherwise involve disproportionate effort.
The incidents described show impressively that lawyers and
Notaries who use information technology for professional communication,
seriously and continuously with the protection and maintenance of their
systems have to deal with. In the connected world, everything is about that
Internet-accessible system a potential target for cyberattacks. this applies
regardless of location, size, legal form or any property
of the person responsible as a person with professional secrecy.

18.4

Loss of media

The loss of devices and data carriers such as memory cards, USB sticks,

CDs/DVDs and hard drives is of particular importance when on these

228

technology and organization

Devices health data that have a higher risk of misuse

are saved.

Every day it happens that patients, for example, from a doctor's office

request the sending of documents from their patient file. Fast

are the requested findings from the doctor's office on a simple USB

Stick copied, put in an envelope and sent by post.

A few days later the patient called saying it was an envelope

arrived, but the USB stick was not included.

If the data contained on the USB stick was not backed up,

there is theoretically both the possibility that there will be disclosure

of personal data could come as well that unauthorized persons

have access to the data. Since in these cases you usually have nothing

If you can determine the exact whereabouts of the USB stick, you will

drive at least can not rule out. So it's from an “injury

of the protection of personal data" according to Art. 4 No. 12 DS-GVO

to go out

According to Art. 33 Para. 1 DS-GVO, the person responsible - in this case the doctor's office -

obliged to immediately and if possible within 72 hours after the

Infringement has become known to the competent supervisory authority

report, unless the violation of the protection of personal

Data not likely to pose a risk to rights and freedoms

of natural persons.

A risk to the rights and freedoms of individuals exists when

them discrimination, identity theft or fraud, financial loss,

unauthorized removal of pseudonymization, damage to reputation, loss of

Confidentiality of data subject to professional secrecy or other

there is a threat of significant economic or social disadvantages (cf.

Recital 85 GDPR).

In addition, Art. 34 DS-GVO provides that the data subjects have the

data breach are to be informed if the violation of the protection of personal

personal data is likely to pose a high risk to personal

rights and freedoms of natural persons. In doing so,

Protection breaches involving special categories of personal data

according to Art. 9 Para. 1 DS-GVO (e.g. health data), in most cases

cases of a presumably high risk, one thing

obligation to notify. There would be no high risk if

the data would have been securely encrypted so that unauthorized persons too

at great expense could not use the data.

According to Art. 34 DS-GVO i. in conjunction with Art. 33 (3) lit. b,

c and d DS-GVO receive the following information: Type of protection violation

tion, the name and contact details of the data protection officer or

another point of contact for further information, a description of the

probable consequences of the violation of the protection of personal data

Dates, a description of the actions taken or proposed

men to remedy the breach of personal data protection,

if necessary, measures to mitigate their possible adverse effects

Effects as well as recommendations to the persons concerned, such as the

adverse effects of the protection violation can be mitigated.

In the case described, the question also arises as to whether data is sent via USB

Stick and letter post may be sent unencrypted at all. The

DS-GVO requires according to Art. 24, 25 Para. 1 and 32 that the person responsible

taking into account the state of the art, the implementation costs,

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

the different probability of occurrence and severity of the risks for

the rights and freedoms of natural persons appropriate technical and

to take and implement organizational measures. that always

once again postal items are lost, will not be in the future either

be ruled out. In contrast to a normal letter,

electronic data carriers such as B. USB sticks, but the possibility

to securely encrypt the content. With such a measure,

also make postage more secure. The risk of losing

of the data carrier the data contained come to the attention of unauthorized persons

can, can clearly with the use of encrypted data carriers

be minimized. Such protection is therefore fundamentally required.

The selected form of encryption must be suitable for the

stored personal data actually effective before a

to protect against unauthorized access. You must use encryption software

be carried out using a correspondingly strong encryption algorithm

rithm, such as B. AES-256, supported. Responsible can search their

design for suitable software with this keyword,

having various commercial and freely available products to choose from

are available that can encrypt individual files or entire data carriers.

The transmission of the password for decryption to the recipient

must also be done in a safe manner. So the password is not allowed

be sent in approximately the same envelope as the storage medium.

A transmission on a separate path (e.g. telephone, encrypted e-mail,

separate letter with delayed dispatch) is recommended.

230

technology and organization

If the data on the data carrier were sufficient, according to the status

the technique encoded form could contain both a message

of the data breach as well as the risk of data becoming known to unauthorized persons

can be avoided in many cases.

18.5

Phase-out of technologies that do not comply with data protection law

Example fax

The data protection regulations for technology design and security

responsible persons are obliged to process personal data,

to critically evaluate their use of technology and adapt to changing ones

to adapt framework conditions. The example of the fax shows that

certain technologies are no longer used in compliance with data protection law

can become. With the gradual replacement of the fax, responsibility

literally in many areas of application due to digitization

specific alternatives that comply with data protection law are available.

I. Initial situation

Last but not least, technological change often leads to changed framework
conditions when processing personal data. these can
the previous compliance with data protection law of the technologies used in
Ask a Question. The data protection regulations make it necessary
that those responsible for changing technological framework conditions
observe and react to them when the changed
also the risk for the processed personal data
changes. Technologies that are no longer data-
can be used in accordance with property rights, be replaced by such
where this is possible. Digitization can be used in many areas
help to improve data protection.
Responsible persons are obliged to implement this requirement,
have a playing field when it comes to the exact type of implementation
space, in particular the selection of specific data protection law-compliant
alternatives are concerned. If there is a choice between several alternatives
ven exists and those responsible have complete control over such
be able to exercise means and procedures - if necessary with assistance
me from processors - this is not just about achieving the
Conducive to data protection law compliance, but also strengthens the digital
Sovereignty of those responsible, i.e. the possibility of their roles in the

digital world independently, self-determined and safe and their
to be able to fulfill data protection obligations (see item 3)
As an illustrative example of what these requirements look like and

how those responsible can do justice to them, the municipality will

communication medium "fax". For its use in processing

personal data, I commented in the reporting period

(Press release "On the transmission of personal data by fax"

from September 14, 2021, https://datenschutz.hessen.de/datenschutz/it-und-

data protection/for-%C3%BCtransmission-of-personal-data-by-fax).

II. Need for replacement no longer more compliant with data protection law

technology

According to Art. 5 Para. 2 DS-GVO, those responsible must

personal data the principles of data processing from Art. 5

Para. 1 DS-GVO (lawfulness, processing in good faith, trans

parenz, earmarking, data minimization, correctness, storage limitation,

integrity and confidentiality) and demonstrate compliance with them

can. According to Art. 25 DS-GVO (data protection through system design and

through data protection-friendly default settings) you are obliged to use these

Principles at the time the funds are determined as well as at the time

the actual processing by suitable technical and organizational

implement technical measures effectively. This results in an obligation

To observe developments in the technological environment, for example

to be able to react immediately to relevant changes.

Even with changing technological framework conditions, the

Guaranteeing the principles of integrity and confidentiality

Art. 5 Para. 1 lit. f GDPR to continue to ensure. technological changes

Changes often affect the way personal data is processed

processed, which may result in adequate security

the processing of personal data is no longer guaranteed. Around

the requirement from Art. 32 Para. 1 DS-GVO, an appropriate level of protection

To be able to guarantee that they can be fulfilled, those responsible must therefore in particular

evaluate and check them regularly in accordance with Article 32 (1) (d) GDPR

and evaluate whether the measures they have implemented are suitable for this purpose

are. This mainly concerns risks due to an unauthorized or unlawful

processing and by accidental loss, accidental destruction

or accidental damage to personal data as a result of

technological change.

232

technology and organization

To ensure compliance with this and other processing principles

Art. 25 DS-GVO must be guaranteed in the long term by those responsible in accordance with

Art. 25 Para. 1 DS-GVO the state of the art, the implementation costs

and the nature, scope, circumstances and purposes of the processing

as well as the different probability of occurrence and severity of the

Processing associated risks for the rights and freedoms of natural

people into account. Proceeding from this, they must in the sense of a

Data protection through system design and through privacy-friendly

default appropriate and appropriate means of data processing

as well as technical and organizational measures in order to

risk to ensure an adequate level of protection.

Due to the predominant role that the Internet plays in networking

most diverse areas of life in all of our everyday lives today, comes the

Transmission as part of the processing of personal data

special role. Frequently, processing operations no longer just find

within an isolated and fully controlled by the person responsible

technical environment. Instead, they also include a transmission

connection to one or more other IT systems, be they servers, mobile end

devices or everyday objects connected to the network ("Internet

of things"). As part of the increasing networking with the help

of Internet protocols or the digitization of formerly analogue ones

The transmitted data packets are transmitted via a variety of technologies

Connections between several intermediary points between the

involved terminals. The connections and points used

are - in contrast to the earlier circuit switching - not for the

reserved for both terminals. It is therefore conceivable that the IT systems involved

teme are distributed worldwide and by different governmental or private

actors are operated. In principle, these actors have the

Ability to access the packages they mediate. This

is particularly problematic when the two terminals of

do not encrypt packets sent to them.

A controller must at all times comply with the obligations outlined above

processing of personal data. Looking at his

Obligations to ensure the security of processing must be in accordance with

Art. 32 Para. 1 DS-GVO taking into account the state of the art, among other things

find It must always be taken into account which data

alternatives that conform to intellectual property rights to replace an outdated and not

more privacy-compliant technology is available. The

The comparability of alternative technologies is very important here

in the application scenarios of the respective processing activity, for which

which the technologies should potentially be used. For example

an asynchronous communication medium (such as e-mail) would not be without it

further as a substitute for a medium for synchronous communication (e.g.

the phone) as it is not in the same application contexts

is used. Likewise, the suitability of different technologies

deviate depending on the area of life under consideration and, for example, a legally secure

re communication with authorities require other properties than that

everyday communication between citizens. The factor

However, the user-friendliness of a technology must not be compromised

the possibility of ensuring the required level of protection of the

personal data processed in each case come to the fore.

As a result, this does not require a step-by-step approach to the replacement

more data protection compliant technologies. So those responsible should

identify which technologies they use result in

1.

that certain processing activities no longer comply with data protection law

can be implemented in a compliant manner

2. determine which data protection law-compliant alternatives for this

exist - possibly taking into account several different

which alternatives for different sub-areas - and finally

3. replace the corresponding technologies.

The replacement of technologies that no longer comply with data protection law is to be

ultimately always be fully implemented, each

but not necessarily done in a single step. A partial redemption

is possible, taking into account the individual circumstances, if alternative

tive, taking into account the relevant functional properties

were determined.

III. Example fax

The fax is a concrete example of a technology that was previously

based on an analog line-based data transmission. were there

Sender and recipient - identified by their respective fax numbers

– the two terminals between which an analogue connection is established

was built. This connection was then made from one end to the other

used to transmit the data streams that represented the fax.

The connection was reserved for the two terminals and was

Duration of communication used exclusively by these terminals. This

Type of mediation and transmission was up to and including the use of

ISDN technology common.

Nowadays, however, packet-switched data transmission also takes place with faxes.

ment with the aforementioned risks. By 2022 it should

In addition, analog telephony and the possibility of use throughout Germany

switched off completely by ISDN connections. At the nowadays

predominantly used packet-switched transmission method as fax over

IP (FoIP) based on standards for data transmission over the Internet

or when using services that automatically convert faxes into e-mails

convert, the data will not be encrypted without additional measures

and thus transmitted unprotected. By transferring over several

Distributed intermediate points there is basically a possibility of access

for unauthorized third parties. In addition, there are other risks inherent in the principle

Use of the fax, e.g. B. unauthorized disclosure of personal information
Data if the destination number is entered incorrectly or when printed out via public
public accessible target devices.
I have therefore pointed out to those responsible that the data protection
Legal requirements require the use of the fax in particular
against the background of the need for protection of personal data
to reflect. Since the fax is also used by such responsible persons,
the special categories of personal data pursuant to Art. 9 or 10
process DS-GVO, I have made it clear that personal data,
which have a special need for protection, generally not by fax
should be transferred if no effective additional protective measures
measures have been implemented by the senders and recipients.
All other bodies should also check whether data protection law-compliant algorithms
alternatives are available. Digitization, which increases the security of the
Fax weakens, but also enables secure electronic solutions
Communication. Concrete digital technologies are already coming in
question how about

– sending content-encrypted e-mail messages (PGP or S/MIME),
– Portal solutions in which the communication partners are news and
be able to provide and retrieve encrypted content,
– DE-Mail or
– area-specific digital communication services, such as the com-
communication about the infrastructure of electronic legal transactions
(EGVP/beA/beN/beBPo) or communication in medicine (KIM).

