Fifty-First Activity Report

to data protection

and

Fifth activity report

to freedom of information

of

Hessian Commissioner for Data Protection

and freedom of information

professor dr Alexander Rossnagel

submitted by December 31, 2022

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

51st activity report on data protection / 5th 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 20/9575

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

detect major violations - in complete contrast to development

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

accepted and not fundamentally questioned. Nevertheless are

in many areas the requirements of the General Data Protection Regulation

Regulation (DS-GVO) is still not sufficiently implemented, lead to

Complaints and require the intervention of the Data Protection Authority.

Most of those responsible eliminate conditions that violate data protection

immediately. If this was not the case, formal orders helped

Enforcement Actions and Sanctions. The digitization of many

Tasks and activities cause additional

che obligations, entails additional requirements and requires

additional attention (Part I Ch. 1).

2. Enforcing data protection law is carried out by technical systems, service

ments, contractors and business models that are not

meet the requirements of data protection, because the providers

are unable or unwilling to comply with European data protection

to meet demands. Those responsible in Hesse who claim them

take, are generally unable to hold their accountability

according to Art. 5 Para. 2 DS-GVO. Therefore it depends

as far as possible technical and organizational alternatives to those from the

Hardware, software, services and platforms offered in third countries

and thereby achieve digital sovereignty (Part I, Chapter 2).

In the year under review, we were able to clearly demonstrate this in the field of video conferences

Successes are achieved (Part I Chapter 3).

3. For the further development of data protection in Hesse, the EU wins

Europeanization with decisions of the European Court of Justice (ECJ)

and the European Data Protection Board (EDPB) (Part I Chap. 1

and 4) as well as the juridification of data protection law with a light

Increase in fine notices (from 29 in 2021 to 113 per year

2022) and court cases (from 34 in 2021 to 35 in 2022)

(Part I Chapters 1 and 5) are becoming increasingly important. This requires stronger

Influencing European developments through dedicated

Participation in working groups of the EDSA and the expansion of the legal department

to deal with the additional process procedures.

4. While in the two previous years the corona pandemic was affecting the work of the

data protection supervision, this changed in 2022.

The corona pandemic ebbed away over the course of the year, new protective measures

took were no longer added, on the contrary, they gradually became

after dismantled. This also reduced the associated with them

privacy issues.

5. 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.

The number of processes to be processed in writing has stabilized at five

years after the GDPR came into effect at a very high level

Level. It fell slightly from 8,404 to 6,836. Through the increasing

Digitization will improve the quality of the processing of the processes

more demanding. Large digitization projects, e.g. B. the implementation

of the online access law or the Hessian school portal

not reflected in the statistics to the same extent as my authority

actually employ (Part I Chap. 19).

6. Form reports of data protection violations in accordance with Art. 33 GDPR

meanwhile a large part of the reactive activity of my supervisory

authority. New forms of cybercrime such as phishing and ransomware

somware attacks, exploitation of security vulnerabilities and

the publication of personal data on the dark web took place in

reporting period (from 2,016 in 2021 to 1,754 in the year

2022), but continued to cause new threats to those affected

Persons and those responsible (Part 1 Chap. 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 the data protection supervisory authority (Part I, Chapter 7).

7.

8. The schools and colleges were primarily characterized by strong

Developments towards more digitization of lessons and examinations,

teaching and learning. When using video con-

great progress has been made in reference systems (Part I, Chapter 3).

In the school sector, I accompanied the developments of the Hessian school

portals and other digitization projects (Part I, Chapter 8).

9. 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 several cases (Part I, Chapter 11).

10. The partial census 2022 was intensively accompanied by me and

controlled. Apart from minor negligence, there weren't any serious ones

Identify data breaches (Part I, Chapter 9).

X

core items

11. With the police, the State Office for the Protection of the Constitution and several

Public prosecutors did not find any serious

violations of data protection regulations. critical

I have comments on the planned amendment of the HSOG in the legislature

practice procedures and the legal basis for a comprehensive

Evaluation of all police data collections in a constitutional

Complaints before the Federal Constitutional Court

(Part I Ch. 6).

12. With regard to internet use, I had to deal with many violations through profile

Education with the help of cookies, through the business models of Social

Media and determine through advertising measures (Part I Chap. 12).

13. In the private sector I had to answer many detailed questions

Data processing at banks, credit agencies, tax consultants and

pursue different companies (Part I Chap. 14).

14. In the first half of 2022, there were still some dates in the healthcare sector

to pursue data protection violations in the context of the corona pandemic. Stronger

However, problems of digitization had to be worked on, such as for

patient file, for uploading medical images or for electronic

Provision of information (Part I, Chapter 15).

15. A key issue during the reporting period was support for the

Research through privacy. In this area, solutions were too

find that enable research projects in the general interest,

but at the same time trust through convincing data protection measures

of the patients (Part I Chap. 16).

16. Although freedom of information in Hesse is still only in the state

administration and a few municipalities and counties, I had as

Freedom of Information Officer many interesting questions in the year under review

on freedom of information and supported many citizens

and citizens in enforcing their claims. Also involved

I am involved in the legal and political development of freedom of information

and worked in the Conference of Freedom of Information Officers (IFK)

with (Part II). Complaints and consultations fell slightly from 123 to 110.

foreword

foreword

foreword

This is the 51st activity report on data protection and the 5th activity report

on the freedom of information of the Hessian Commissioner for Data Protection and

freedom of formation. With these reports I fulfill my information obligations

according to Art. 59 General Data Protection Regulation (GDPR) and §§ 15 Para. 3

and Section 89 (4) of the Hessian Data Protection and Freedom of Information Act

(HDSIG).

According to these regulations, as of December 31, I have

a report to the state parliament and state government each year

the result of my work in the areas of data protection and

freedom of information and privacy improvements

to stimulate I also have the activity report on data protection

the public, the European Commission and the European

to make the data protection committee accessible.

The activity reports have the function of presenting the current practice of data

protection and freedom of information in Hesse as well as the possibilities of

supervisory authority, on these in favor of fundamental rights and democracy

influence, describe and analyze.

The 51st activity report on data protection, covering developments in the year

2022, describes the conditions and results of the supervisory activity

in the field of data protection. Protects the fundamental right to data protection

the self-determination of the individual about his data and is at the same time

an objective of social order and development

Protection of democracy and the rule of law. The Data Protection Authority has

basic task, this individual and social self-

mood within the framework of the legal system towards the bodies that the

use the processing of personal data to increase their power,

defend and power imbalances caused by data processing

arise to balance.

However, this task is becoming increasingly difficult and creates new challenges.

requirements for the Hessian data protection supervisory authority. The digitization of everyone

areas of society leads to more intensive processing of personal

Genetic data and the business models of global corporations make it difficult

Enforcement of data protection, because they are often subject to data protection supervision

revoke. The penetration of information technology into everyday life

human actions and leads to an "explosion" of personal data.

Nevertheless, the Hessian data protection supervisory authority succeeded, even in the year

2022 to enforce data protection in many places and in many procedures.

For the exercise of fundamental rights and participation in democratic

In a digital society, political decision-making is next to data protection

access to public information is of particular importance. This

Freedom of information has only been enshrined in law in Hesse since 2018. Her

practical claim and fulfillment has yet to be established in Hesse

develop. Access to information is regulated in the Information Act

State administration planned, but only for the municipalities and districts,

if they apply the right to access information for their public

public bodies have expressly stipulated by statute. have this

so far only a few municipalities and districts have decided. Here will be in

further discussions on the advantages and disadvantages of a

information claim to be kept. For me, further development

and enforcement of information access to public bodies

important task.

Prof. Dr. Alexander Rossnagel

XIV

I

First part

51. Activity report on data protection

51. 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 Hessen in the year 5 since the date of application of the basic data protection

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

legal framework for the practice of data protection are overwhelmed

the. Many controversial issues have now been clarified, others are still in

the discussion, new questions are added. These concern before

especially complex challenges of large digitization projects in all

areas of society. The Europeanization of data protection, however

cooperation between the supervisory authorities in Germany is also progressing

progress and are increasingly changing the tasks and options for action

the data protection supervisory authority.

corona pandemic

In the two previous years, the corona pandemic shaped the work of the

data protection supervision very strong - both through constantly new content

Challenges (see 50th Activity Report, Chapter 2) as well as through their

Effects on the working mode of the supervisory authority (see 50.

performance report, chap. 1). This changed in 2022. The corona pandemic

ebbed away over the course of the year, and no new protective measures were taken

on the contrary, they were gradually dismantled. With that reduced

also the privacy issues associated with them. Such were

to a large extent only to be processed in the first half of the year. examples

Were the data processing within the framework of test procedures (Section 15.4)

and the postal delivery of COVID vaccination certificates (see Chapter 15.6). In

to the same extent, the measures within the authorities to

Maintain workability of the supervisory authority, gradually

be withdrawn. The pandemic mode of work in the office

gave way to work according to the new service agreement on mobile working.

According to this, the employees can do their work up to three days a week

Perform work in the home office or in other suitable places.

With this service agreement, the supervisory authority has the good experience

ments with mobile working from the pandemic period to the normality of the

transferred to working life. The ebbing of the pandemic also allowed

to carry out external supervisory activities on site again.

In the reporting period, however, the task of data protection

unlawful conditions that prevailed at the beginning of the corona pandemic and during

of the first lockdown in spring 2020 to cope with the then

Emergency situation had to be tolerated, again to the data protection law

adapt to requirements. This made a lot of demands on the supervisory authority.