Because my authority for citizens and private and public
Places via alternative communication channels that comply with data protection law

reachable, i have my own fax numbers from all web sites

and styles removed under my responsibility.

235

Labor Statistics Privacy

19. Labor Statistics Privacy

Labor Statistics Privacy

19.1

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 in the reporting period

DS-GVO have been received. When complaints are at

Receipt counts those transactions that are submitted in writing

hen and where a natural person is a personal one

affected, applicable to Art. 77 GDPR

is. This includes duties. Complaints by phone

are only counted if they are written down

(e.g. by note).

b. "Consultations"

Number of written consultations. This includes total

marisch consultations of those responsible, those affected

people and their own government.

Not: (telephone) oral advice, training, lectures

Etc.

c. "Privacy Breach Notifications"

Number of written reports

i.e. "Remedial Actions"

Number of actions taken in the reporting period

were hit.

(1) according to Art. 58 Para. 2 a (warnings)

(2) according to Art. 58 Para. 2 b (warnings)

(3) according to Art. 58 Para. 2 c-g and j (instructions and instructions

regulations)

(4) according to Art. 58 Para. 2 i (fines)

(5) according to Art. 58 Para. 2 h (revocation of certification

gene)

case numbers

01/01/2020

until

12/31/2020

case numbers

01/01/2021

until

12/31/2021

5,414

5.179

(of that

855

(of that

953

taxes)

taxes)

1,983

2.123

1,433

2.016

(1) 1

(2) 31

(3) 13

(4) 2

(5) 0

(1) 1

(2) 28

(3) 3

(4) 29

(5) 0

237

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

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.)

f. "Formal support for legislative projects"

Here, as a lump sum, the total number of Parliament/

Government requested and conducted consultations

called. This also includes participation in public

committees and opinions dishes

(1) 198

(2) 5

(3) 724

(1) 47

(2) 16

(3) 1011

54

34

19.2

Supplementary explanations of facts and figures

The following illustrations explain and supplement the evaluations

on Section 19.1 also in comparison with the previous year and the other working

command in the reporting year. Overall, the number of cases is stabilizing in

my authority six years after entry into force and four years after

the entry into force of the GDPR at a very high level. while doing so

observed that in many areas the quality of the complaints

and the need for advice has changed. While at the beginning questions

according to the more formal requirements of the GDPR

(e.g. after the obligation to appoint a data protection officer, to

information and access rights of the person concerned), many questions

with which I had to deal in the reporting year, more in depth and

raise fundamental questions.

Complaints and Advice

This year, too, the data protection implementation of the always

again changing specifications of the Corona regulations by the responsible

present throughout the year. However, he made it through

the digitization push triggered by the pandemic also via the pandemic

also a very basic need for advice. So stood out in the

reporting year that technical solutions such as video conferencing technology

nik, which was quickly deployed during the pandemic, to support schools,

Keeping universities, companies and administration running, also about

to be used beyond the pandemic. Because in the introduction hurry

was required, the requirements of the data protection

be brought to bear. Other major digitization projects,

such as the implementation of the Online Access Act, the federal government,

The federal states and local authorities are obliged to reduce their administrative services by 2022

also offer online via administration portals, beat in the statistics

not to the extent that they actually concern the HBDI.

The cookie banners that are now placed upstream of almost all websites

many questions and ensure a significant increase in the number of cases in

Internet area.

In almost all areas in which I work, the question continues to play a role

according to the requirements for GDPR-compliant international data transfers

a major role.

The numbers in the area of credit bureaus and collection

so. On closer inspection, however, it can be observed that, above all,

the number of complaints relating to the provision of information is decreasing

relate and in processing unlike cases involving it

the storage of negative characteristics or debt collection is usually easier

are to be edited.

Finally, compared to the exceptionally high volume of

telephone inquiries the number under review returned to normal

measure decreased.

The following overview presents the amounts of input (complaints

and consultations) of the reporting year compared to the previous year:

Number 2020

Number 2021

areas of expertise

credit bureaus,

collection

school

school, archives

e-communication,

Internet

employee

data protection

video observation

credit industry

trade, craft,

Business

traffic, geodata,

Agriculture

loading

difficult-

the

1.201

loading

ratun-

gene

19

191

545

565

263

317

323

264

238

53

170

90

15

74

47

inputs

in total

difficult-

loading

the

1,220

736

618

433

407

338

338

285

634

132

772

255

413

314

212

220

loading

ratun-

gene

11

811

56

208

74

9

53

49

inputs

in total

645

943

828

463

487

323

265

269

239

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

201

17

137

201

80

169

65

63

91

3

52

57

20

11

10

see other

time

see other

time

86

258

115

73

119

4

59

56

17

91

29

0

3

29

1

s.

other

time

s.

other

time

287

275

252

274

199

173

124

119

108

94

81

57

23

40

11

see other

total

see other

total

20

6

26

286

7

142

141

72

197

77

85

79

11

94

25

2

8th

17

3

14

14

160

180

146

90

73

5

48

52

10

32

12

2

3

19

5

7

3

1

4

446

187

288

231

145

202

125

137

89

43

106

27

5

27

21

10

17

1

18

4,559

1,959

6,518

4.226

2.123

6,348

health, care

operational/

Official DPO

municipalities

Choose

police, judiciary,

frame protection

clubs, associations

address trading,

Advertising

housing, rent

social

supply

company

IT security,

IT technology**

insurances

broadcasting

see press

religious community

work

data protection except

half of the EU

research, statistics

Aliens Law

taxation

certification

Miscellaneous topics <

10 (e.g. chambers,

foreign affairs,

finance)

Subtotal

complaints and

consultations

240

Labor Statistics Privacy

40

40

1,433

7,991

9,444

2.016

8,404

6,384

17,435

14,789

BCR procedure

with German

or pan-European

leadership of

HBDI

reports from

data breaches*

Total

documented

inputs

Plus total tele-

phone consultation

and information

te of more than 10

minutes**

Total

documented

+ telephone

inputs

*Telephone inquiries that are not reflected in writing will generally

shelled recorded. They took the form of advice, information, explanations and understanding

questions about the GDPR and the like. both on general topics and on specific ones

questions such as B. for the concrete data protection implementation of the Coro-

na regulations. As an example, such telephone calls are made in November, as a month

without any special occurrences, counted and extrapolated as an average value.

**Other IT topics were accompanying a legal request or a data

to check the breakdown report and were therefore not counted independently.

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 38 requests for information from citizens

processing of your data at the HBDI and 11 corresponding

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

In 2021 I received 95 press inquiries. Numerous publications

and assistance was given to those responsible, citizens

on my homepage (e.g. on the subject of video conferencing technology).

provided.

– training services

Legal trainees were trained in their electoral or

management stations trained.

– Training and lectures

29 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

with contacts from non-European third countries

now essential for successful data protection in Hesse. The

Committee work is sometimes very time-consuming, but no longer dispensable.

Due to the pandemic developments, face-to-face meetings were held

often replaced by video conferencing. The conferences of the data

(DSK) and the Freedom of Information Officer (IFK) met

about every two months on current topics. The results of the year

2021 are printed in extracts in Appendix I and Appendix II,

but also in detail on the homepage of the data protection conference

www.datenschutzkonferenz.de.

I am involved in all areas of the DSK working groups. Also

in the sub-working groups set up for special topics,

employees get involved. In numerous EU

Labor Statistics Privacy

Committees (e.g. International Transfers Expert Subgroup, Border, Travel,

Law Enforcement Expert Subgroup, Financial Matters Expert Subgroup,

CSC, SCG SIS II, SCG Eurodac, SCG VIS) they could cooperate

bring in In addition, support services were also provided to the

EU Commission, such as B. through participation and contributions within the framework

the Schengen evaluation.

Remedial Actions and Legal Proceedings

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

Number

2020

1

31

13

2

0

47

Number

2021

1

28

3

29

0

61

Number

2020

19

2

Number

2021

24

2

Other

In total

* Of which two preliminary proceedings before the ECJ and 2 proceedings before the VGH in the 2nd instance.

8th*

34

4

25

243

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

Data Breach Notifications

Reports according to Art. 33 GDPR and § 60 HDSIG

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 mailing list

Abuse of Access Rights

Prohibited Posting

Incorrect assignment of data

Non-compliant disposal

Unencrypted e-mail transmission

Other

In total

most affected areas

Credit industry, credit bureaus, trade and commerce

Employee data protection

health sector

Number

2020

494

184

142

107

85

Number

2021

628

579

144

121

98

76

43

25

21

9

7

240

1,433

73

44

38

19

12

7

253

2.016

cases

2020

491

254

230

cases

2021

640

399

288

244

Appendix to I

Appendix to I

Appendix to I

1. Selected Resolutions of the Conference of Independents

Federal and state data protection supervisory authorities

"Use the opportunities of the Corona-Warn-App 2.0" from April 29, 2021

The conference of the independent federal data protection supervisory authorities

and the countries (DSK) recalled in view of more than a year

ongoing pandemic and the associated data protection issues

associated fundamental rights encroachments on the fundamental rule of law

The need to continuously and critically assess and evaluate these interventions.

In the course of such an evaluation and adjustment, the DSK asks for infectious

protective instruments by the federal and state governments, which are compatible with version 2.0

the Corona-Warn-App (CWA) opened up data-saving possibilities

the pseudonymised cluster detection and contact notification

to be examined in detail and in a timely manner.

The DSK recommends that the federal states consider the use of the CWA to be

Complete possibility to notify potentially infected people

and cluster recognition in their concepts for fighting pandemics

take into account.

Since the update to version 2.0, the CWA has had a corresponding one

Function that can be used to register at places or events,

where many people gather to register. Even if this

- unlike other apps - no personal data is collected

and can later be transmitted to a health authority

Pseudonymized cluster recognition of the CWA makes a significant contribution to

break chains of infection.

Through the direct networking of the CWA users, people

who were exposed to a potential risk of infection, immediately and

thus informed faster than via the health authorities. In addition, due to

the high acceptance of the CWA with meanwhile more than 27 million downloads

the likelihood is high that people will miss out on this possibility

Pseudonymous digital to be preferred from a data protection point of view

access registration.

Promoting the use of the CWA for cluster detection could help

result in the app being used by even more people. This

in turn, the chance of recognizing and warning of risk

continue to increase encounters outside of the use of cluster detection

and thus actively contribute to the fight against the pandemic.

2. Selected decisions of the Conference of Independent

Federal and state data protection supervisory authorities

2.1

"Energy supplier pool" must not become transparent consumers

lead" from March 15, 2021

Credit bureaus and energy suppliers are considering a so-called

to create an energy supplier pool. In this central data pool should also

Positive customer data is stored and sent to other energy suppliers

be transmitted. Positive data is data about contracts where the

do not give any reason for complaints, i.e.

behave compliantly.

Information on the number of contracts concluded and the respective

Duration of contract can indicate whether consumers*

intend to have a longer contractual relationship with an electricity supplier or

for example, regularly use offers for new customers. consumers,

who regularly select the most cost-effective offer on the market for you and

want to switch providers to do this, could

be excluded from attractively priced offers.

However, every citizen has the right to competition

between the energy suppliers and look for cheap ones on the market

search for offers. The desire to attract supposed "bargain hunters" in

to collect them in a central data pool in order to use them when initiating a contract

to be able to identify such and, if necessary, exclude them from offers

no legitimate interest i. s.d. Art. 6 (1) sentence 1 lit. f) GDPR.

It was precisely the aim of the legislature, by liberalizing the

effective and undistorted competition in the energy market

to enable the supply of electricity and gas. The attempt to

knew and to identify consumers who are willing to change and, if necessary,

to exclude them from certain offers would run counter to this objective.

Even if the interests of companies are considered legitimate

would prevail in such cases, the interests worthy of protection

and fundamental rights of customers. Contractual consumers may

rightly expect that none go beyond the purpose of the contract

Your data will be processed, which may limit your options, freely

to operate in the market.

The storage and transmission of positive data by an energy

sorgerpool would contribute significantly to transparent consumers and

would be illegal under Art. 6 Paragraph 1 Sentence 1 Letter f) GDPR.

249

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

2.2

“Processing of positive data from private individuals

Contracts for wireless services and permanent trading accounts

Credit Bureaus” from September 22, 2021

The DSK decides the following:

After re-examination of the legal situation, the decision of the DSK dated

06/11/2018 maintained, so that continue

1. the transmission and processing of so-called positive data to or through

Commercial and business information agencies generally do not rely on Art. 6

Paragraph 1 subparagraph 1 lit. f GDPR can be supported and

2. it is regularly necessary for the transmission and processing of so-called positive data

With the effective consent of the person concerned, taking into account

which requires high standards of voluntariness.

Reason:

In its decision of June 11, 2018, the DSK determined that trade and

Credit agencies so-called positive data on private individuals in principle

cannot collect on the basis of Article 6 Paragraph 1 Subparagraph 1 lit. f GDPR.

Positive data is information that does not have a negative payment history

ments or other behavior that is not in accordance with the contract,

but, for example, the information about the fact that a contract

was completed. With such positive data, this regularly predominates

legitimate interests of the data subjects, even beyond the use

to determine their data. If the data is used by a responsible

transmitted to a credit agency, the transmission is already in this respect

This data is regularly inadmissible in accordance with Article 6 Paragraph 1 Subparagraph 1 Letter f GDPR.

The processing of this data by the credit agency is also inadmissible.

The DSK now had to check whether the widespread practice of transmission

and processing of positive data relating to mobile service contracts and

Individual standing trading accounts require a different rating

is. This practice affects longer-term contracts that are

obligations or financing or deferral elements as credit-related

cal risks are considered, but do not show any breaches of contract.

They are used in the formation of score values for the persons concerned

Use trade or banking for credit checks, regularly

included along with a variety of other issues.

As part of this review, companies and associations had up to

August 31, 2021 opportunity to comment on the issues raised

submit legal questions. After careful evaluation of the received

Appendix to I

Genetic statements, the DSK comes to the conclusion that for the

Transmission of the positive data by the mobile service provider and the

Although commercial companies have legitimate interests, the quality of the

improve credit ratings and the economic actors involved

to protect against credit risks. Special circumstances that – as with

credit institutions, in particular because of their specific obligations

according to the Banking Act - in accordance with the resolution of the DSK dated

11.06.2018 regularly the interests, fundamental rights and fundamental freedoms

ten of the data subject overriding interest of the person responsible

or would arrange for third parties to process certain positive data,

however, the DSK was not able to determine this during its review. One

evaluation deviating from the above-mentioned basic rule is therefore not possible

Justifiable: Even with positive data on contracts for mobile phone services and

permanent trading accounts comes to the interests, fundamental rights and fundamental freedoms

rights of the data subject to determine for themselves whether they

relevant positive data for transmission by mobile communications service providers

and trading companies and processing by credit agencies

credit rating wants to reveal crucial importance. Here falls

particularly important that otherwise indiscriminately large amounts of data

collected and processed about common everyday processes in economic life

without the persons concerned having given cause for this.

Therefore, neither those responsible nor third parties can have an overriding interest

claim interest in these processing operations.

Data processing that takes place against the will of the data subject

of positive data on mobile service contracts and standing trading accounts

by contractual partners and credit bureaus is therefore without prejudice to others

Requirements not justified according to Article 6 Paragraph 1 Subparagraph 1 lit. f GDPR.

Your data protection-compliant transmission and processing is only on the

based on the consent of the data subject, for which the

general requirements must be met. In particular, the

Granting consent to the storage of the positive date is not required

be made a condition of the affected contract conclusion.

2.3

"Processing of the date 'vaccination status' of employees

the employer" of October 19, 2021

Employers may enter the date "vaccination status" of their

generally employed without an express legal authorization

not process it - not even in the context of the COVID-19 pandemic.

251

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

The legal basis for the processing of the date "vaccination status"

of employees § 26 paragraph 3 sentence 1 of the Federal Data Protection Act

(BDSG) not applicable.

The date "vaccination status" is a health date

Article 4 Number 15 Regulation (EU) 2016/679 (General Data Protection Regulation

tion – DS-GVO) and thus a special category of personal data

Data, Article 9 Paragraph 1 GDPR. Their processing is fundamental

prohibited and only permitted in exceptional cases.

In individual cases, the "vaccination status" date is processed on the basis of

legal regulations possible:

– Certain employers specified in the law

from the healthcare sector (hospitals, medical practices, etc.).

under the in §§ 23a, 23 paragraph 3 of the Infection Protection Act (IfSG)

the legal requirements mentioned above, the vaccination status of their employees

to process

– Certain employers specified in the law, e.g

Example providers of child day-care facilities, outpatient

Nursing services, etc., are allowed under those mentioned in § 36 paragraph 3 IfSG

Prerequisites related to the vaccination status of their employees

process with COVID-19;

– Employers are allowed to check the vaccination status of those

process employees who have a claim against them

Monetary compensation (wage replacement) according to § 56 paragraph 1 IfSG

chen. Its requirements may also apply in individual cases in the event of a

possible infection with COVID-19 and subsequent

quarantine available. The requirement for a claim is, among other things, whether

there was a chance of vaccination.

– Employers are allowed to check the vaccination status of employees

also process, insofar as this is due to legal ordinances on pandemic

control based on the IfSG is specified.

The processing of the date "vaccination status" of employees on the basis

Location of consent is only possible if the consent is voluntary

and has thus been granted with legal effect, § 26 paragraph 3 sentence 2 and paragraph

2 BDSG. Due to the between employers and

existing relationship of superiority and subordination to their employees

there are regular doubts about the voluntary nature and thus legal validity

the consent of employees.

In connection with querying the date "vaccination status" are further to

observe:

252

Appendix to I

GMO:

– Principle of "data minimization", Article 5 paragraph 1 letter c DS-

First of all, it must be checked whether simply querying the vaccination status

achievement of purpose is already sufficient. Then there is no storage

necessary. If the vaccination status is to be saved, no copies are allowed

Vaccination cards or comparable certificates (in the original or

as a copy) in the personnel file. it is sufficient

if it is noted that these have been submitted in each case.

– “Storage limitation” principle, Article 5(1)(e).

DS-GVO, right to erasure, Article 17 DS-GVO:

As soon as the purpose for storing the vaccination status no longer applies

this personal date will be deleted.

– Principle of “accountability”, Article 5(2) GDPR:

Employers must - if relevant - also

be able to prove that consent was voluntary, Article 7 paragraph

1 GDPR.

2.4

On the possibility of non-application of technical and

organizational measures according to Art. 32 GDPR on express

common request of data subjects”1 of November 24, 2021

1. The technical

Technical and organizational measures are based on objective

Legal obligations that are not at the disposal of those involved.

2. A waiver of the technical data to be provided by the person responsible

and organizational measures or the lowering of the statutory

prescribed standards on the basis of consent in accordance with Art. 6

Paragraph 1 subparagraph 1 lit. a GDPR is not permitted.

3. In compliance with the data subject's right to self-determination

and the rights of other data subjects, it can be documented in

be possible that the person responsible for

express wish of the informed data subject on their own initiative

certain technical and organizational measures to be taken

does not apply to her to a reasonable extent.

4. Chapter V of the GDPR (transfers of personal data to

third countries or to international organizations) remains unaffected.

1 The decision was made by the Conference of Independent Data Protection Supervisors

Federal and state authorities decided against the vote of Saxony.

Appendix to I

3. Selected guidance from the Conference of

independent federal data protection supervisory authorities

and the countries

Measures to protect personal data at

Transmission by email1 (as of June 16, 2021)

1. Objective

This orientation guide shows which requirements are to be met by the

drive through to send and receive e-mail messages

Controllers, their processors and public email service providers

bidder2 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 processors3 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

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

1 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.

2 Service providers who provide their own or third-party e-mail services for public use

hold.

3 processors exclusively with regard to their obligations under Art. 32 DS-GVO.

255

Transmission processes to be taken into account, which may be 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.4

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.5

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.

Certain persons, such as lawyers as well as

Doctors have special obligations as they are subject to professional secrecy

to keep the data entrusted to them confidential. In addition to the data
additional penal provisions, e.g. B. § 203 StGB, and professional law
observe. For the enforcement of these regulations are not the data protection
supervisory authorities, but law enforcement authorities, other authorities or
Chambers responsible for certain professional groups.
Nevertheless, data protection authorities have, when assessing the
to take into account the risks of processing personal data,
whether the data is subject to professional secrecy. In recital 75
The DS-GVO states: “The risks for rights and freedoms
natural persons ... can result from the processing of personal data
5
4 For communication with affected natural persons (e.g. with customers), a
Communication channel consist in the provision of a web portal.
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.
256
Appendix to I
Data emerge that become physical, tangible or intangible
damage could result, in particular if the processing leads to ... a
Loss of confidentiality of personal data subject to professional secrecy
data related to data ... can lead to ..."
If data is subject to professional secrecy, data protection

From a legal point of view, always check whether their processing is at a high level
risk within the meaning of the GDPR. This is particular when choosing
of technical and organizational measures within the meaning of Art. 32
GDPR must be taken into account, see Section 4.2.3.
Under data protection law, those responsible are obliged to
to take measures to the extent and extent described.
The requirement to take such measures can also arise
professional law and job-specific criminal law. In addition, can
this right justify further obligations that are independent
would have to be fulfilled by data protection law.
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.
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
SI/MIME (RFC 5751) and OpenPGP (RFC 4880) i. i.e. R. in connection with
PO/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 technical guidelines

never 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 the best possible, with proportionate

must achieve protection that can be achieved by means of means.

3.2. Due diligence when using e-mail

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.

258

Appendix to I

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 risks6

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

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. Obligations in the case of high risks

If a person responsible receives data specifically by e-mail in which the

Breach of confidentiality poses a high risk to the rights and freedoms of the

concerned natural persons, then he must be both qualified

6 For the classification of risks see briefing paper no. 18 of the independent data protection authorities

of the federal and state governments "Risk to the rights and freedoms of natural persons",

available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/

Kurzpapiere/DSK_KPNr 18_Risiko.pdf.

Transport encryption (see No. 5.2 below) and reception from end to

Allow end of encrypted messages.

If a person responsible accepts data specifically by e-mail, in which the

breach of integrity poses a high risk to the rights and freedoms of those affected

fenen natural persons, then he must existing (PGP or

Check S/MIME) signatures in a qualified manner (see No. 5.4 below).

4.2. Sending e-mail messages

4.2.1. Obligations for normal risks

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

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 by law

Confidentiality obligated

According to recital 75 of the GDPR, when processing

personal data that are subject to professional secrecy

a loss of confidentiality risks to the rights and freedoms of

affected person occur. This gives people unauthorized access to

the personal data contained in an e-mail message

this constitutes a personal data breach imposed by

technical and organizational measures (such as individual addressing

and, if necessary, encryption) is to be prevented.