But she could - especially when using video conferencing systems

temen – support those responsible to make decisive progress

achieve (see Chapter 3).

digitization projects

Digitization is advancing in all areas of society. This

leads to major digitization projects in business and administration

mostly set up on digital platforms and with the help of which own applications

development. For them it is important that data protection law

requirements are taken into account from the start. For this it is advisable

the professional competence of the supervisory authority in the form of advice

to claim something. while e.g. B. the corona pandemic above all many

has caused small-scale problems of everyday life, which in the

Processing of the individual case was to be pursued, digitization projects

data protection supervision faces more complex challenges: here it goes

about changing the Terms to reflect privacy requirements

realize. This is often no longer technically and economically possible if

in digitization projects, data protection is only taken into account retrospectively

becomes. If the conception is already completed, applications are already pro-

grammed, the available funds spent, the system introduced and

the work organization changed, the fulfillment of data protection law

Requirements are often very expensive, extremely time-consuming or even non-existent

possible. The supervisory authority must therefore try to intervene at an early stage

and to recognize the problems for data protection and - preferably with the

stakeholders together – to be solved by designing the systems.

This problem increases when the digitization projects on platforms

ment of international corporations that operate technical systems

and pursue business models that are compatible with data protection

demands are incompatible. The problem here is that the operators

About such platforms are mostly based in Ireland, so I do not

I am directly responsible for ensuring that you behave in accordance with data protection regulations

to stop Since they usually operate their platforms via a cloud as a contract

offer workers are for the data protection-compliant use of the platforms

responsible for those responsible in Hesse who use them. Therefore I am

forced to encourage them to behave in accordance with data protection regulations - and

not the platform providers, who are actually responsible for the data protection violations of their

platform use are causal. However, those responsible are

responsible for the technical systems they use. So it must be the goal

be to get those responsible in Hesse to close technical systems

use that enable them to comply with data protection requirements

(see Chapter 2 on digital sovereignty).

Jurisprudence of the European Court of Justice

National data protection law and the activities of the supervisory authorities

are increasingly being influenced by the case law of the European Union

Court of Justice (ECJ). He now has some important decisions

on data protection and the interpretation of the DS-GVO and by them

existing disputes resolved. But every decision is focused

on the subject of their decision and yet also always contains information about it

pointing remarks. This leaves behind the decisions

many new issues that are being debated and the legal uncertainty for

responsible and supervisory authorities (see 50th activity report,

Cape. 1).

In the reporting year, the decision of September 20, 2022 (C-

793 and C-794/19, ZD 2022, 666) on data retention in Germany

Significant (see Roßnagel for more detail, data retention - what else is possible

and what not?, ZD 2022, 650 ff.). In its judgment, the ECJ in

accordance with its meanwhile established (for data retention

protection directive ECJ of April 8, 2014, C-288/12, MMR 2014, 412; to

the regulations in Sweden and Great Britain ECJ of 21 December

2016, C-203 and 698/15, ZD 2017, 124; to the regulations in France,

Belgium and Great Britain ECJ of October 6, 2020, C-511/18 et al., ZD

2021, 520; on the regulations in Estonia ECJ of March 2, 2021, C-746/18,

ZD 2021, 517 and on the regulations in Ireland ECJ of April 5, 2022,

C-140/20, ZD 2022, 677) and further case law (on the

data storage in Bulgaria ECJ of November 17, 2022, C-350/21)

the permanent obligation of providers of electronic communications services
according to §§ 113a ff. TKG 2015, the traffic and location data of almost all
to store participants without cause and across the board, as a union
rated unlawfully. This decision is for further legislation
and for the interpretation of existing regulations in the field of internal affairs
Security is paramount.
Regulations requiring general and indiscriminate retention
of traffic and location data, record the electronic
Communications of almost the entire population, without any differentiation,
Restriction or exception based on the objective pursued. you concern
thus also "persons for whom there is no indication that
their behavior in even an indirect or remote connection
with the aim of combating serious crime", and

set “in particular no connection between the data whose
Retention is intended, and a threat to the public
safety ahead". They limit data retention “neither to
the dates of a period and/or a geographic area and/or
a group of people who are in any way involved in a serious crime
Could be implicated, nor on persons whose retained
Data contribute to the fight against serious crime for other reasons
could" (ECJ, ZD 2022, 666 para. 66.).
Even the obligations of the Member States to safeguard the basic
Rights from Art. 3, 4 and 7 GRCh cannot be “so serious

justify interventions” (ECJ, ZD 2022, 666 para. 123). Even if they do

Aim to fight serious crime and serious threats

to prevent public safety, they "exceed the limits of the

absolutely necessary" and cannot be "as in a democratic society

be considered justified by society". Traffic and location data

must therefore “not be the subject of a systematic and continuous

storage” (ECJ, ZD 2022, 666 para. 74.). Even one for the common good

serving objective - such as the fight against child pornography - "can,

essential as it may be, necessity in and of itself

a measure of general and indiscriminate data retention

storage of traffic and location data ... not justify" (ECJ, ZD

2022, 666 para. 123f.).

These statements exclude any classic data retention

out of. However, they also accept the Commission's proposal that operators

to commit to tronic communication, without cause, across the board, without

Exception and unlimited electronic communication thereafter

investigate whether references to child pornography are included, and for this

also to decrypt encrypted communications, as incompatible with

appear in Union law.

For the ECJ, however, the security obligations and the security

interests of the Member States are not ignored. you justify

depending on the threat to security and the severity of the encroachment on fundamental rights

limited to what is absolutely necessary, regulated by law and

encroachments on fundamental rights from Art. 7, 8 secured against abuse

and 11 CRCh. So he lets z. B. (for further exceptions see Roßnagel, ZD

2022, 650, 653 ff.) very narrow exceptions for the storage of IP address

sen zu: For the ECJ it is crucial that in the case of a criminal offense on the Internet

and especially in the case of child pornography, the IP address is the only one

A clue can be used to determine the identity of the perpetrator. Due to the

Severity of the encroachment on fundamental rights may only be used to protect the “national

security" or to "fight serious crime and prevention

serious threats to public safety”. "Besides, may

the duration of storage is absolute in relation to the objective pursued

Do not exceed what is necessary. Finally, such a measure must

strict conditions and guarantees regarding the evaluation of these

Data, in particular in the form of tracking, in relation to the on-

line communications and activities of those affected" (ECJ,

ZD 2022, 666, para. 102). The storage of IP addresses could therefore

exclusively for the source of the communication in strict compliance with

proportionality and if the respective measure is absolutely necessary

be justifiable under Union law.

European legislative initiatives

2022 was a year of European legislative initiatives on digitization

can deeply affect data protection, even if it is not their topic

is. The five key initiatives are as follows:

– The Digital Market Act (DMA) of September 14, 2022 (EU OJ L 265

of October 12, 2022) is in force as an EU regulation on November 2, 2022

Has entered into force and is applicable in the Member States from 2 May 2023. You

regulates important aspects of the European digital economy and should do so

protect the functioning of a fair digital single market. For this reason

does it contain special requirements for central platform services that

as gatekeepers through their monopoly power on large collections

based on personal data, endanger the market economy and

Treat traders and consumers unfairly.

- The Digital Services Act (DSA) of 19 October 2022 (EU OJ L 277 dated

27 October 2022, 1) is as EU Regulation (EU) 2022/2065 on a

Internal market for digital services and amending Directive 2000/31/

EC came into force on November 16, 2022 and applies in the member states

in parts from November 16, 2022, otherwise from February 17, 2024.

It updates the EU legal framework for electronic commerce

traffic, regulates new requirements for digital services and sets

Due diligence for providers of brokerage services, in particular

Online platforms such as social media and marketplaces.

– The EU Commission has drafted the Artificial Intelligence Act (AIA).

of 21 April 2021 (COM(2021) 206 final). The Legislative

drive to this EU regulation has come a long way. she will

the offer and use of IT systems for artificial intelligence

to regulate the development of an internal market for legally compliant,

Facilitate safe and trustworthy AI applications. She

prohibits certain systems with unacceptable risks and requires by

high-risk systems require a high level of transparency, risk provisioning and con-

formity ratings.

– The Data Governance Act (DGA) of May 30, 2022 (EU OJ L 152 of

June 3, 2022, 1) is effective as of June 24, 2022 as EU Regulation (EU) 2022/868 in
Entered into force and applicable in the Member States from 24 September 2023.
It organizes the infrastructure of a future data economy by
Data provision by public authorities, a data market with data
intermediaries and data altruism through data donations to trustees.
– The Data Act (DA) is based on a draft regulation of the EU Com-
mission of 23 February 2022 (COM(2022) 68 final) and is currently being
negotiated in the legislative process. She will make demands on the
contain European data economy and obligations to disclose
regulate data and rights to access and use of data.
All these adopted and future regulations always affect
data protection, because the broad concept of personal data many
which includes data whose handling it regulates. They all determine
men that the GDPR also applies to personal data in their
respective area of application applies. But they also regulate the conditions
the transfer, publication and use of this data and have
thus influence on the implementation conditions of the regulations in the
GDPR. This applies above all to the requirements for the admissibility of data transfer
processing, the rights of the persons concerned and the obligations of the
responsible. This gives rise to many legal questions that neither
from the GDPR will still be answered by the new regulations.
Data protection supervision is also affected by these regulations. This
Regulations stipulate that the supervision of the processing of personal
personal data from the independent data protection supervisory authorities
remains. However, they establish for their respective specific objectives
other supervisory regimes, each with their own supervisory authorities, whose

Competences are separated from those of the data protection supervisory authorities
Need to become. In addition, all these supervisory authorities together
work. This competition and cooperation also creates many
Future challenges faced by data protection regulators
need to adjust.