260

Appendix to I

Because the existence of professional secrecy is an indication of a high risk

ko, those subject to professional secrecy have the amount of the respective

Risks to be checked carefully. Conversely, the fact that a

Data processing, here the revelation or disclosure of the data, criminal

or is not prohibited by professional law does not automatically mean that they are too

is permissible under data protection law or that from a data protection point of view

there is no high risk.

Are those responsible particularly obliged to secrecy, e.g. B.

carrier of professional secrecy i. s.d. § 203 StGB7, and exist upon transmission

of messages high risks for data subjects, so are the in Section 4.2.2

implement the listed requirements. As far as given the concrete

circumstances, only normal risks exist, the requirements of the

Section 4.2.1.

4.2.4. Permitted recipients of an email

When sending an e-mail message, due to technical and

organizational measures - additional measures are taken to ensure that

the recipient only people the message to be sent at their

take note of the receipt to which a disclosure of the

message is allowed. A suitable measure, especially at high

There is a risk of end-to-end encryption with individual ad

address to a person for whom the content is legitimately intended.

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 send

the MTA (Mail Transfer Agent) can be reached by the following measures

– the corresponding configuration settings are (En)Forced TLS,

Mandatory TLS or similar. If the remote station does not support TLS, then

7 For the relationship between data protection law and professional law, see Section 2.

the connection establishment is aborted. Some MTA allow a

domain-specific or rule-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

Verification of a certificate from a trusted certificate service

provider (S/MIME) or authentication of other trusted and

demonstrably reliable third party (OpenPGP). It is express

Lich pointed out 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

Use is to be carried out by retrieving validity information from the certificate

service provider (retrieval of CRI via http, OCSP). The review

Verification of the validity of an Open PGP 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 Open PGP key

server or the website of the key owner. Unless it's on a

such retrieval possibility is lacking, there must be guarantees 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.

263

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection

5.4. signature

With a signature using the SI/MIME and OpenPGP procedures, it is 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

generate security parameters that securely store the private key and

to use; as far as no direct comparison of the key between transmitter and

Recipient takes place, the corresponding public key of

reliable and trustworthy third party and they

make available to their communication partners.

Depending on the authenticity and integrity

risks mentioned in chap. End-to-end encryption measures listed

on the verification and management of the keys of the transmitters in

apply accordingly.

264

II

Second part

4. Activity Report on Freedom of Information

4. Activity Report on Freedom of Information

The Hessian Commissioner for Data Protection and Freedom of Information

introduction

1. Introduction Freedom of Information

introduction

This fourth activity report on freedom of information describes

and analyzes the freedom of information in Hesse in the year 4 since the regulation

the right of general and unconditional access to files

of public administration in the Hessian data protection and information

Freedom Act (HDSIG). As of May 25, 2018, this claim, his

Restrictions and its enforcement in the fourth part of the law

regulates After that, each person has free, unconditional and free of charge

Access to information held in public bodies. Included

the fundamental rights of third parties must be respected and protected. These concern the

free self-determination about your own personal data and

the protection of confidential secrets. The affected third parties are on

participate in the information release process. Likewise can

overriding public concerns such as public safety

prevent access to information. To the decision-making of

not to impair public bodies, there is access to information

only on files from completed proceedings. Access to information is

excluded from public bodies, insofar as he is responsible for the fulfillment of the task

of these positions would hinder. This regulatory concept was founded by

Legislators as follows:

"Administrative action should be more open and transparent in the future

the. In the fourth part ... regulations for a right to

Information access to the public authorities in Hesse created.

This gives citizens the opportunity to gain direct insight into

to take processes of the public administration. administrative decisions

tion become comprehensible and their acceptance is increased. The creation

a right to access information has such an important democratic

and constitutional function, because free access to public authorities

available information is an essential part of public participation

and control of state action. It promotes democratic opinion

and formation of will. The effective protection of personal data remains the same

guaranteed, conflicting legitimate public and private interests

are adequately taken into account" (state parliament printed paper 19/5728, p. 97).

The federal government and twelve states had already had regulations on information

mationsfreiheit or even to the transparency of the administration that the

Information access to all public bodies opened. Hesse chose

however, its own control concept. The right of general information

tion access only applies to the state administration. The communities and

However, districts should each decide for themselves through statutes whether

they open access to information about their files. Such information

So far, however, only four rural districts and one major city have freedom statutes

and a few small towns passed. For most administrations in

Hesse therefore does not yet have freedom of information. Accordingly, the
Freedom of information in the practice of administration in Hesse also in
to a lesser extent and still needs to develop in the future (see item 2).
As Freedom of Information Officer, I still had a lot in the year under review
to answer interesting questions about freedom of information
Citizens involved in enforcing their claims
participate in the discussion on the legal-political development of information
freedom of information and worked with other freedom of information officers in
Germany in the Conference of Freedom of Information Officers (IFK)
together. The fourth activity report offers information on these fields of activity
a small selection. He examines the question of which data of the applicant
ing person to which bodies may be passed on (see item 3),
explains why the Freedom of Information Officer is not acting on behalf of
an applicant can obtain information (see Section 4), and
describes the political discussion about an open data law in Hesse
(see item 5).

2. “Unconditional” access to information and community Statutory reservation

Access to information and municipal statute reservation

The right to information from public authorities is linked to
Freedom of information right not to the concern of the applicant
person on a specific matter. The request for information
Access may only be denied if this is evident from the information
freedom of information can be derived normatively. A municipality issues one

Freedom of information statute within the meaning of the HDSIG only related to their

self-government area, this is not illegal, but it harmonises

not with the overall concept of the Hessian freedom of information law.

1. The Freedom of Information Complaint

A lawyer (complainant) applied in a road traffic

opportunity (speed violation of his client) to me and complained that

that he has access to documents on test measurements (radar systems) in

the city of Kassel had not been granted. The Hessian Ministry of the Interior

I am involved in this context and have a right to access information

rejected. The petitioner therefore asked me to address the issue of access to information

claim to review in the matter.

2. “Unconditional” Access to Information

The Hessian Ministry of the Interior and Sport (HMdIS) had in one

Letter to the complainant his denial of the information

The right to freedom is justified, among other things, with the following statement:

"The transparency of the fine procedure and the legal protection of your client

were consequently included in the documents for the test measurements by the refusal

gen not injured. Against this background, we have already stated that

also an inspection of the documents of the

Test measurements according to §§ 80 ff. Hessian data protection and information

Freedom Act (HDSIG) resigns.”

This explanation was reason for me to add a supplementary position to the HMdIS

to ask for a letter from me. Because the quoted passage suggests that

A claim to freedom of information is only given if the applicant

could claim to be charged in the specific matter, for example

due to a lack of "transparency of the fine procedure".

But that is exactly not the case: In this respect, freedom of information is "of

unconditional", yes, that is almost what makes her special compared to others

Information claims (e.g. Art. 15 DS-GVO or § 29 HVwVfG), i.e

its essence, so to speak.

269

The Hessian Commissioner for Data Protection and Freedom of Information

4. Activity Report on Freedom of Information

Requests for access to information may only be denied if the

Freedom of information regulations justify this (§ 80 HDSIG).

§ 80 HDSIG

(1) In accordance with Part Four (= freedom of information), everyone has vis-à-vis public

Claim access to official information (access to information) …

(2) Insofar as special legal provisions regulate the provision of information, they go to the

provisions of Part Four.

Against this background, I asked the Ministry to explain why

exactly §§ 80 ff. HDSIG the information request in the matter

heit and informed the complainant about this

state of affairs.

The complainant then informed me that the city of Kassel, and

supported by the Ministry of the Interior, opposite him with a view to the information

information freedom right rejected the information access with the reason

have, the freedom of information statute of the city of Kassel only affects the

self-government area, but not the area of delegated

administrative tasks that are at stake here.

Then I got the freedom of information statute from the city of Kassel

can be submitted that explicitly allow access to information only for self-

administrative area, the city's own sphere of activity (§ 2 HGO).

3. Municipal statute reservation in the Hessian

Freedom of Information Right

Legal basis for information access statutes in municipal

The area is Section 81 Paragraph No. 7 HDSIG.

§ 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.

This provision establishes the validity of the Hessian freedom of information law

in the municipal sector, i.e. subject to the statutes.

Access to information and municipal statute reservation

In the legislative process there was no doubt that the statutory reservation

relates both to access to information in local self-government

area as well as to the tasks assigned to the municipalities by the state

refers (cf. § 4 HGO: instruction tasks, order matters).

It was also not considered that a municipality would respond to the "idea"

could come, the access to information with regard to the task type

split. To consider such a split to be unlawful would be the informa-

of course not beneficial, because then the municipality could

also equally opt to access information (in turn) entirely

to fail: So partial access is better than none at all.

Nevertheless, the situation in Kassel for the Hessian freedom of information quite bizarre: the state legislature has passed through for the state area Standardization of §§ 80 ff. HDSIG on freedom of information known. kassel is now denying access to information on the country's legal status related instruction tasks and order matters in the sense of § 4 HGO by explicitly stating access to information in its statutes just for self-government (one's own sphere of activity within the meaning of § 2 HGO).

All in all, the legal situation in Kassel is relatively positive, because the other larger cities in Hesse do not have any at all enact information access statutes and thereby prevent information access claims complete. And from the counties have so far also only Marburg-Biedenkopf, Groß-Gerau, Darmstadt-Dieburg and the Main-Taunus-Kreis opted for a freedom of information statute, that is just four out of 21 districts in Hesse.

The complainant I have concluded the process via the above the factual and legal situation described.

271

Disclosure of applicant data

3. Disclosure of applicant data

Disclosure of applicant data

If an applicant from the body requested for information the transfer of your data to third parties is prohibited, this is from the office observe. However, this can mean that in this case no information can be given in the matter.

1. The occasion

A citizen complained to me that he was at a university

so far unsuccessfully with the information access to contractual agreements

had desired at an institute. I then asked the university to

Information access application in accordance with the Hessian information

right to freedom (§§ 80 ff. HDSIG). Against this background

the university decided not only to accept the information access request

content, but together with the personal details of the applicant to the institute

to be announced for his opinion. This happened though in which

Request expressly the transfer of personal data to third parties

had been prohibited.

The university was of the opinion that it was authorized to do this, so that the institute

comprehensive for his position on the information access request

is informed.

2. Legal Assessment

This disclosure of the applicant's personal details by the university

to an institute was unlawful. A legal basis for such

Data transmission against the will of the applicant, i.e. evidently without

his consent (Art. 6 Para. 1 Subpara. 1 lit. a DS-GVO), is in such a

Constellation in accordance with the data protection and freedom of information

not available on the right (with regard to Art. 6 Para. 1 Subpara. 1 lit. e, Para. 2 and

3 GDPR, §§ 22, 83 HDSIG).

Even from the special procedural regulation in the case of involvement of third parties, § 86

HDSIG, can the agency responsible for information be authorized to

not derive the applicant's personal details against his will,

but the body responsible for information must give the third party only the opportunity

give an opinion on the request for access to information.

§ 86 HDSIG

The body responsible for providing information gives a third party whose interests it is through the application

Access to information are touched upon, opportunity to comment within a writing

month, provided there are indications that he has a legitimate interest in

exclusion of access to information.

However, an applicant's refusal may be about that

Name of the third party who is also affected by the access to information

known is given, cause the third party to oppose the coveted

issue of information. That can then have the legal consequence, for example

if a trade secret of the third party is concerned, that no information

is given, § 82 No. 4 HDSIG.

I have informed the applicant and the university about this legal situation

done. I also asked the university to contact the institute

arrange for the applicant's transmitted data to be deleted,

what happened then.

In the present case, the institute had no objections to the

Provision of information and the university then offered the applicant the

documents for inspection.

(No) information gathering for the applicant

If an entity refuses to provide information to an applicant

the Hessian Freedom of Information Authority cannot do this

legally binding obligation to provide information, nor may the

Hessian freedom of information officer himself the information

for the purpose of making them available to the person concerned

deliver.

1. The occasion

A citizen approached me with the request that I should get a job from

who he himself had unsuccessfully requested information to

release this information to me, and then I should

then transmit the information to him.

(No) Binding Order

2. Legal Assessment

2.1

The Hessian freedom of information law (§§ 80 ff. = fourth part of the HDSIG)

regulates in § 89 HDSIG the legal status of the Hessian Freedom of Information

Commissioner (Freedom of Information Authority). This norm gives after her

Paragraph 1 of every person who violates their right to information

sees the right to apply to the Hessian Freedom of Information Authority

complain.

§ 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.

In the event of such a freedom of information complaint, it will be

Checked by the Hessian Freedom of Information Authority. Is the complaint

justified, the freedom of information authority can the information obligation

Body (i.e. the body that has the requested information, § 85

Para. 1 sentence 1 HDSIG) request that the violation of the Hessian information

to remedy the right to freedom, i.e. to remedy the complaint (§ 89 Para. 3

p. 3 HDSIG).

275

The Hessian Commissioner for Data Protection and Freedom of Information

4. Activity Report on Freedom of Information

§ 89 HDSIG

(3) (...) If the Hessian Freedom of Information Officer establishes violations of the

provisions of the fourth part, he or she can rectify them within a reasonable period of time

demand. The competent supervisory authority must be informed of this.

However, such a request is not a (legally binding) decision

the Hessian Freedom of Information Authority towards the information

obligatory body, but (only) a legal appeal. The form of action

Administrative act within the meaning of the Hessian administrative procedure law (§ 35

HVwVfG), i.e. a binding order to act, is the

Hessian freedom of information authority towards public authorities

not available.

In this respect, there is a significant difference to data protection law.

The Hessian data protection officer is responsible in this area of law, namely

lich quite authorized to issue administrative acts to public authorities

enacted (cf. Art. 58 Para. 2 DS-GVO), but only under certain conditions

Conditions (cf. § 14 Para. 1 Clause 2 HDSIG). In freedom of information law

on the other hand, a "prompt" as already mentioned is (only) an appeal

to the body responsible for information. An additional emphasis is created

by informing the supervisory authority of the person obliged to provide information

body (Section 89 (3) sentence 4 HDSIG).

In this respect, the complainant's request that the Hessian information

information freedom authority may "oblige" the information-obligated body

to provide the requested information is not met

become.

2.2 No provision of information on the part of the Hessian

Freedom of Information Authority in favor of the complainant

However, there is one more provision, the meaning of which depends on the

Hessian freedom of information authority towards the complainant

rer with a view to his concerns, with her help to the coveted documents

was to be clarified. After all, the Hessian information

freedom of information of the freedom of information authority the right, with regard to

object of the complaint to the information-obligated office

and to inspect the relevant files and files

(Section 89 (3) sentence 2 no. 1 HDSIG).

276

(No) information gathering for the applicant

§ 89 HDSIG

(3) (...) The Hessian Freedom of Information Officer is particularly involved

1. Information regarding the issue about which she or he was called

grant and provide access to relevant files and files (...).

However, the Hessian Freedom of Information Authority allows this regulation

not to itself the information requested by the complainant

procure them in order to subsequently make them available to the complainant

to provide.

Because that would result in the legislative decision that the

Freedom of information authority towards the information-obligated body

can only appeal, counteract.

Such a procedure would namely constitute an inadmissible "enforcement"

on the part of the Freedom of Information Authority by way of one of the information

"Substitute performance" not entitled to by the health authority at the expense of the

means subject to obligation. However, such an approach is the

Hessian Freedom of Information Authority.

In the event of the (final) refusal of the

only the possibility of this before the administrative court

to sue for the provision of information (see also Section 87 (5) HDSIG).

I have informed the complainant of this legal situation.

277

Is open data coming to Hesse?

5. Is open data coming to Hesse?

Is open data coming to Hesse?

During the reporting period, I received a request from the Hessian state parliament to

a draft law by the FDP parliamentary group to open access to so-called

to comment on open data.

In principle, I support access to open data in the sense of the greatest

possible transparency of the public sector. The current developments

in the European Union show that increasing access to data

public authorities is desirable and the EU has a legal framework

men for uncomplicated access to data from public authorities and the

establishment of "data rooms" wants to establish.

1. Benefits of providing and using open data

When providing open data is in contrast to the previous

Legal situation, according to which an application for access to official information

information must be submitted, no application is necessary. The official

Information is already held and accessible ex officio

made. This increases the welcome transparency of the public sector.

But economic aspects also allow the provision of Open

Data appear desirable. To fulfill their public service

Public bodies collect a large amount of data. The provision

of these enormous data pools beyond the borders of the respective authority

has great economic importance. So promises the use of

Open data added value for large parts of the economy - right now

also for small and medium-sized companies (open data strategy

of the Federal Government, 2021, p. 10). In the following I will therefore present the current

applicable legal situation in the EU, in the Federal Republic of Germany and in

Hessen, the open data strategy of the EU and the federal government as well as

Outline the data governance law to show how in the future

use of open data could be designed.

2. Term "Open Data" and goal of providing open data

The term "open data" and the purpose of providing open data

are in Recital (EG) 16 of Directive (EU) 2019/1024 of the European

European Parliament and Council of 20 June 2019 on Open Data and

the re-use of public sector information (Open

Data Directive) (Official Gazette 172 of June 26, 2019, p. 56).

EC 16 Open Data Directive

The concept of "open data" (Open Data) denotes according to the general understanding

Data in an open format that can be freely used by anyone for any purpose.

det and can be passed on. A policy of promoting open data, the one

wide availability and reuse of public sector information

private or commercial purposes with minimal or no legal, technical

or financial restrictions and the dissemination of information

promotes not only for economic actors, but above all for the public, a

play an important role when it comes to promoting social commitment and the

Development of new services that combine such information in novel ways

ing and using, initiating and promoting. Member States are therefore encouraged to

the generation of data according to the principle "conceptually and by default open"

(open by design and by default) for all documents falling within the scope of this

fall policy, promote. This should provide a consistent level of protection to the im

also ensure goals in the general interest, such as public safety

in cases where it is sensitive confidential information on protection

critical infrastructures. You should also ensure that protection

personal data is ensured, even in cases where the information

in a single data record does not pose a risk of identification or

accessible to a natural person, but in combination with others available

information could create such a hazard.

The possibility of access to open data is not intended to provide access to personal

open relevant data. As far as personal data in the

data to be provided are included, it must be ensured that these are

the provision are anonymized and that also with the help

no re-identification of data subjects can take place based on additional knowledge.

3. Legal basis at EU and federal level

Recital 16 of the Open Data Directive already shows

that the provision of Open Data by public bodies within

half of the EU is a declared goal. There are also legal regulations at the federal level

Basics for the provision of open data. For the first time were through

the so-called Open Data Act (Federal Law Gazette I, 2206) with the on July 13, 2018 in

Section 12a of the E-Government Act (EGovG) that has come into force

indirect federal administration obliged to provide open data.

With the so-called second Open Data Act of July 16, 2021 (Federal Law Gazette I, 2941)

this obligation was basically applied to all authorities of the indirect federal

administration expanded. This regulates the implementation of the Open Data Directive

Data Usage Act (DNG) of July 16, 2021 (BGBl. I p. 2941, 2942, 4114)

finally details on the provision and further use of open

Data. The federal government has developed an open data strategy that

the implementation of the legal basis specified.

280

Is open data coming to Hesse?

4. Legal situation in Hesse

The legal obligation of public bodies to provide Open

Data goes one step further than the ones currently in force in Hesse

Freedom of Information Rules. The principle of freedom of information

says that public bodies request access to official information

have to grant. In Hesse, this is regulated in the fourth part of the HDSIG.

So far there is no obligation to provide Open in Hesse

Data, even if the DNG relies on the provision of Open Data by the

countries (Open Data Strategy of the Federal Government, 2021, p. 16).

5. EU Open Data Directive

The member states are bound by the Open Data Directive

to ensure that public data is further processed by public authorities

can be used, both non-commercial and

for commercial purposes. Expanded access to data should always be

be free of charge, with exceptions according to Art. 6 Para. 2 of the Directive, e.g. B. for

Libraries and museums are possible. Exceptions to the Obligation

for the provision of open data are regulated in Art. 1 Para. 2 of the Directive

and concern e.g. B. Documents that are trade secrets or confidential

contain information, or those for reasons of protection of

national security are not publicly available.

Chapter V of the Open Data Directive has special regulations for thematic

Created high quality dataset categories. Defines what those are

they in Art. 2 No. 10 and in Art. 14 Para. 2 Sentence 1.

Art. 2 No. 10 Open Data Directive

For the purposes of this Policy, the term means

10. "high-quality datasets" documents whose further use with important advantages

to society, the environment and the economy, in particular

because of their suitability for the creation of value-added services, applications and

new, quality and decent jobs and the number of

potential beneficiaries of value-added services and applications

these records;

Art. 14 para. 2 sentence 1 Open Data Directive

(2) The determination of certain high-quality data sets in accordance with paragraph 1 is based on the

assessment of their potential

a)

for the achievement of significant socio-economic or environmental benefits and

innovative services,

281

The Hessian Commissioner for Data Protection and Freedom of Information

4. Activity Report on Freedom of Information

be useful for a large number of users, especially SMEs,

b)

c) serve to generate income and

d) to be combined with other data sets.

According to Art. 14 Para. 1 Sentence 1 of the Open Data Directive, the Commission enacts

Implementing acts allowing the list of these high value data sets

ze is set. There are currently six categories in Annex 6 to the Directive

called high-quality datasets, namely spatial data, earth observation and

Environment, Meteorology, Statistics, Business and Corporate Property

as well as mobility. This particular high quality records need to be after

Art. 14 para. 1 sentence 2 of the Open Data Directive machine-readable, in principle

be available free of charge, via API and possibly as a bulk download.

6. The federal government's open data strategy

The federal government's open data strategy lists three fields of action,

in order to be able to use open data more efficiently and meaningfully in the future (open

Data Strategy of the Federal Government, 2021, p. 19 ff.):

– Improvement of data provision as well as efficient and sustainable

sustainable design of the data infrastructure;

– Increasing an innovative, public welfare-oriented and responsible

efficient use of data;

– Increasing data competence and establishing a new culture in the

Handling data to ensure the quality and usability of the data provided

to increase.

7. Outlook: The data governance law of the EU

Since the regulations in force to date on access to open data

Further use of data that affects the rights of third parties,

not permitted, the EU Commission has planned an advance to also

allow further use of such data. With the suggestion of

25 November 2020 for a regulation of the European Parliament

and the Council on European Data Governance (Data Governance

Law; hereinafter DGG) (COM(2020) 767 final) prepared the European

Commission proposes a European data space, the basis for a

future data economy should be. After opinion of Parliament

and the Council's common position, the Council and Parliament agreed

ment on November 20, 2021 in the trilogue on a common version of the

Is open data coming to Hesse?

Regulation (Council Document 14606/21) pending by Council and Parliament

must be formally decided.