All of these new regulations encourage the use of personal data
ten. In a special way, this is the goal of the DGA and the DA, the one
want to initiate and promote the internal data market. pursued for this purpose
the EU Commission has set itself the goal of initiating 13 European data rooms. For
she already has the first data room, one for health data

8th New tasks and framework conditions

Regulation for a “European Health Data Space” in the
introduced the legislative process. Many national laws
should have promote the use of personal data – how
such as the legislative initiatives provided for in the coalition agreement for a
Research Data Act and a Health Data Utilization Act. As new
Challenges of data protection supervision arise from a variety of questions, such as
the objectives of the comprehensive use of data and what is required
can reconcile data protection. The data protection goals
of earmarking and data minimization seem at first glance
to oppose a widespread use of data. The con-
The primary goals are probably technology design that leads to anonymization
of personal data or a data analysis at the source
of the data enables or the personal data with special
technical and organizational guarantees (see e.g. Chapter 16.1). The one with it

related questions of the conception and implementation of such technical systems

Data protection-compliant data use occupied the supervisory authorities in

to a large extent during the reporting period.

European cooperation

Not only the Union legislation and the case law of the ECJ, but

Also the requirements of the DS-GVO for union-wide cooperation

Supervisory authorities are leading to ever-increasing Europeanization

of data protection law (see also 50th activity report, Chapter 1).

On the one hand, the supervisory authorities work in the European data protection

Committee (EDPB) together. In the form of recommendations,

Guidelines and opinions in abstract terms, such as regulations in the GDPR

are to be understood in practice enforcement and how between the supervisory authorities

arising disputes are to be decided. With that he contributes decisively

contribute to legal certainty in data protection law in the Union. Also he can in

contentious issues overruling the national supervisory authority and to

instruct specific actions (see Chapter 4.2). 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.

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

the GDPR envisages close cross-border cooperation

of the supervisory authorities in the Member States. Touches a supervisory

if several Member States proceed, the supervisory authorities should decide

agree on the necessary measures. If no agreement is reached

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

This cooperation between the supervisory

authorities proves to be difficult and time-consuming above all because
it lacks the necessary cultural basis. All Member States have
different data protection traditions and different understandings
se from data protection supervision. Therefore must between the supervisory authorities
very often about different understandings of terms, enforcement practices and
Objectives in the implementation of the law are negotiated. to be added
the language problems and the cumbersome procedures of cooperation.
Overall, the GDPR sets a culture change of cooperation in all
Member States that it cannot guarantee itself. Since but in
these collaborative processes will decide who influences
the future understanding of data protection in the European Union,
intensive participation is necessary (see Chapter 4.1). Nevertheless, it is often frustrating
struggling to watch helplessly as 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 GDPR has new legal options for those affected
Persons and the supervisory authorities created. These are fundamental
to be welcomed, but lead to stronger juridification of the supervisory
task. On the one hand, according to Art. 77 DS-GVO, every data subject has this
Right to lodge a complaint with a supervisory authority if you believe
that the processing of their personal data against

violates the regulation. Isn't she dealing with her complaint?

consent, it can be submitted to the competent administrative

court filed a lawsuit against the legally binding conclusion of the complaint

de-proceedings by the supervisory authority. Strengthen both rights

the protection of fundamental rights because they help individual enforcement of rights

and individual self-determination against powerful data processors

can support. The complaints are for the supervisors too

helpful means of gaining insight into data protection practice.

On the other hand, the GDPR has the supervisory authorities in Art. 58 GDPR

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,

increasingly characterizes the nature of the task and character

the activities of the supervisory authority. These become more formal and

more. They are increasingly shaped by questions of procedural rights

File management, the burden of proof, the evidence and procedural tactics

considerations. Impartial advice and assistance against

about the controller and the data subjects, which very quickly

can become a legal opponent are becoming more difficult.

The number of complaints, which is leveling off at a high level, leads to
the resources of the supervisory authority to the dilemma that the
supervisory authority can only cope with the increasing workload
when it uses means of work rationalization. However, this can
bring about peace among those who have lodged a complaint, and
to an increase in lawsuits against the supervisory authority. This in turn
increase the workload and jeopardize the regulator's reputation
as a trustee of the fundamental rights of the data subjects.
Through the juridification of the supervisory activity, the jurisprudence of
national courts have an increasing importance for data protection (see
Cape. 5.1 and 5.2) without being specialized in data protection issues.
This can be a uniform application of the GDPR in the European
make the Union more difficult (see 50th activity report, Chapter 1). So it's content
to be welcomed when a court like the Administrative Court of Wiesbaden
does not decide disputed questions of interpretation itself, but submits them to the ECJ
final clarification. In the reporting period, the administrative
Wiesbaden court in six proceedings, a wide range of legal issues before the ECJ
submitted. Since I thereby become one of the parties involved in the ECJ proceedings
was, I had to hire a law firm and the opinions
before the ECJ together with the lawyers in complex work.
Participation in a procedure was also intensive in the reporting period
before the Federal Constitutional Court, whose hearing on 20
December 2022 took place. With a constitutional complaint turned
several citizens to the court because they are in the potential
Processing of your data by the analysis software hessenData of the hessi-
national police saw a violation of their fundamental rights. In her opinion

was the enabling norm for this data use in § 25a Hessian

Law for Safety and Order (HSOG) unconstitutional (see Chapter 6.1).

For this procedure, too, the work on my brief was

complex and the preparations for the oral hearing extensive.

Cooperation with the supervisory authorities in Germany

Another important framework for exercising supervisory

responsibilities is the increasing need for oversight

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

German data protection supervisory structure. The coordination that takes place

nation is necessary on the one hand because within the Union only in Germany

the data protection supervisory authority is organized on a federal basis and Germany in

EDSA has only one vote. The German supervisory authorities must

therefore agree on one opinion for the decision-making process in the EDPB.

On the other hand, there is an understanding within Germany on the issues

necessary, which concern facts that are not only important for a federal

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

regularly the case and again and again in many areas of the federal, state and

cooperation or in transnational cooperation. In the

most data protection issues is therefore a nationwide enforcement of

data protection law required. The supervisory authorities of the

Federal and state governments as part of the conference of independent data

data protection supervisory authorities of the federal and state governments (DSK).

closer together. This requires more and more coordination within the framework

of the conference, in the technical working groups of the conference and in a

increasing number of task forces to temporary joint

Tasks.

Representatives of my authority work in all 25 working groups and in the

most of the task forces of the DSK. I chair the working groups

"Organization and Structure" and "Science and Research"

such as co-chairing the “credit agencies” working group and the task force

“Research Data”. The working groups meet at least twice a year

and hold several meetings in sub-working groups. The Task Forces

deal with urgent or cross-working group issues

and meet significantly more often.

Third, supervisors need common concepts and strategies

evolve to assert themselves against strong data processors

can. Only if they appear together and share their positions

fight through, they have chances to advance data protection in Germany

bring to. The most important decisions are therefore made in the committees of the

DSK. Accordingly, the importance of

of participation in these committees and is thus increasingly changing the

Work tasks of the employees in the supervisory authority.

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

Founded the "DSK 2.0" working group, which emphasizes the obligation of cooperation

New tasks and framework conditions

increase and increase the perception of a uniform task fulfillment

should improve. In addition to its biannual two-day conferences, the

DSK meanwhile additionally hold at least three one-day interim conferences

through. In addition, in 2021 she has set up a weekly jour fixe

to talk to each other via video conference, even on everyday issues

to inform and vote. Furthermore, she has hers in 2022

Rules of Procedure - under my direction - further developed to the effect that

that it can make binding majority decisions. Without on the

being dependent on unanimity for a decision, it can now easily

ter achieve a uniform application of data protection law. To the

At the end of the reporting period, the DSK had to increase its effectiveness

Bureau created, in which the previous chairman, the next year

Chair and the two representatives of Germany in the EDPB the current

support chairmen. Further measures to improve and strengthen

Cooperation in the DSK will follow.

2. Digital sovereignty and data protection

Digital sovereignty and data protection

The normative commitment of the European Union, the fundamental right

on privacy and protection of personal data in accordance with Art. 7

and 8 Charter of Fundamental Rights (GRCh) can only be fulfilled

if the tools used for the digitization of social relations

IT systems ensure this protection and do not counteract it.

Only if the person responsible for protection is able to provide this protection

to ensure his data processing, these fundamental rights

be implemented.

At the latest the political events of 2022 around Putin

Attack on Ukraine showed the importance of dependencies

to reduce and in certain areas to a high degree of independence

true. Germany and Europe can look to global relationships, global

Communication and global economic exchange not renounce and

don't want that either. However, this must not lead to them being due

of dependencies give up the pursuit of their own goals and values or

even make oneself open to blackmail. This also applies to digitization. Therefore

is in the areas of digitization where the limitation of

dependencies seems sensible and feasible, "digital sovereignty" a

important political goal.

Digital sovereignty as a political goal

For example, the data strategy of the EU is pursuing an explicit distinction from the USA

and China the goal in the digitization of the economy and administration in

Europe "to find our own European way by

exchange and channel the broad use of data while maintaining high

Maintain data protection, security and ethics standards" (EU Commission,

A European Data Strategy, 19 February 2021, COM(2020) 66 final,

p. 4). Also the white paper of the EU Commission on artificial intelligence

Calls on the EU to "act as one and on a European basis

Value their own way to promote the development and use of

KI (to) define" (EU Commission, White Paper on Artificial Intelligence –

A European approach to excellence and trust, 19 February

2020, COM(2020) 65 final, p. 1). In Germany, the federal government wants

with its data strategy "a contribution to Europe's digital sovereignty

achieve" (Federal Government, An innovation strategy for social

Progress and Sustainable Growth, January 27, 2021, p. 9). Also for

the coalition agreement of November 27, 2021 is digital sovereignty

central goal (SPD, Bündnis90/Die Grünen, FDP, dare more progress,

Coalition Agreement, 2021, pp. 15-20). In its research framework program for

The federal government calls IT security “technological sovereignty” 32 times

as a research goal (BMBF, digital.safe.sovereign, research framework

program of the federal government on IT security, 2021; BMBF, sovereign.digital.

networked, research program communication systems, 2021). strategic

There are also commitments to digital sovereignty as a political goal

in the strategy of the IT planning council (IT planning council, strategy for strengthening

of digital sovereignty for IT in public administration, 2021) and

in many strategy papers of the federal states (see e.g. for Hessen Hessische

Minister for Digital Strategy and Development, Digital Hessen – where

Future is at home, 2021, p. 9; ibid., KI made in Hessen, 2022, p. 45, 50).

All these political strategies in Europe and Germany see digital

Sovereignty as an expression and obligation of their normative orientation.

For them, however, digital sovereignty is not just a question of security,

of competitiveness and innovation, the development of

democracy, political self-determination and responsibility

for the social consequences of digitization, but also a question of

rule of law and the protection of fundamental rights. They refer to the political

cal objectives of digitization – in conscious distinction to

Strategies in North America or Asia, for example – on their value orientation. She

see the protection of personality, as it is about in the basic rights

Privacy and data protection in Art. 7 and 8 GRCh is expressed as

a crucial point of orientation and the GDPR as an important one

normative basis for the digitization of society.

About technological sovereignty as a prerequisite and consequence of digital

to achieve self-assertion are - as the statement of the Hessian

state government on my 50th activity report (LT-Drs.

20/9709, p. 2) – coordinated efforts in many policy areas such as the

Economic and industrial, competitive, research, educational, legal

and digital policy in the EU and in Germany. they require

In addition to data protection aspects, there are also those relating to technology (hardware and

software), digital competence, IT security and cost control

to consider. In this activity report, however, I will focus on the

restrict the data protection aspect of digital sovereignty (see

also Roßnagel, Digital Sovereignty in Data Protection Law, MultiMedia and

Law (MMR) 2023, 64 ff).

16

Digital sovereignty and data protection

Digital self-assertion for fundamental rights and democracy

The EU guarantees everyone on its territory fundamental rights and

Data protection. She also stands by this guarantee if the data

of these people in third countries or in the Union through technical systems and

Service providers from third countries are processed. Therefore, data protection

law and the protection of fundamental rights also apply and are enforced

if the manufacturers of IT systems and service providers from third countries

assume lower requirements because lower ones in their home country

Protection requirements apply. If the Union wants to keep its promise of protection,

must she insist that anyone entering the European market

meets the protection requirements applicable here. A lower level of protection

in other countries may not be transferred to the Union. From this

The selection of techniques or services must not be justified either

lead to a (de facto) lower level of protection.

At the same time, the enforcement of fundamental rights and data protection is

a measure towards manufacturers and suppliers from third countries

Self-assertion of European democracy: the rules of co-

Bens in the digital world are to be determined democratically. You may not

private market power of global corporations and the private ones set by them

be left to legal systems. In the event of a conflict, they are democratic

enforce established rules.

enforcement of data protection law

My task, which is mentioned first in Art. 57 letter a DS-GVO,

Enforcing data protection law is carried out by technical systems, service

ments, contractors and business models that are not

comply with data protection requirements. Three examples should

show that those responsible for providing such services, technology systems

or contractors, usually not able to

are to comply with their accountability according to Art. 5 Para. 2 DS-GVO.

They would have to demonstrate that they meet all data protection requirements

fulfill, but cannot do this because they do not have the necessary information

information or the services they have used

do not meet these:

– Facebook should serve as an example for social media. Meta offers under

“Pages” responsible for its “Facebook” service, which these

may use to disclose information to the public.

In doing so, Meta collects personal data about the inquirers,

without informing the responsible users what data it

for which purposes it is collected and how the data is processed,

without demonstrating that such tracking and profiling is permissible, and

without an agreement on joint responsibility with the users

to complete the wording. They also transmit personal data

without sufficient additional protective measures in the USA (see more details

Cape. 12.2). Other social media offers from USA and China offer

similar fundamental problems.

– Microsoft will only offer its Office programs as MS 365 in the future

as cloud-based services in a contractual relationship. development

pursuant to its “Privacy Addendum” dated September 15, 2022

for MS 365, Microsoft wants to provide these services without the

To enable those responsible to give him as a contractor more precise

to issue instructions without providing information about what data is in

which way processed for own purposes, without any changes

To inform subcontractors with sufficient precision and without data

to delete or return according to the specifications of the DS-GVO (see also

Federal Government, Bundestag printed paper 20/4852, p. 44). Microsoft also wants to

Requirement that US authorities be allowed to release data

and process data without adequate protective measures in the USA

ten. Cause other cloud-based services from third countries

comparable problems.

– As an example of problems with US providers of video con-

reference systems (VKS) should serve Webex from Cisco. Cisco offers Webex

not in on-premise operation, but operates the VKS itself. This

prevents those responsible from being able to check for themselves whether and to where

personal data leaks. In the operation of the VKS Cisco processes

personal data in the US without sufficient additional

protective measures. Although the content data in video conferences

encrypted, but the keys are not held by the person responsible

generated, but distributed by Cisco, so access from US-American

Canan authorities on the keys is not excluded (see 50.

Activity report, chap. 4.1). Other VKS also have similar problems

from third countries.

All of these providers have their main office in Ireland. I am for them

not responsible. But I have to enforce data protection in Hesse, too

if those responsible in Hesse use their offers. As far as responsibility

literally dependent on such technology systems or services

are, I often face the dilemma, either they by orders

to hinder them in their business activity or the fulfillment of their duties or

to refrain from enforcing data protection requirements (see 50.

Activity report, chap. 3.1). This dilemma can only be avoided if

dependence on the products of such suppliers is overcome.

18

Digital sovereignty and data protection

The providers of social media, cloud, video conferencing and other

Technology systems from third countries are often unwilling to deny their systems

adapt to data protection requirements. From a practical point of view

are therefore technical and organizational alternatives to those from the
Hardware, software, services and platforms offered in third countries
necessary in order to enable data protection-compliant data processing.
In many cases, therefore, digital sovereignty is a prerequisite
Enforcement of data protection requirements.
The necessary conditions for the required variety of technical and
organizational alternatives in as many areas of processing as possible
promoting personal data is primarily a political task.
Fulfilling them requires action in many policy areas. But also
the controller must contribute by using its IT systems that
selects the services it uses and its contractors in such a way
that he can fulfill his data protection obligations.

responsibility of those responsible

The responsibility of the person responsible for the conditions to
To be able to meet data protection requirements, the ECJ has
made clear in his judgment of July 16, 2020 (C-311/18 – Schrems II).
and using the example of the transfer of personal data to an insecure
third country (in this case the USA) (see 50th activity report,
Cape. 3.1). The court's remarks make it clear that the selection
of the technical systems and services by the person responsible under
his responsibility falls. The EDPB has this in its “Recommendations on
Measures to supplement transmission tools to ensure the
level of protection under Union law for personal data” (recommended
1/2020, Version 2 of June 18, 2021) convincingly worked out.
The person responsible must check before putting personal data in a
Third country transmits whether the data enjoys comparable protection there

like in the EU. If this is not the case, he must take additional protective

take action or stop the data transmission.

Legal definition of digital sovereignty

The responsibility formulated by the ECJ for international data traffic

However, we cannot speak for the protection of the fundamental right to data protection

only apply to the questions to be decided in the Schrems II judgment,

but goes beyond the obligations in international data transfer

to extend all data protection obligations. The person in charge has

fundamentally the obligation by the selection of the technology used by him

and the services used its data protection law

to secure the need for action. He must not put himself in constraints

or dependencies that make it impossible for him to fulfill his responsibility

to live up to the word. Conversely, he cannot claim that

certain data protection obligations do not apply to him because

because of the techniques he uses and the

services is not able to fulfill them. Digital sovereignty

in a constitutional sense with regard to data protection law,

if the controller uses technology systems or services that

enable him to meet data protection requirements.

This definition is not aimed at protectionist preference for European ones

technical systems and services, but solely on enforcement

Union and Member State law.

Digital sovereignty is not a legal concept, it does not exist as such

the GDPR. However, it is a term used for a wide range of data protection

liche problems, which are based on the same structural problem, one

called solution. This structural problem is that

Providers from third countries offer technical systems or services

and pursue business models that comply with the legal requirements in the

EU and Germany are not compatible. You want contrary to legal

Regulations stick to it and also use it because of their market power

often through. In data protection law, however, those responsible are also responsible for

Obliged to comply with data protection regulations if they

Use technology systems and services. You need engineering systems

and choose services with which they are able, which concern them

to meet requirements. This applies not only to the question of the international

Data transfers to third countries, but also for

- the data protection system required by Art. 25 Para. 1 DS-GVO

tem design that meets the requirements for data processing

is to ensure that the data protection principles according to Art. 5 DS-GVO

adheres to This obligation also includes the hardware and

Select software systems, platforms and services in such a way

that data protection-compliant data processing is possible. The re-

lativation of this obligation by taking into account the state of the art

and the implementation costs in Art. 25 Para. 1 DS-GVO means that

the person responsible between suitable technical alternatives that

correspond to the state of the art, but not that

he does not have to meet data protection requirements if he

finds no technical alternative for its processing purpose

can be used in accordance with data protection.

- the data protection-friendly required by Art. 25 Para. 2 DS-GVO
presets. For its purposes, it must use IT systems, services and
Select platforms that give him e.g. B. enable any tracking
connect and comply with all the requirements of § 25 TTDSG (see these
DSK, Telemedia Orientation Guide, December 2021).
- the assumption of joint responsibility required by Art. 26 DS-GVO
wording. The person responsible may IT cooperation with common
accept responsibility only if the partners have agreed
26 Para. 1 S. 2 DS-GVO, in which they stipulate
how data protection-compliant data processing takes place, who does which
Obligations fulfilled, in particular towards data subjects
and who meets which information obligations. This continues
provided that the partner provides the person responsible with the necessary information
information given.
- the inclusion of processors required by Art. 28 GDPR,
who ensure that they meet all the requirements of data protection law
(can). With regard to the obligations of companies from the
third country to make data from the EEA accessible to their authorities
chen, responsible contractors may transfer personal data
only entrust if these are not foreign government agencies
are obliged to oppose the release of this data by them
Art. 48 DS-GVO, or additional protective measures
prevent disclosure of personal data. You may
only transfer data to contractors if they ensure

that they do not use the data for their own purposes.