On the one hand, the regulation serves to avoid distortions of competition

in the internal market by the public sector with regard to value-added services,

which is developed based on public sector data and

are offered (non-discrimination, prohibition of exclusivity

agreement). On the other hand, the directive harmonises the conditions of the

Further use of accessible data (formats, fees) (Hartl/Ludin,

Right of access to data, MMR 2021, 534 (535)). For this purpose, public

Provide private companies and data subjects data about which they

dispose of, disclose to others for use. This is supposed to make a difference
on the previous regulations on the provision of open data
apply to personal data. It should be noted here that in the
future data room, the fundamental rights of data subjects are protected
the should. To this end, EU law should be effective in the European data space
enforced and the protection of personal data unrestricted
be respected (Roßnagel, protection of fundamental rights in the data economy, ZRP
2021, 173 (174)).
The DGG is the first attempt to normative data usage and data protection
to reconcile. This is mainly due to the fact that the DS-GVO
also in the field of data management retains its full validity and through that
DGG supplemented only selectively with regard to three types of responsible persons
will: public bodies, data intermediaries and data altruistic organizations.
With regard to data protection, it makes sense to distinguish between personal
and to differentiate between non-personal data (Roßnagel, ZRP 2021,
173 (175f.)). For the protection of personal data are specific
Protective measures are necessary, which are only included in the recitals to the DGG,
but not contained in the legal text itself. What matters is that one
Re-identification of the persons concerned is prevented. Is such
sufficient protection of fundamental rights is guaranteed by the creation of a
European data space through a data governance law
desirable.
A strengthening of the European economy through freer access to data
is also possible through access to data from private
have been collected (so-called "business-to-business data sharing"
or “B2B data sharing”). However, the DGG does not require a legal one

Access to private data, but strengthens voluntary data sharing.

The proposal goes even further than the regulations outlined above

the European Commission for a law on digital markets (Digital

Markets Act - DMA) (COM(2020) 842 final). It remains to be seen how that

283

further regulations on access to data, the economic interests

ressen on the one hand and the necessary protection of fundamental rights on the other

reconcile with each other.

In Hessen it will be discussed how this development is supported and

as for the Hessian legal system to the resulting regulations of the

Union law has to be adapted and make it more concrete and supplement it

can.

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

2020

64

47

2021

71

52

285

ANNEX to II

Appendix to II

Appendix to II

1. Selected Resolutions of the Conference of

Freedom of Information Officer in Germany

Appendix to II

1.1

"More transparency in the protection of the Constitution - trust and

Strengthen legitimacy!” from June 2, 2021

The federal and state authorities for the protection of the constitution have the task of

free democratic basic order of the Federal Republic of Germany

protect against threats. The advance of specific dangers to fulfilment

information gathering measures taken in their duties

are mostly subject to secrecy. But this does not mean that

their entire activity must inevitably be opaque.

Transparency obligations, such as the obligation to create constitutional protection

directed, are found not only in the constitutional protection laws of the federal government

and the federal states (cf. § 16 BVerfSchG). In principle, the press has

a right to information under press law, unless the operational

business of the authorities is affected. So are e.g. B. Topics and participants

of background talks, even against the will of the authorities,

to rent. In addition, citizens have

Environmental information laws of the federal and state governments basically one

Right to access environmental information from the constitutional

protection authorities.

If the authorities according to press or environmental information law

must provide information, unless their secret activity is affected,

it is not clear why they respond to corresponding general questions

according to the freedom of information right to remain silent.

More transparency strengthens trust in the authorities for the protection of the constitution

and increases their legitimacy.

The conference of freedom of information officers in Germany demands

therefore call on the legislators at federal level and in the states concerned to

abolish exceptions for the protection of the constitution and the corresponding

Appropriate exception to the protection of specific security concerns in the

limited to individual cases.

1.2

"Demands for the new federal legislative period: A

Create a transparency law with a role model function!” of June 2, 2021

Information is the basis of a democracy. A democratic state

cannot do without a free and well-informed public opinion

consist. The right of access to information is a key element

to regulate the flow of information from government agencies to citizens

and citizens in Germany. Modern transparency laws provide the

Information about a register on the Internet without prerequisites and free of charge

available.

The Conference of Freedom of Information Officers in Germany (IFK)

therefore calls on the legislature to

of to modernize in the next legislative period and the IT

federal freedom law to a modern transparency law

develop a transparency register. In particular, the IFK demands:

A Further development of the Freedom of Information Act in a

Transparency Act with a Transparency Register

– The Federal Freedom of Information Act (IFG) must become a real one

Transparency Act with a legally regulated transparency register

to be further developed.

– In the Federal Transparency Act, the IFG and the Um-

World Information Act (UIG) to be merged. different

Regulations in the IFG and UIG complicate access to information

no unnecessary. The summary of information claims in one

Law is clearer and more citizen-friendly. "A unified

overarching Transparency Act would increase awareness, the applica-

the friendliness and assertiveness of all information access

increase laws." (cf. Federal Environment Agency (Dec. 2020): Evaluation of the

UIG; p. 163)

– As in several countries, the transparency register should be a catalogue

contain information subject to disclosure. The publication

other appropriate information should be explicitly allowed.

– About the information published in the Transparency Register,

should, in particular, cabinet decisions and their associated

Binett templates, contracts of public interest, expert opinions, studies

and essential company data of state holdings.

– A provision should be included in the law according to which internal

information made available upon individual request,

can also be published in the information register (Access for

one = access for all) if there is a public interest in the publication

tion exists.

B Area Exceptions and Reasons for Exclusion

– The reasons for exclusion of the IFG require a fundamental revision

because some grounds for exclusion are superfluous or overlap

the. They should be reduced and harmonized.

– A general weighing up of interests between information and secrecy

interest (so-called public interest test) should be used as an additional corrective

be introduced.

– The area exception for the protection of the constitution goes too far and should

no longer be included in a new transparency law.

C Regulations to promote freedom of information

– The requirements for freedom of information are i. S.v. "Free information

heit by design” in the design of the IT systems right from the start

and include organizational processes.

– In the new Transparency Act, the appointment of an official

chen Freedom of Information Officers are provided as binding.

D Federal Commissioner for Data Protection and the

Freedom of Information

– The Federal Commissioner should be given the power to

men to eliminate violations of the right to freedom of information

to be able to

E legal policy

– In the new legislative period, the Federal Republic of Germany should

Ratify the Tromsø Convention. The Tromsø Convention is once a year

2020 international treaty that came into force, the minimum standards

advocates the right of access to official documents.

291

The Hessian Commissioner for Data Protection and Freedom of Information

4. Activity Report on Freedom of Information

1.3

“More transparency through official

Freedom of Information Officer!” from June 02, 2021

All public bodies should appoint freedom of information officers

as is already mandatory for data protection. In two countries

this is already provided for in the law: both in Rhineland-Palatinate and in

Thuringia is to have the right through the appointment of official officers

be encouraged to access information.

The advantages of such an order are obvious:

– Freedom of information officers can public bodies in similar

support in a way and promote freedom of information, as stipulated in the

area of data protection has long been envisaged.

– Freedom of information officers can assist their public bodies

be when these questions on the interpretation of the Freedom of Information Act

have, for example, when it comes to justification and scope

raised information access claims. This is guaranteed at the same time

the uniform application of the law within the public body.

- You can also ensure that an access to information

directed inquiry as an application for the realization of a subjective right

and not just qualified as a "simple request", but on time

is processed.

– It would also be expedient for them to process the corresponding

coordinate applications. The information freedom officers can

were available for support. This ultimately leads to a

Ease of work, since the employees are informed about their knowledge

benefit from the right to freedom of information.

– The freedom of information officers inform and advise the public

liens also to the proactive publication of information.

- At the same time, they are available to applicants for related issues

with the Freedom of Information Act as contact points.

The Conference of Freedom of Information Officers in Germany (IFK)

therefore calls on the federal and state legislators to

Development of official freedom of information officers in all German

mandatory freedom of information laws. The IFK recommends

bodies subject to information obligations, also within the scope of their organizational sovereignty

without obligation to appoint official freedom of information officers.

292

Appendix to II

1.4

"Implement the EU directive on whistleblower protection promptly!

Whistleblowers comprehensively and effectively

protect!” from November 03, 2021

Whistleblowers are people who report information

significant grievances in companies or authorities. They help,
thereby uncovering serious violations of the law, their elimination in
is in the public interest. This is mostly done by providing information
information, report legal violations to the authorities or to their
Inaction inform the media. whistleblowers
ensure transparency and enlightenment. The information of the public
however, is regularly in a tense relationship with her work
legal loyalty and confidentiality obligations. If employed
By making violations of the law transparent, they often run the risk of
breaching contractual obligations. informants
often risk not only theirs by disclosing information
workplace, but also their career and reputation.
Against this background, the EU issued a directive in October 2019
not only the conditions for the protection of whistleblowers
and whistleblowers, but also sets a minimum standard of protection
(Directive (EU) 2019/1937). The policy applies to reporting violations
against European law. However, it allows the Member States to
urged that protection be extended to whistleblowers reporting violations
report against national law. Whistleblowers who
adhere to the reporting procedure specified in it, should
be protected from reprisals. deadline for timely implementation
December 17, 2021. The Federal Republic of Germany has the directive
not yet implemented, however, since the last federal government did not agree
the reach of a whistleblower protection law.
There is no unequal treatment of whistleblowers
understandable. Why should someone who violates European

Law reports are better protected than someone who violates

German law revealed? After all, it is in the public interest

to become aware of any relevant violation of the law and to

deliver. Whistleblowers can also

Interlocking of European and national law often only in advance

very difficult to assess which legal matter is specifically affected. It is

therefore important that the legislature treats all whistleblowers equally

well protected and creates legal certainty.

293

The Conference of Freedom of Information Officers in Germany (IFK)

Calls on federal legislators to enact EU directives on the protection of whistleblowers

leblowers and whistleblowers as quickly as possible and

to extend the protection to whistleblowers who violate

report national law.

1.5

"Environmental information: advisory and control competence also on

State Commissioner for Freedom of Information transferred!" from 03.

November 2021

The report on the evaluation of the Federal Environmental Information Act

(UIG) proposed in October 2020 that a Federal Commissioner or a

To create Federal Commissioner for Environmental Freedom of Information, who or the

for compliance with and control of the provisions of environmental information law

responsible is. The report recommends that this task be assigned to the

Federal Commissioner for Data Protection and Freedom of Information (BfDI)

transferred to. Federal lawmakers approved this recommendation in March 2021

followed and has the or the BfDI in § 7a UIG expressly the authority

given to monitor compliance with environmental information law.

While the federal government now explicitly has a uniform advisory and control committee

If there is authority for both legal matters, this is the case in most countries

not the case so far. The State Commissioner for Freedom of Information

often only depend on compliance with the general right to freedom of information,

but not the environmental information law. Since the legal matters

do not differ significantly, their existing expertise remains

unused. With the people who turn to them, this meets with

confession. They want to be supported in that their concerns

is fully taken into account. The same applies to the authorities who

Freedom of Information Officer already in environmental information law

ask for support.

An applicant may currently be in disputes with federal authorities

count on the support of the Federal Commissioner. The arbitration

in disputes with state authorities or communities, however, you remain largely

going fails just because the request for information about the environment

addressed to a state authority. This unequal treatment is unacceptable

substantiate in a comprehensible manner.

The conference of freedom of information officers in Germany demands

therefore the state legislators to follow the example of the federal government and

the State Commissioner for Freedom of Information, if not already done

hen, expressly also the advisory and control competence for the handling

transfer world information law. To fulfill this new task

are the officers with sufficient human and material resources

equip.

1.6

"Ratify Tromsø Convention and uniform minimum standard

create access to information throughout Germany!”

from 03 November 2021

The Conference of Information Officers (IFK) calls for the new federal

government to approve the Tromsø Convention in the new legislative period

sign and begin the ratification process.

On 1 December 2020, the Council of Europe Convention No. 205 on the

Access to Official Documents (Tromsø Convention) of 18 June 2009

entered into force without German participation.

The Convention is an international treaty that

its member states are obliged to do so by way of national legislation

general right of access to official documents of the public

To create administration while maintaining minimum standards in processing

of information access requests. The convention thus applies

as the world's first international agreement that provides a general right

constituted on access to information on official documents. In the event of

of the violation of a contracting state, the European Court of Justice for

human rights are invoked.