– the adequate data security required by Art. 32 GDPR. This

can be at risk when companies from a third country are affected by the

domestic authorities can be obliged to cooperate with them

to work and for this purpose in their software or hardware

build in vulnerabilities that allow these authorities to

invade IT systems of controllers from the EEA.

Whether the manufacturer, service provider, platform operator or processor

from a third country meets these requirements, the person responsible must

review before signing a contract. Can't or doesn't want to fulfill them

the person responsible may not entrust him with any personal data.

New transatlantic developments

The discussion about digital sovereignty is being driven by the efforts of a

new "Trans-Atlantic Data Privacy Framework" between the USA and the

EU revives. On October 7, 2022, the US President issued an Executive Order

on Enhancing Safeguards for United States Signals Intelligence Activities”

(EO), which is intended to enable the Commission to

who submit to the framework, an appropriate level of data protection

to acknowledge. This new legal construction could solve the problem

of data transmission to the USA will be placed on a new basis.

For the other aspects of digital sovereignty presented above

however, nothing changes as a result of the framework and its recognition.

The EO attempts to address the two central criticisms of the ECJ in its original

part of the repeal of the previous decision on "Privacy Shield" (16.

July 2020, C-311/18 – Schrems II): the disproportionate ones

Data Processing Powers of Intelligence Services and the Lack of

Legal protection for Europeans.

According to the EO, the security

Security and educational interests of the USA continue to have top priority. The

However, measures of "signal intelligence" should be aimed at the surveillance objective

be tailored and "not disproportionately impact privacy and civil liber-

ties". Mass surveillance of Internet traffic (like after the programs

PRISM and upstream) should still be possible. The usage

However, the data collected in this way should be limited insofar as the monitoring

target can be achieved through tailored monitoring measures

can (sec. 2 c). However, the EO expressly states that in no

way "any signals intelligence collection technique" limited by

previous regulations are permitted (Sec. 2 e). The powers under Section

702 of the Foreign Intelligence Surveillance Act (FISA), which the ECJ considered not

declared compatible with European fundamental rights continue to apply.

With regard to legal protection, the EO also sees a two-stage process

Grievance mechanism in place if a non-US person submits an opinion

is that the surveillance measures of the US intelligence services against

violate applicable US law. In the first stage, one of the US

recognized organization (e.g. a European data protection supervisory authority)

for an individual, a review by a Civil Liberties Protection

Officer (CLPO) in the Office of the Director of National Intelligence.

In the second stage, a “Data Protection Review Court” can be held with the Attorney

General review the case. As a result of the respective decision in the

first and in the second stage, the appellant must be neither confirmed

nor can it be denied that he was monitored. Rather, he may

regardless of the result of the investigation - only be informed

that the investigation either does not identify a violation of fundamental rights

could or has led to an appropriate remedy (Sec. 3 c, d).

22

Digital sovereignty and data protection

Based on the EO and other US Framework regulations

On December 13, 2022, the Commission issued a draft

identification decision submitted. In the subsequent process

according to Art. 45 Para. 3 DS-GVO the Commission according to Art. 70 Para. 1

Letter s DS-GVO to the EDSA including all necessary documents

of correspondence with the US government and the EDPB

has issued an opinion on the appropriateness of what is required in the USA

assess protection levels. After that, the Member States are in the frame

the comitology procedure according to Art. 45 (3) and 93 (2) GDPR

as well as Art. 5 VO (EU) 182/2011. The Commission issues the

Adequacy decision as an implementing act pursuant to Art. 291

TFEU according to Art. 5 Para. 3 of Regulation (EU) 182/2011 not if the weighted

majority in committee gives a negative opinion on the draft.

In this case, you have to renegotiate and the new result again

Submit to committee or refrain from further prosecution of the draft.

After this "timetable" is with a binding decision on the

Adequacy of the level of data protection in the specific area of the

USA, in which the agreement is to apply, is not expected until mid-2023.

However, the Commission does not want the decision to come into force until the

USA implemented all relevant regulations in the intended manner

have. This should be the case in autumn 2023 at the earliest.

If the Commission's adequacy decision has come into force, this

according to Art. 288 (4) TFEU binding effect for the supervisory authorities,

to the extent that it is determined that the USA has an adequate level of protection

ensure and the transfer of personal data as a result

is approved (ECJ of July 16, 2020, C-311/18).

The ECJ will have to rule on this decision. He will him on

Standard of Art. 7, 8 and 47 GRCh as well as Art. 44 sentence 2 and Art. 45 para. 2

GDPR and its Schrems II decision. Decisive

will be whether the US has “effective and enforceable rights” and “effective

administrative and judicial remedies for data subjects”

from Europe, an effective independent supervisory authority also in

Establish reference to the US security authorities, which also compared to the

US intelligence services can issue binding orders (EDSA,

Statement 1/2022 v. April 6, 2022), and the monitoring practice (“Application

of the legislation”) to proportionate measures.

For this purpose, the ECJ will e.g. have to decide the following questions:

Is an Executive Order of the President a sufficient legal basis

location? Does it have more than an internal effect? Provides sufficient

Legal certainty if at any time – e.g. B. by a Republican

Presidents – can be changed or revoked? Is it enough from the

Requiring intelligence services to increase their surveillance "proportionately".

practice if the legal bases for mass surveillance

be explicitly retained? Does the proportionality also apply to the

automated mass data collection or only for the subsequent

use of the data? Is "proportionality" in the sense of "absolutely necessary"

meant, as the ECJ demands in many decisions (see Chapter 1)?

Or does the EO mean "proportionality" in a US understanding of the

sense adapted to surveillance objectives? Is the “Data Protection Review

Court” is actually an independent tribunal or effectively just a committee

within US government agencies? Is his review the decision

Civil Liberties Protection Officer appointments are a real court case

in the sense of Art. 47 GRCh? To what extent is this limited to

a complaint and the denial of an opportunity to bring an action, the lack of it

Public and the pre-punched decision tenor limited?

Once these and other questions have been answered, it cannot be ruled out that

that the ECJ the adequacy decision of the Commission – after

Safe Harbor and Privacy Shield – a third time. In any case

there is a great deal of legal uncertainty until the decision of the ECJ.

This avoids anyone who makes his investments and other decisions

Digital projects in the long term to the previous case law of the ECJ and

oriented towards the goal of digital sovereignty – especially a decision

of the ECJ, which would confirm the adequacy decision, only one

of many reasons for digital sovereignty, namely the international ones

Transfer of personal data, apply only to the USA

would. Even if only international data transfer is taken into account, it is closed

take into account that questions of digital sovereignty have arisen in recent years

very focused on the USA for years. Similar questions arise

but also in many other third countries to which data is transferred.

Implementation of digital sovereignty in Hesse

It therefore makes sense to stick to the goal of digital sovereignty in the long term

to orient. For this reason, the EU Commission, the Federal

government and the state governments this goal in their initially mentioned

Digitization strategies for public administration included. In

Implementation of these strategies have been around at the federal level by now

launched many projects - such as the Sovereign Management Cloud,

the Sovereign Workplace, the Sovereign Tech Fund and the Center for

Digital sovereignty (ZenDiS) of public administration. thereby has

the federal government “made decisions and implemented measures at an early stage,

the use of these products (= MS 365) for the federal government in principle

make dispensable". The federal government is already doing almost nothing today

completely based on the use of MS 365 (BT-Drs. 20/4852, p. 44f.)

Hessen is involved in the projects for the sovereign administration cloud and for the

Confident workplace involved. Possibility to switch between IT solutions

In the context of digital sovereignty, e.g. in the HessenSW 2025 project

Developed. A successful example of the implementation of digital sovereignty is

also the Hessen school portal (see Chapter 8.2). Particular advances could

in Hesse with the participation of my authority in the field of video conferencing

be achieved. Through technology selection and technology design, data

protection-compliant system solutions are developed and put to use:

– In the Hessian state administration, approx. 70,000 employees have been working since

the end of the reporting period from the Hessian Ministry for Digital

Strategy and development as "Hessen Connect 2.0" a system solution

rolled out step by step. It is operated by T-Systems and integrates

uses the open source solution "Matrix/Elements" as a chat system and

as VKS the open source solution "Jitsi" (see Chapter 3.4).

- Since autumn 2022, Hessian schools have been able to participate in the Open as VKS

Use the BigBlueButton source solution. The system is powered by this

Hessian company German Edge Cloud operated. The Hessian

Ministry of Education offers it for safety reasons integrated in the school

portal for all 2,000 state and private schools in Hessen free of charge

at. The school authorities and schools can now legally secure a VKS for

Use school purposes (see Chapter 3.2).

– For the Hessian universities, moderated by the Hessian

Ministry of Science and Art to be clarified which VKS

be used lawfully through appropriate technology design

can. In the future, the German Open Sour

ce system BigBlueButton, but also a secure technical design of the

US VKS Zoom. This VKS is named after the “Hessian

Model" with the involvement of a Hessian service provider (specifically

case Connect4Video) used in-house. This is also in the

invoice interposed and controls external access to system

me The university uses an identity management system to prevent

Pseudonymization, VPN and encryption of the content data that

personal data reach Zoom (see Chapter 3.3).

– The consideration of data protection and digital sovereignty

also occurs in the "Data protection" module in the IT design principle BaSiS (Bar-

free IT, information security and data protection) to express that

the Minister for Digital Strategy and Development together with the

25

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

State Commissioner for Accessible IT, the Hessian Ministry of

Inside and for the sport and me. This design principle

should in future be the nationwide IT standard for project implementation in all

Phases of the digitization projects of the state of Hesse - already

in the conception, the tender and the selection - binding

be applied.