The Federal Republic of Germany has to sign and ratify

of the contract so far waived. The last federal government argued

that with the Federal Freedom of Information Act (IFG) such a

Minimum standard for all of Germany already created and the goal of

convention has been reached. Ratification is therefore not necessary.

This view is incorrect, because the IFG only applies to the federal government, not

however for the countries. Not all countries have a freedom of information law

created with state commissioners for freedom of information. Bavaria, Nie-

Dersachsen and Sachsen currently have neither freedom of information laws

relevant state representatives. A uniform minimum standard

for access to information provided for by the Convention exists in

So not Germany.

In addition, the regulations of the Convention are not completely

with the provisions of the already existing freedom of information laws

of the federal and state governments. The convention is particularly at

the collection of fees much more citizen-friendly than the German one

Right.

If you want to achieve transparency and freedom of information permanently, you have to

also guarantee access to official information under international law.

More than twelve years after the agreement came into existence, it will be the highest

It's time for Germany to come up with a Europe-wide minimum standard for

acknowledges access to information.

List of Abbreviations

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection / 4th activity report on freedom of information

List of Abbreviations

OJ EU

Section.

Conditions

AES

TFEU

API

ArbZG

kind

Official Journal of the European Union

Unit volume

General terms and conditions of business

Advanced Encryption Standard

Treaty on the Functioning of the European

union

Application Programming Interface

interface or programming interface)

Working Hours Act

Article

Federal Labor Court

BigBlueButton

Binding Corporate Rules (binding internal

data protection regulations)

Federal Data Protection Act

Special electronic mailbox for lawyers

Special government mailbox

Special notary mailbox

decision

Works Constitution Act

Federal Commissioner for Data Protection and

Freedom of Information

Federal Fiscal Court

Civil Code

Federal Law Gazette

Federal Court of Justice

Federal Registration Act

BAG

BBB

BCR

BDSG

beA

beBPo

beN

acc.

BetrVG

BfDI

BFH

Civil Code

Federal Law Gazette

BGH

BMG

BTprints. and BT-Drs

BSI

BTLE

letter

BVerfG

BYOD

or.

approx.

Federal Office for Information Security

technology

Borders, Travel & Law Enforcement (Subgroup)

Letter

Federal Constitutional Court

Bring Your Own Device (mobile working with you

a private end device of the

employees)

respectively

Approximately

297

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection / 4th activity report on freedom of information

CoKoBeV

CoSchuV

COVID-19

CVE

CVSS

that.

i.e. H.

DNG

GDPR, GDPR

DSK

EDSA

EDPS

efA

eGovernment

EGovG

EGVP

recital

Etc.

EU

ECJ

EEA

EWO

f.

FAER

onwards

FIU

DeadlinesVO

GG

possibly.

GPS

GVBl.

Corona contact and operational restrictions

regulation

Coronavirus Protection Ordinance

Coronavirus disease 2019

Common Vulnerabilities and Exposures

Common Vulnerability Scoring System

the same thing

That means

Data Use Act

General Data Protection Regulation

Conference of the independent data protection

federal and state supervisory authorities;

in short: data protection conference

European Data Protection Board

European Data Protection Supervisor

One for all

e-government

E-Government Law

Electronic Judicial and Administrative

P.O. Box

recital

et cetera

European Union

Court of Justice of the European Union

European Economic Area

Registration office

the following

driving aptitude register

following (pages) / subsequent

Central office for financial transaction companies

searches

Regulation laying down the rules for the

Deadlines, dates and deadlines

constitution

in which case

Global Positioning System (Globales

positioning system)

Law and Ordinance Gazette (Hessen)

GWG

HBDI

HDSIG

HGO

HHG

HMdJ

HKM

HSchG

HSOG

HLKA

HMdIS

HTTPS

IBAN

ID

i. i.e. R

IfSG

ICU

i. r.d.

i. s.d.

i. S.v.

i. V. m.

IfSG

IMI

ISDN

IT

vehicle

AI

COM

List of Abbreviations

Money Laundering Act

Hessian representative for data protection and

Freedom of Information

Hessian data protection and information

liberty law

Hessian Municipal Code

Hessian Higher Education Act

Hessian Ministry of Justice

Hessian Ministry of Education

Hessian school law

Hessian law on public safety

and order

Hessian State Criminal Police Office

Hessian Ministry of the Interior and Sport

Hypertext Transfer Protocol Secure

International bank account number

Identification Number

usually

German Infection Protection Act

collection agency

within the framework of

in terms of

with the meaning of

combined with

German Infection Protection Act

Internal Market Information System

market information system)

Integrated Services Digital Network

information technology

motor vehicle

Artificial intelligence

European Commission

State VKS

lit.

LfV

LT Drs.

State video conferencing system for schools

Litera, letter

State Office for the Protection of the Constitution

State Parliament printed matter (Hesse)

299

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection / 4th activity report on freedom of information

mmr

NZA

No.

or similar

above

OLG

OVG

OWA

OWiG

OZG

PGP

PIMs

POLAS

PSD2

QR code

RED

No./Rn.

RegMoG

Rs.

S

s.

s.a.

SDG-VO

SIS II SCG

S/MIME

so-called.

SPH

Tax ID

StGB

StPO

300

Multimedia and Law (Journal)

New Labor Law Journal

number

or similar

above/named/named/named

Higher Regional Court

Higher Administrative Court

Outlook Web Access

Administrative Offenses Act

Online Access Act

Pretty Good Privacy

Personal Information Management Service

police information system

Payment Services Directive 2

Quick response code

Right-Wing File

marginal number

Register Modernization Act

case

page or sentence

please refer

see also

Regulation (EU) 2018/1724 of the European

Parliament and Council of 2 October 2018

about the establishment of a unified digital

Gateway to information, procedures, support

and problem solving services and to change

of Regulation (EU) No. 1024/2012

Schengen Information System II

Secure/Multipurpose Internet Mail Extensions

so-called/so-called/so-called

School portal Hesse

Tax identificationnumber

criminal code

Code of Criminal Procedure

StrlSchG

StVG

see below

TB

TKG

TOM

TTDSG

and

etc.

Subpar.

AROUND

UNITED STATES)

etc.

AssemblyG

VG

see.

VKS

VPN

e.g. B.

item

ZRP

List of Abbreviations

Radiation Protection Act

Road Traffic Act

see below

activity report

Telecommunications Act

Technical and organizational measures

telecommunications telemedia data

protection law

and

among other things

subparagraph

unified messaging

United States of America

and so forth

assembly law

administrative court

compare

video conferencing system

Virtual Private Network

for example

digit

Journal of Legal Policy

301

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection / 4th activity report on freedom of information

Register of Legislation

Register of Legislation

Register of Legislation

The versions valid at the time of processing are quoted.

law/regulation

site(s)

TFEU

ArbZG

BDSG

BDSG

BDSG

Civil Code

Civil Code

BetrVG

BMG

Treaty on the Functioning of the European Union, version

based on the contract that came into effect on December 1, 2009

Lisbon (Consolidated version published in OJ EC

No. C 115 of 09.05.2008, p. 47) last amended by the file

on the conditions of accession of the Republic of Croatia and the

Adjustments to the Treaty on European Union, the Treaty

on the functioning of the European Union and the Treaty on

Foundation of the European Atomic Energy Community (OJ EU L 112/21

from April 24th, 2012)

Working Hours Act 06.06.1994 (Federal Law Gazette I p. 1170, 1171); last

amended by law of December 22nd, 2020 (Federal Law Gazette I p. 3334)

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

changed by Article 10 of the law of June 23, 2021 (Federal Law Gazette I

p. 1858)

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

amended by Art. 10 G of June 23, 2021 (Federal Law Gazette I p. 1858, 1968)

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

Civil Code in the version published by

02.01.2002 (Federal Law Gazette I p. 42, 2909; 2003 I p. 738), last amended

by Art. 2 of the law of December 21, 2021 (Federal Law Gazette I. p. 5252)

Works Constitution Act in the version of December 10th, 2021 (Federal Law Gazette I,

p. 5162)

Federal Registration Act

CoKoBeV/

corona contact

and operating

restrictive

regulation

Ordinance on Limiting Social Contacts

and the operation of facilities and offers

Due to the corona pandemic (corona contact and

Operating Restrictions Ordinance) from 07.05.2020, reopened. through

Article 4 No. 3 of the Ordinance of November 26, 2020 (GVBl. p. 826)

303

The Hessian Commissioner for Data Protection and Freedom of Information

50th activity report on data protection / 4th activity report on freedom of information

CoKoBeV/

corona contact

and operational

restrictive

regulation

Ordinance on the restriction of social contacts and the

Operation of facilities and offers based on the

Corona pandemic in the version that will come into force on August 15th, 2020

the amendments by Art. 3 of the Seventeenth Ordinance on the

Adaptation of the regulations for combating the corona virus of

11.08.2020 (GVBl. p. 538)

CoSchuV/

coronavirus

protective regulation

Ordinance to protect the population from infections with the

ronavirus SARS-CoV 2 of 06/22/2021, repealed by Article 2

of the ordinance of November 24, 2021 (GVBl. p. 742)

CoKoBeV/

corona contact

and operating

restrictive

regulation

CoSchuV/

coronavirus

protective regulation

CoSchuV/

coronavirus

Protection Ordinance

Corona Contact and Operating Restriction Ordinance of

November 26, 2020, last amended by Article 2 of the Ordinance of

05/26/2021 (GVBl. p. 272)

Regulation to protect the population from infection with the

Coronavirus-SARS-CoV-2 from June 22, 2021 (GVBl. 2021, 282)

Regulation to protect the population from infection with the

Coronavirus SARS-CoV-2 from November 24th, 2021, last changed by

Ordinance of January 15, 2022 (GVBl. p. 57)

coronavirus

entry regulation

Ordinance on protection against entry-related risks of infection in

Reference to the coronavirus SARS-CoV-2 from September 28th, 2021 (BAnz AT

09/29/2021 V1)

Regulation of the European Parliament and of the Council on

European data governance (Data Governance Act;

hereinafter DGG) (COM(2020) 767 final)

Data Usage Act of July 16, 2021 (BGBl. I p. 2941, 2942, 4114)

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 to repeal Directive 95/46/EC (Privacy Basic

regulation) (OJ EU L 119 p. 1)

Law to promote electronic administration (e-government

law) (Federal Law Gazette I, 2749), last amended by law dated

July 16, 2021 (Federal Law Gazette I, p. 2941)

EU-US Privacy Shield

Commission Implementing Decision (EU) 2016/1250 of

07/12/2016 according to the directive 95/46/EC of the European

Parliament and Council on the adequacy of the EU

U.S. Privacy Shield protections (disclosed at

File number C(2016) 4176)

DGG

DNG

GDPR

EGovG

EU-US Privacy

shield

304

Register of Legislation

DeadlinesVO

GG

GWG

law on artificial

real intelligence

(suggestion of

European

Commission)

Council Regulation (EEC, Euratom) No. 1182/71 of 03.06.1971

laying down the rules for deadlines, dates and deadlines (OJ

No. L 124 p. 1)

constitution

Money Laundering Act of 06/23/2017 (Federal Law Gazette I p. 1822), the last

by Article 269 of the Ordinance of June 19, 2020 (Federal Law Gazette I p. 1328)

has been changed.

Proposal for a regulation of the European Parliament and

of the Council laying down harmonized rules for artificial

Intelligence (Artificial Intelligence Act) and amending

certain legal acts of the Union, COM/2021/206 final, 21.04.2021

HDSIG

HDSIG

HGO

HGO

HHG

HSchG

HSchG

HSOG

IfSG

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. 9 of the law of November 15, 2021 (GVBl. p. 718, 729)

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)

Hessian Municipal Code in the version of the announcement

of 03/07/2005, modified by art. 3 of the law of 11

December 2020 (GVBl. p. 915)

Hessian Municipal Code (HGO) in the version of

Announcement from March 7th, 2005 (GVBl. I p. 142), last changed

by Article 1 of the law of 07.05.2020 (GVBl. p. 318)

Law on the reorganization and amendment of higher education law

regulations and to adapt other legal regulations from

December 14, 2021 (GVBl. No. 56 p. 931 ff)

Hessian school law of August 1st, 2017, last amended by Art.