These examples show that there are already areas of digitization

in which the fundamental problem of implementation is due to digital sovereignty

of data protection through technology systems and services that

not based on the legal requirements of the GRCh and the DS-GVO,

can be resolved or at least mitigated.

26

video conferencing systems

3. Video Conferencing Systems

video conferencing systems

Above all, the digitization push caused by the corona pandemic has

increased use of video conferencing systems (VKS).

In the process, the pressure to find quick solutions resulted in many systems

selected that do not meet the data protection requirements.

This is especially true for many widely used VKS made by US American

niche providers. These transfer personal data to

the USA and thereby cause a loss for the persons concerned

in exercising their fundamental rights (see 50th activity report, Chapter 3.1).
However, they also often violate other data protection regulations because they
pursue a business model that is incompatible with the GDPR (see 50.
performance report, chap. 4.1). VKS are therefore a technology area in which digital
Sovereignty supports and facilitates the implementation of data protection law
(see Chapter 2). In this area, however, digital sovereignty is already possible
lich. In this chapter, three successful digitization projects are presented
the reporting period presented to enable from the unlawful
switch usage from VKS to legitimately usable systems. They are
an example of how technological dependency can be avoided,
satisfies the general need for technology use and solves problems
data protection compliant system design can be achieved. They show,
that it was right, in the last two years on systemic consulting and
Design of digitization projects instead of intervention in individual cases
and to give those responsible the necessary information for this transformation
to give some time. Before these projects are presented, however
to clarify which data protection requirements apply to VKS.

3.1

Classification of video conferencing systems under data protection law

With regard to the data protection classification of VKS, there are large
Uncertainty. On the one hand, this is due to the fact that video conferences only started in
the Corona pandemic have taken a rapid rise and therefore
only recently been widely used. On the other hand, only before
recently changed the legal basis: valid since December 1, 2021
new rules in the Telecommunications Act (TKG) and the new telecom
nikation Telemedia Data Protection Act (TTDSG). To the uncertainty of how

the offer and use of video conferences under data protection law

are to be classified, I asked this question for the data protection conference

is looking for (see Roßnagel for more detail, Video conferences as telecommunications services?,

New Legal Weekly (NJW) 2023, Issue 7, 400 ff.).

27

Telecommunications?

Video conferencing services are telecommunications services if they

meet the definition for that term. Then they would have to according to § 3 No. 61

TKG "generally provided for a fee via telecommunications networks

Services” must be one of the three categories of services specified in the regulation

are equivalent to. Only classification as an “interpersonal tele-

communication service". According to Section 3 No. 24 TKG, this is “an ordinary

service provided for a fee which has a direct interpersonal and

interactive exchange of information via telecommunications networks between

available to a finite number of people. In addition, the

be determined by the organizers of the video conference.

As a rule, video conferences offer a direct interpersonal and

interactive visual and auditory information exchange between the

participants. The signals of the video conferences are transmitted via telecommunications

cation networks. To be able to participate in a video conference,

you have to be invited. Therefore, only takes part in a video conference

a finite number of people.

As an interpersonal communication service, the service must use the direct

“Enable” interpersonal and interactive exchange of information. Not

the individual video conference is an interpersonal communication service,

but the service that enables the organizer of a video conference to

to hold such a conference by audio and video transmission. To

This video conferencing service also includes the performance features

Ways to book the conference room, invite to the conference,

control the conference, add participants later,

mer, form subgroups, operate a chat channel,

to operate microphones and cameras centrally, to record the conference,

granting rights (e.g. uploading documents) and similar functions

to perceive. Such video conferencing services are z. B.Zoom, Cisco

Webex, Microsoft Teams, Google Meet, GoToMeeting, Skype, BigBlueButton,

Jitsi, alfaview and many more.

Whether they are to be regarded as interpersonal telecommunication services,

according to § 3 No. 24 and 61 TKG still depends on whether it is "usual" or

"usually for a fee". So the definition starts

mutual performance relationship between "market participants". The

Video conferencing service must be an independent service included in

exists that the provider gives the customer the opportunity to

hold conferences with participants designated by him. This

The performance ratio thus affects the operator of a video conferencing service

as a provider and the organizer of video conferences as a customer.

28

video conferencing systems

In contrast, however, there is no interpersonal telecommunications

service if the requester uses the service to hold a video conference

to perform. As far as the organizer participants in the video conference

invites to communicate with them out of their own interest, he offers

They don't have the option of even conferencing with all the ancillary functions

to host. In this case, the participants do not pay any fee.

But if not a video conferencing service in a market for such services

is offered and related to such a service no reciprocal

If there is a performance relationship, the conceptual prerequisites are missing

the offer of an interpersonal telecommunications service according to § 3

No. 24 TKG and a telecommunications service according to Section 3 No. 61 TKG. Who

Using video conferencing services to host video conferences is not

Provider of video conferencing services and therefore not an addressee of the TKG.

Rather, such a user is comparable to a person who

telephone connection to telephone other people. This person

is also not considered to be a provider of a telecommunications service.

The consequences of this differentiation can be practical in the following

examples are illustrated. Providers of video conferencing services such as

Zoom, Cisco, Microsoft, Google, Telekom and others bid on a worldwide

market, for a fee, to use their services to videoconfer

to perform limits. This possibility is z. B. from administrative

den, universities, schools, medical practices, law offices, associations and

companies and they pay a fee for it. These providers

thus provide interpersonal telecommunications services and are subject to

the TKG.

If, on the other hand, the universities use their paid video conferencing service

zen to communicate with their members and thus to their tasks

to comply with teaching and research, then they do not offer them any service

a market for which participants pay a fee. Nor

A market for video conferencing services is emerging when schools ask their teachers

as well as pupils to participate in virtual lessons

enable hours. Comparable administrative authorities require none

Charges if they hold internal meetings between administrative

teten or consultation hours with citizens via video conference

carry out. Lawyers' offices and medical practices can also use their acquired

Use video conferencing licenses to communicate with clients or patients

to communicate and also from a distance their consulting services

to provide. You do not charge for participation in the video conference

fee. Likewise, clubs that hold their board meeting in the form of a

Conduct video conference, no charge for by the board members

Participation. After all, companies demand from their employees

no charge if you use video conferences for internal meetings.

The same applies when they are using video conferencing with their partners, clients

or suppliers keep in touch. In all these cases, the organizers open

of video conferencing does not have a market where they can

perform, offer and provide for a fee, but

use these. They are therefore not providers of telecommunications services.

It should therefore be noted that the providers of video conferencing services

provide a telecommunications service for a fee and therefore under

the telecommunications law, i.e. the TKG and §§ 1 to 18 and 27 bis

30 TTDSG fall. Opposite are those that use video conferencing services

only use the GDPR and, in addition, the relevant regulations

Telemedia in §§ 1 and 2, 19 to 26 and 28 TTDSG to apply.

Telecommunications secrecy or informational self-determination?

This result also fits with the regulations of telecommunications secrecy

in the TTDSG. According to Section 3 (2) TTDSG, “providers of publicly accessible

chen telecommunications services” and “providers of all or part

Commercially offered telecommunications services” to safeguard the

committed to telecommunications secrecy. After that, telecommunications secrecy applies

for providers of video conferencing services such as Zoom, Cisco, Microsoft and others.

They offer public telecommunications services to anyone in the market

and they provide them permanently to third parties, i.e. in a business-like manner.

On the other hand, associations, universities, schools, administrative authorities, medical

practices and legal offices as well as companies that want to

conducting video conferences for own purposes to communicate with

Members, employees and contractual partners use, not to protect

committed to telecommunications secrecy because they do not

provide services for a fee. However, you must have the fundamental right to

protect the informational self-determination of all data subjects. With

this fundamental right are in practice largely the same level of protection

and the same requirements as with telecommunications secrecy.

data protection supervision

The concept of telecommunications also decides on the responsible

supervisory authority. According to § 29 paragraph 1 TTDSG the Federal Commissioner for the

Data protection and freedom of information the competent supervisory authority,

as far as telecommunications services are concerned, i.e. for providers of

Video conferencing services in the telecommunications market such as e.g. Zoom, Cisco,

Microsoft et al. Not him, but the data protection officers of the countries

video conferencing systems

are, however, responsible for the use of these video conferencing services,

if they are used for their own purposes usually or usually free of charge

Communication with members, relatives, employees, customers,

Apply or suppliers are used.

Application of the GDPR

Insofar as providers of video conferencing services use publicly accessible telecom

provide communication services in public communication networks, subject

do not follow the GDPR, but the ePrivacy Directive according to Art. 95 GDPR

line 2002/58/EG and the national regulations for their implementation. For

the regulations in the TKG and the data protection regulations therefore apply

in §§ 1 to 18 and 27 to 30 TTDSG. This supremacy of the ePrivacy Directive

however, only applies insofar as the ePrivacy Directive addresses the respective legal issues

specifically regulates. The ePrivacy Directive contains such regulations, e.g. B.

not for order processing or for international transfer per-

sun-related data. Therefore also apply to telecommunications services

Art. 28 and 44 et seq. GDPR.

On the other hand, the use of video conferencing services as a whole is covered

the GDPR. The organizer is responsible within the meaning of Art. 4 No. 7

DS-GVO and must ensure according to Art. 5 Para. 2 and 24 DS-GVO that

all principles of data processing according to Art. 5 Para. 1 DS-GVO and all

other requirements of the GDPR are complied with. In addition, the

relevant regulations for telemedia services in §§ 19 to 26 TTDSG.

Whether the provider of video conferencing services is to be considered a contractor

depends on whether he enables his contractual partner to be responsible

literally to host his own video conferences, or whether he himself

Video conference for the participants as a paid service

he brings. As far as he supports the person responsible, own video conferencing

to organize zen, this must him as a contractor according to Art. 28 Para. 1

Select DS-GVO carefully. It must offer sufficient guarantees that

that he takes appropriate technical and organizational measures

means that the processing is in line with the requirements of the GDPR

takes place and ensures the protection of the rights of the data subject.