1 of the law of January 18, 2021 (GVBl. p. 166).

Hessian school law of August 1st, 2017, last amended 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 3 of the

Law of September 30, 2021 (GVBl. p. 622)

Law on the Prevention and Control of Infectious Diseases

in humans from 20.07.2000 (Federal Law Gazette I p. 1045), last changed

by Article 2 of the law of December 10, 2021 (Federal Law Gazette I p. 5162)

IfSG

Law on the Prevention and Control of Infectious Diseases

in humans from 20.07.2000 (Federal Law Gazette I p. 1045), last changed

by Article 4a of the law of December 21, 2020 (Federal Law Gazette I p. 3136)

Open Data Law

First law amending the e-government law (1.

EGovGÄndG) (Federal Law Gazette I, 2206)

Directive (EU) 2019/1024 of the European Parliament and of

Council of 06/20/2019 on open data and re-use

of public sector information (Official Gazette 172 of

June 26, 2019, p. 56).

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)

Online Access Act of August 14, 2017 (BGBl. I p. 3122, 3138),

which was last amended by Article 16 of the law of June 28th, 2021 (Federal Law Gazette I

p. 2250) has been changed.

Law establishing a standardized central file of

Federal and state police and intelligence services

to combat violent right-wing extremism

(Right-Wing Extremism File Act – RED-G) of 08/20/2012

(Federal Law Gazette I p. 1798) FNA 12-13, last amended by Art. 23 Eleventh

Responsibility Adjustment Ordinance of June 19, 2020 (Federal Law Gazette I p. 1328)

Register Modernization Act of March 28, 2021 (Federal Law Gazette I p. 591),

which was last amended by Article 11 of the law of July 9th, 2021 (Federal Law Gazette I

p. 2467) has been changed.

Regulation (EU) 2018/1724 of the European Parliament and

of the Council of October 2nd, 2018 on the establishment of a uniform

digital gateway to information, procedures, tools and

problem-solving services and amending Regulation (EU) No.

1024/2012

The Ninth Book of the Social Code – Rehabilitation and

Participation of people with disabilities, as amended by

Announcement of December 23, 2016 (Federal Law Gazette I p. 3234), last amended

by Article 7c of the law of September 27th, 2021 (Federal Law Gazette I

p. 4530)

Council Decision 2007/533/JHA of 06/12/2007 on the

Establishment, operation and use of the Schengen

Second Generation Information System (SIS II)

Criminal Code in the version published by

13.11.1998 (Federal Law Gazette I p. 3322), which was last amended by Article 47 of the

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

open data

policy

OWiG

OZG

RED-G

RegMoG

SDG-VO

Social Code IX

SIS II

StGB

306

StPO

StPO

StrlSchG

StVG

TKG

TTDSG

Register of Legislation

Code of Criminal Procedure, as amended by the notice of

04/07/1987, last amended by Art. 2 G for the implementation of the VO

(EU) 2019/1148 of the European Parliament and of the Council of

06/20/2019

Code of Criminal Procedure in the version published by

07.04.1987 (Federal Law Gazette I p. 1074, 1319, last amended by Art. 1 of the

Law of December 21, 2021 (Federal Law Gazette I p. 5252)

Law to protect against the harmful effects of ionizing

Radiation from 06/27/2017 (Federal Law Gazette I p. 196), last changed by

Art. 1, 2 First Amendment Act of May 20, 2021 (Federal Law Gazette I p. 1194 in conjunction with Bek. v.

03.01.2022, Federal Law Gazette I p. 15)

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)

Telecommunications Act of June 23, 2021 (Federal Law Gazette I p. 1858), last

changed by Article 8 of the law of September 10th, 2021 (Federal Law Gazette I

p. 4147)

Telecommunications Telemedia Data Protection Act of June 23, 2021

(Federal Law Gazette I p. 1982), which was last amended by Article 4 of the law of

12.08.2021 (Federal Law Gazette I p. 3544) has been changed.

AssemblyG

Assembly Act in the version published on

November 15, 1978 (BGBl. I p. 1789), last amended by Article 6 of the

Law of November 30th, 2020 (Federal Law Gazette I p. 2600)

sites

factual terms

A

remedial actions

account

paper shredder

administrative assistance

request for administrative assistance

anonymity

workers

Working time measurement

retention obligation

supervisory authority

– lead

- Affected

supervisory activity

processor

I 18.1, I 18.2, I 18.3, I 19.1, I 19.2

I 9.4, I 18.3

I 2.2

I 5.1

I 5.1

I 17.6

I 11.1, I 11.3

I 11.1, I 11.2

I 17.3

I 5.5

I 5.1

I1, I2.3

I 3.1, I 4.1, I 4.2, I 5.1, I 10.3, I 11.4,

I 14.2, I 18.1, I 18.2, I 18.3, I 18.5,

Employee data protection

Employment Type

Complaint

I 2.2

I 14.1

I 5.1, I 19.2

I 18.1, I 18.4

I 11.3, I 18.2

I 1, I 2.1, I 2.5, I 6.2, I 6.3, I 11.1,

I 11.2, I 11.3, I 11.4, I 13.2, I 18.1

Annex I 2.3, Annex II 1.4

I 2.1, I 2.5,, I 6.3, I 11, I 11.1, I 18.1,

I 19.1

I 2.5, I 11.1, I 11.2, I 11.3

I 1, I 2.2, I 2.3, I 2.5, I 3.1, I 5.1, I 6.1,

I 6.2, I 6.3, I 7.4, I 8.2, I 9.2, I 9.6,

I 10.1, I 11.2, I 11.3, I 11.4, I 12.1,

I 12.2, I 13.2, I 14.1, I 14.2, I 15.2,

I 16.1, I 18.2, I 19.1, I 19.2, I 2.1,

II 2.2, II 2.3, II 4.2, II 6

I 2.2, I 2.6, I 3.6, I 6.2, I 8.2, I 9.6

data subject rights

Internal Market Information System I 5.1

credit check

Brexit

Federal Network Agency

I 18.1

Appendix I 3

I 18.5, Appendix I 3.1; Appendix I 4,

Appendix I 5

I 18.3, I 18.5, Appendix I 3.1,

Appendix I 4, Appendix I 5

Appendix I 5.2, Appendix I 5.3

I 19.2

I 8.1

I 13.2

I 1, I 24, I 2.5, I 4.1, I 4.2, I 6.2, I 8.2,

I 9.1, I 9.2, I 9.4, I 12.2, I 17.1, I 17.2,

I 17.6, I 17.5, Appendix I 2.3,

Appendix I 2.4, II 3

I 2.2, Appendix I 2.3

Appendix I 2.1

I 18.5

I 17.2, Annex I 3.2, Annex I 4.2,

Appendix I 5.3, Appendix I 5.4

I 2.5, I 7.2, I 7.4, I 13.2

I 3.1, I 4.1, I 5.1, I 6.3, I 10.1, I 10.2,

I 11.1, I 11.3, I 11.4

I 3.1, I 5.1

Exchange

f

Facebook

I 7.4

I 16

I 1

I 5.1, I 19.1, I 19.2

I 14.3, I 18.1, I 19.2

I 9.2

I 7.1

I 15.1

I 17.6

I 9.5, I 17.3

I 18.3

I 2.2, I 2.3

I 2.2, I 2.3, I 6.2

I 2.2, I 2.3,

I 6.2, I 11.4, I 19.1, I 19.2

I 8.2

I 7.1

I 2.2, I 2.4, I 2.5, I 6.2, I 11.1, I 14.3,

I 17.2, I 17.3, I 17.4, I 17.6, I 18.1,

I 18.3

I 2.5

I 11.3

Google

314

I 9.4

I 1, I 3.1, I 4.2, II 5.7

I 1, I 4.2, I 9.2

I 1, I 2.1, I 4.1, I 11.2, I 11.2, I 18.1

I 13.2

I 2.2

I 15.2

I 2.1, II 5.7

I 5.1

Appendix I 2.3

I 2.5

Appendix I 2.3

Appendix I 1

I 2.2, I 2.6, Annex I 1

II 1, II 2, II.3, Appendix II 1.2,

Appendix II 1.6

II 1, II 2, II 3, II 4, II 5, Annex II

II 15.1

I 9.6, I 11.3, I 15.1, Appendix I 2.2

I1, I12.2

I 8.2, I 18.2

I 2.5, I 8.2, I 11.2, I 18.2

I 2.2, I 2.6, I 6.3, I 8.3

I 6.2, I 7.1, I 7.2

I 11.2, I 11.3, I 13.5

– Monitoring of

members

mobile device

N

intelligence services

tracking

user profiles

O

epiphany

disclosure

One shop stop

Online services

Online Access Act

open data

open source

administrative offences

P

padlet

Pandemic

parking spaces

houses of Parliament

316

patients

- - data

- - file

personnel file

I 2.3

I 2.2, I 2.3, I 17.1

I 9.5, I 11.1, I 11.2, I 11.3, I 12.1,

I 12.2, I 13.2

I 8.1, I 12.2

I 10.2

I 12.2

I 14.1, I 16.1

I 6.2, I 7.1, I 7.2, I 7.3

I 7.3

I 3.1, I 5.1

Appendix I 2.2

I 6.3, I 8.1, I 9.3, I 12.2

I 3.1

I 18.2, I 18.3

I 11.3, I 18.4, Appendix I 1

I 18.2

I 11.2, Appendix I 2.3

I 17.2

I 3.1, I 6.3, II 4

I 7.2

I 13.1

travel returnee

restaurant

risk assessment

risk areas

S

sanctions

Statutory reservation, municipal

scoring

Schengen Information System

second generation (SIS II)

Schrems II judgment

Students

school portal

school board

protection level

vulnerabilities

redactions

confidentiality

screenshots

security agencies

security of processing

signature

meeting minutes

sovereignty, digital

Social networks

State Education Board

318

I 8.1

I 2.4

I 2.1, I 2.3, I 6.2, I 7.3

I 18.2, I 18.3

I 2.4, I 8.1

I 6.1, I 18.2, I 11.4, I 18.1

II 2

I 18.3

I 7.2

I 1, I 3.1, I 4.1, I 5.1

I 4.2, I 9.1, I 9.3, I 9.5, I 9.7

I 9.1, I 9.7

I 4.2, I 9.3, I 9.7

I1, I3.1, I5.1, I17.2, I18.3, I18.5

I 18.3

I 9.6

I 17.1, I 17.3

I 11.2

I 3.1

I 3.2, I 4.1, I 6.1, I 18.2, I 18.3, I 18.5

Appendix I 3.2

I 8.2

I 3, I 4

I 2.5

I 9.3

320

I 7.3

I 18.2

I 4.1, I 14.1, I 17.2, I 18.2, I 18.3,

I 18.4, Appendix I 3.2, Appendix I 4.1,

Appendix I 4.2, Appendix I 5

I 9.6, I 17.1, I 17.2, I 17.3, I 18.2,

I 18.3, I 18.4, I 18.5, Annex I 3,

Appendix I 4

I 11.2, I 19.1, I 19.2

I 6.2, I 7.1, I 7.3, I 13.2

I 13.2

I 3, I 4, I 11.1, I 18

I 3, I 4, I 11.1, I 18

I 12.2

I 18.2, I 19.2

I 6.2, I 12.2, I 19.2

I 13.2

I 14.1

I 3.1, I 8.2, I 9.3

I 15.2

I 11.1

I 6.2, I 7.1, I 9.2, I 9.3, I 10.2, I 18.5,

Appendix I 3.2