The controller must work with the video conferencing service provider

conclude an order contract according to Art. 28 Para. 3 DS-GVO. In this

the conditions for compliance with the GDPR must be agreed. In the

operation, the person responsible must ensure that the contractor

mers to check again and again whether they comply with these data protection requirements

also actually complies, and according to Art. 29 DS-GVO accordingly

point. These specifications pose special problems when the provider

the video conferencing services of the jurisdiction of an unsafe third country

(see Chapter 2).

3.2

Video conferencing system for all Hessian schools

More than two and a half years after the first school closures and the

Introduction of distance learning, which schools often combine with the

Use of legally dubious VKS was accomplished, the Hessian has

Ministry of Education (HKM) an efficient as well as data protection

formal solution implemented. The Hessian schools can now open

resort to a digital tool that goes beyond the pedagogical

area could also be applied.

There was an urgent need for action by the Ministry

In my 50th activity report (Section 5.2) I had, among other things, described that

that HKM approached me in March 2020. It asked for the first

ten school closures and in view of the urgency of the matter

as well as because of the lack of knowledge of many school administrations around the

Data processing when using VKS is pragmatically oriented

Release of the applications offered on the market. The security

development of the school's education and upbringing paired with a

previously unknown situation surrounding the pandemic development

then persuaded me to accept a temporary toleration until August 2020 for almost everyone

VKS systems for the pedagogical area based on Art. 6

Paragraph 1 subparagraph 1 letter d and e GDPR.

The data protection-compliant, nationwide offer I demanded for the

Schools, which the HKM should make available, could

cannot be realized at the beginning of the 2020/21 school year. That's why this happened

Ministry approached me again and asked for the extension of the

formation phase. I had complied with this request and the toleration until

Extended July 31, 2021. However, there were conditions attached to the extension

linked (for details see https://datenschutz.hessen.de/datenschutz/

universities-schools-and-archives/hbdi-tolerates-temporary-use-of-

video conferencing systems in schools).

Europe-wide tender is overturned by the court

In the spring of 2021, as part of a Europe-wide

th tender selected a provider that all 2,000 Hessian

Schools should be able to use a VKS. against the result

of the selection process, an inferior competitor went through

initiation of an award review procedure. First, the

Public procurement tribunal determined deficiencies in the tender and demanded

a re-tender. The HKM appealed against this to the OLG

Frankfurt a. The court confirmed the decision at the end of December

2021 the decision of the Public Procurement Chamber. The Ministry had to

initiate a new tendering process that replaces the original

set schedule obsolete. Also on the new situation I have

reacted with a lot of pragmatism. Although I have the tolerance for the use

non-compliant VKS not extended again, but within the framework

at my discretion, no repressive measures against schools

initiated, the z. B. the questionable, especially US American

Systems, continue to use (see also: https://datenschutz.hessen.de/datenschutz/

Universities-schools-and-archives/toleration-for-use-particularly-

us-applications-expiring).

A new VKS service provider will be appointed in early summer 2022

The second call for tenders from the ministry was ultimately

better sign. The choice fell on the German provider German Edge

Cloud (GEC), which is based in Eschborn near Frankfurt am Main. The

company is already responsible for the operation of the school portal Hessen (SPH)

responsible and provides a VKS with the open source web conferencing service

BigBlueButton (BBB) available.

In early autumn, integration into the country's school portal began, via

which the system i.a. is accessible for reasons of IT security. From

At the end of September 2022, the Hessian schools had the new offer

progressively and as needed. After agreement with me could

the schools initially continue to work with the existing VKS. With expiration

The time for use ended in the first half of the 2022/23 school year

of non-data protection compliant VKS. My employees were at

Still in the review phase at the end of the reporting period. Especially aspects

IT security, access and integration of the VKS application

into the SPH require further investigation. In addition, I still stood

Not all the required documentation is available. The previous

However, tests lead us to expect that the VKS will comply with the central data protection

meets legal requirements.

Handling of use requires a definition

Without a doubt, the procurement of the state-wide VKS for the schools

intended for the implementation of distance learning. That's about them

Corona pandemic beyond. Just think of bad weather events that

make it impossible for students to go to school. The short-term use

of the VKS is a tried and tested alternative to an impending cancellation of lessons.

But there are other possible uses. class or

School conferences or even parents' evenings could be

Such case also be carried out, insofar as it is related

outstanding data protection issues have been clarified. However

there is a need for more specific specifications with regard to use

Ministry on the issue of how far the scope of an educational

usage is enough. In addition, it will have to be discussed whether and in what form the

classic school administration will be able to use the digital instrument.

Added value under data protection law in the context of digital sovereignty

The introduction of a high-performance and data protection-compliant

I very much welcome VKS for all Hessian schools. Even if that

Process up to the selection of a provider and the concrete implementation

demanding and sometimes tedious, the effort has become mine

Worthwhile for everyone involved. So will the Hessian schools now

offered a system that is integrated into a protected IT infrastructure, the SPH,

is embedded. The implementation of data protection is

Development of the open source product BBB and hosting in a German

data center easier. A transfer of personal data in

a third country without the level of protection of the GDPR and access by third parties

this data is therefore without sufficient legal protection for the persons concerned

excluded. The specifications of the ECJ from the Schrems II judgment are

thus sufficiently implemented.

In addition, with the nationwide unique project, the aspect of

digital sovereignty into account. The realization of national like

European digital data processing projects under the protective umbrella

of the GDPR, an adequate Al-

alternative to the offers of the large, international corporations and

compliance with the required protection of fundamental rights is better than this up to now

guarantee.

3.3

"Hessian model" for video conferences in universities

In my 50th activity report (chapter 4.2) I reported which ones

Challenges of the corona pandemic for the Hessian universities

asked. The life of students and teachers has changed significantly

video conferencing systems

changes. Since then, VKS have been increasingly used to organize courses

to perform. When selecting the VKS, data protection was often not considered

placed in the foreground, but rather back to providers established on the market

seized, which promised a high level of comfort and a stable connection.

Among other things, the VKS Zoom is widespread at the universities. To however

also the aspects of data protection when using the VKS in the necessary

The universities and I have to observe the scope under moderation

of the Hessian Ministry for Science and Art (HMWK).

suitable solutions sought. Here, the University of Kassel with my

Support developed a "Hessian model" with which the VKS Zoom

Can be configured and operated by colleges without being opposed

violating the data protection requirements of the European Court of Justice.

The background is the decision of the European Court of Justice of July 16

2020 (so-called Schrems II judgment) (see detailed 50th activity report, Chapter 3.1).

According to this, personal data may only be transferred to the USA

to the extent that it is impossible for US authorities to access them

can. However, a US service provider cannot do that

guarantee, especially not if he - like the VKS service provider

Zoom – provides for the transfer of data to the USA. That's why I have it

Pandemic-related tolerance of such systems, which was pronounced in April 2020

ended on July 31, 2021 and subsequently the Hessian universities

requested that the use of VKS US providers privacy

fair or to switch to data protection-compliant systems.

At Hessian universities, the VKS Zoom can therefore only be used for

Lectures are used when the colleges are appropriate

Take steps to stop the outflow of personal data

in the USA and to limit access to them by US authorities

to avoid.

Requirements for a data protection compliant application

If the Hessian universities use this “Hessian

model" in the practical use of zoom, I evaluate the remaining

Risk for the participants in Zoom video conferences at the

existing options with the data protection regulations as

compatible. The requirements underlying the "Hessian model".

are described below.

1. Installation, configuration and operation by suitable processors

The university uses an intermediary processor

with headquarters and location of data processing in the EU or the EEA,

the one here shows the on-premise operation of the Zoom audio-video connectors

offers. The responsible university closes with one

operator an order processing contract in accordance with Art. 28 Para. 3 Sentence 1

DS-GVO and meets their respective due diligence obligations as for the

responsible for data protection. The processor closes

with the provider Zoom the standard contractual clauses of the EU Commission

in the currently valid version.

The contractor provides the responsible university with the VKS Zoom

available and is their direct billing partner. Through this

can transfer billing data to the provider Zoom

be minimized or made anonymous.

In particular, the processor uses such technical measures

circumstances that may be likely to pose a risk from accessing content

data by the provider Zoom itself becomes less likely

(e.g. through regular, process-controlled monitoring

to detect and prevent undesired connection establishment).

2. Pseudonymization, technical and organizational measures

Type and scope of personal data collected despite the operation

of the connectors by the processor continue to be transmitted to Zoom

are averaged (connection, telemetry and diagnostic data), are in

to the extent that it is due to technical and organizational measures

is possible, limited.

The responsible university manages the user identities for

Participation in video conferences in one operated locally

Identity Management (IDM). It restricts the transmission of personal

data drawn by the IDM to the provider Zoom to an extent

one that does not make a personal reference possible. This includes, among other things,

that the IDM excludes the transmission of real names to Zoom.

Organizational measures must be taken to ensure that this is not the case

e.g. force event managers to give clear names if

this z. B. an attendance check in the context of seminar formats

carry out.

This also includes the deactivation of functionalities,

which only through the transmission of personal data to the provider

zoom can be used. These include e.g. B. the recording and storage

arranging the conference in the cloud, using the chat function or the

Participation via browser.

3. End-to-End Encryption

The end-to-end encryption of the Zoom client must be protected by the

responsible must be activated. In doing so, the keys

video conferencing systems

created in the universities' Zoom client and not centrally by Zoom

distributed. The security of the underlying cryptographic procedures

is proven by an external certification.

4. Virtual Private Network (VPN)

The responsible university offers the university members a

VPN access that is suitable for the transmission of personally identifiable information

to block IP addresses from Zoom. She makes sure that one

VPN access by all interested participants for the

any application can be used. This includes in particular

the provision of sufficient technical capacities.

That a personal date of the host of an event

(Name of the event manager) is transmitted, however, cannot

be prevented. If a transmission of this date from the host

is not desired, he can switch to an alternative data protection compliant

Dodge VKS that the college offers.

5. Restriction on Use

The responsible university uses the VKS Zoom as part of the

implementation of courses. It basically closes

Use cases in which the processing of more sensitive, personal

related data takes place, e.g. B. for purposes of internal university self-regulation

administration, student interest groups, staff representatives

or for the implementation of application procedures. holds for this

the responsible university an alternative data protection compliant

VKS ready.

6. Sufficient information of the participants

Insofar as the security measures mentioned involve the participation of the

VKS require participants or give them a choice,

the university must inform the participants sufficiently

what measures they use to exercise their informational self-determination

can protect. This information must be both contiguous

easy to find as well as in the individual usage steps in the

Application of the VKS is offered to the extent required in each case

become.

Summary

In summary, it can be stated that the universities

intellectual property deficits of the US provider Zoom

guarantee the same and data protection-compliant operation of the VKS

can. With the “Hessian model” they therefore ensure that they

– a processor independent of Zoom based in the EU or

in the EEA, the video conferencing system on servers in the EU

or to operate and settle accounts with them in the EEA,

– end-to-end encryption of all content data is available

place,

– the outflow of participants' personal data to the USA

and prevent access to such data from the USA,

– limit the use of Zoom to courses,

– an alternative data protection-compliant VKS for other purposes or for

Offer teachers who do not want to work with Zoom

- the teachers and students about further, supporting

Measures to protect informational self-determination

inform in detail.

3.4

Video conference system in the Hessian state administration

In the reporting period, the Europe-wide tender for the

Construction and operation of a VKS and the subsequent additional services

division two major milestones on the way to a new and

data protection-compliant VKS for the Hessian state administration

become. I have been advising on this major project not just since the current

reference period. Also for the future I expect a continuation of the

successful cooperation with the Hessian Minister for Digital

Strategy and Development (HMinD).

background

Also in the state administration at the beginning of the corona pandemic

the search for suitable VKS data protection questions have been postponed for the time being.

I did this in the first year of the pandemic given the urgent

may be considered justifiable after a short-term provision of VKS.

At the same time, I expressed the forecast that the large-scale use of

VKS will not remain a short-term phenomenon and in many areas with

long-term use can be expected (50th activity report, Chapter 4.2).

It was therefore necessary to look for data protection-compliant alternatives.

The general conditions for the introduction of a new VKS have changed

changed since the beginning of the pandemic. Due to the large number of

which offers a situation has existed for some time in which responsi-

lich within the meaning of Art. 4 No. 7 DS-GVO have the option of setting up a VKS

video conferencing systems

to select, design and use that they have according to the DS-GVO

able to fulfill existing obligations. Those responsible are therefore in the

Location, in the area of VKS with a view to data protection digitally sovereign

to act. Accordingly, I have called on those responsible to

to use their digital sovereignty and set off towards one

to make VKS compliant with data protection law.

Depending on the purposes and the general conditions of use

of a VKS, it can be the conception, the implementation and the

management of a project of considerable size and duration. here is

it is essential that data protection requirements are met from the outset,

consistently and comprehensively considered and implemented. Straight

the early project phase is of particular importance here. Then

This is where trend-setting decisions are usually made

and thus the foundation for all further project phases as well as the application

of the VKS.

The advice offered by my authority

My authority supports public bodies in Hesse within the framework of

IT projects. The consulting services offered can affect this

different data protection issues and topics

in different project phases as well as strong in type and scope

vary. The specific design depends on the specifics of each

depending on the project and its need for advice. Despite advisory

With the support of my authority, the implementation remains subject to data protection law

Requirements Task of those responsible. The same applies in particular

Measures for decisions within the project as well as for the acceptance of

documents, milestones or other project results. It is therefore

imperative that on the project side there is sufficient data protection

che expertise is planned and made available. The advice of my

Authority does not replace this - especially since advice is always only within the framework of the

existing resources of my authority can be done.

The HessenConnect 2.0 project

The central VKS of the Hessian state administration HessenConnect 1.0

was introduced before the corona pandemic. during the pandemic

increased its importance for cooperation within and between

to the offices of the Hessian state administration in leaps and bounds. So was-

de the VKS in my authority, for example, only after the outbreak of the

Pandemic made available at every workplace. Within a very short time

time, it has subsequently become an indispensable part of communi-

communication portfolios of my employees.

It has long been clear that HessenConnect 1.0 will be replaced by a new

VKS needs to be replaced. The HMinD has yet to do this

initiated a multi-year project during the reporting period, which I am already involved in

was involved early on. Since then, employees of my

authority with a legal and technical focus on the Hessen-

Connect 2.0. As a result, I was already able to create the for

the specifications required under public procurement law

give due weight to data protection requirements.

With the tender, taking into account data protection regulations

From my point of view, a first major milestone has been reached.

It turned out that the integration of data protection in tender

procedure is a key success factor for subsequent project phases.

The explicit inclusion of data protection requirements

by no means a deterrent effect on potential suppliers. Much more

made a significant contribution to ensure that providers comply with the

ten of data protection law the necessary importance and this

considered accordingly in their offers.

With the completion of the tender and the award of the contract

a second major milestone was reached in the reporting period. Hesse-

Connect 2.0 should be based on an integrated and open source software

based solution (Matrix/Elements as messenger service and Jitsi as

VKS) are implemented and operated. I see a promising

de Basis for the follow-up phases already started in the reporting period

of the project.

The two milestones underline that those responsible at VKS and

Various alternatives that comply with data protection law are available.

You are therefore not forced to access problematic data protection law

resort to solutions. However, this requires that those responsible

che fulfill their role and fulfill the data protection regulations

Demand requirements explicitly and emphatically. Only on this basis

they can also exercise their digital sovereignty in terms of data protection law

actually use.

I expressly welcome the fact that the Hessian state administration is using its

has exhausted the possibilities to jointly develop a future-proof and data protection

to find a legally compliant VKS solution. The course of the project so far represents for

me a particularly positive example of a cooperative, solution-oriented approach

and successful cooperation within the framework of data protection law

Advice on IT projects by my authority.

video conferencing systems

outlook

In the future, the implementation started in the current reporting period

of the VKS HessenConnect 2.0. My employees

will also actively support the project in the next phases in an advisory capacity

Stand by and continue the successful cooperation so far, provided that

this is desired by the project managers.

I assume that the Hessian state government and in particular

the HMinD will continue their efforts unabated in order to

employees of the Hessian state administration at the end of the

Project a data protection compliant and data protection friendly VKS

to provide. In any case, with the milestones reached so far, there was one

promising basis for this.

4. Europe, International

Europe, International

The DS-GVO has led to a strong Europeanization of data protection law, however

also led to data protection enforcement. With the EDSA is a European

Data protection institution emerged, which is to be enforced in all Member States

through recommendations, guidelines and binding decisions

exerts influence. These decisions are made in sub-committees of the EDPB

prepared. At the same time, the GDPR requires intensive cooperation

between the supervisory authorities of the Member States, for all to one

considerable extra work. In the EDPB, in its sub-committees and in the

daily supervisory cooperation is decided as of

European data protection is to be understood and lived. Hence cooperation

of the German supervisory authorities in the European data protection association

essential (Section 4.1). That this cooperation makes it possible to exert influence

and even to correct the decisions of other regulators,

show two examples of methods for setting fines

Meta Ireland (Section 4.2).

4.1

Cooperation with other supervisory authorities in Europe and in Germany

With the entry into force of the GDPR, numerous innovations for the

cooperation between the supervisory authorities in Germany and Europe.

Art. 60 Para. 1 S. 1 DS-GVO obliges the European data protection
supervisory authorities, in cases of cross-border data processing
Strive to reach a consensus to cooperate closely. To the com-
to cope with the additional communication and organizational effort that
resulting from the intensification of cooperation, I have in 2019
set up the European and International Office, which acts as a link
between the Hessian data protection supervisory authority and various
offices outside of Hesse 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 (see also 47., 48.,
49th and 50th activity report, chap. 2.1, 3.2, 4.2.2 and 5). 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 establishment in the EU or the
EEA there, but the processing has a significant impact on data subjects
has or may have persons in more than one Member State.

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 the processor (Art. 56 Para. 1 DS-GVO)

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

responsible or the processor (Art. 56 Para. 6 DS-GVO). This

brings to a company the relief to look out for one and the same

Only deal with data processing with a supervisory authority

must. However, this means additional work for the supervisory authorities,

because the lead supervisory authority does not decide alone. Much more

In addition to the lead supervisory authority, all other

involved supervisory authorities in the decision-making process. "Affected"

("Concerned") are, according to Art. 4 No. 22 DS-GVO, all supervisory authorities in

whose territory the controller or the processor

is allowed, individually affected persons ("data subjects") their place of residence

have or to whom a complaint has been made.

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

with a cross-border connection, which in the European data protection

authorities are entered into as a first step in a procedure

according to Art. 56 DS-GVO to determine the responsible and affected

Regulatory authorities included in the IMI system. Here is the situation

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 me, because 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

Europe, International

to my respective specialist department, which then after thorough examination

of the facts contact the person responsible.

In the event that the lead for a complaint received by me,

Request or report according to Art. 33 DS-GVO at another European

supervisory authority, the Office for Europe and International

read them via the IMI system for processing to the responsible person

competent authority. To do this, the input and all other required

processing of necessary documents and relevant information

to be translated into English. As the supervisory authority concerned, I act in

participate in the decision-making process and remain in the so-called one-

Stop-Shop contact person for the submitter and

inform you 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 reach a consensus (Article 60 (1) GDPR). The lead

The supervisory authority examines the case in accordance with Art. 60 (3) sentence 2 GDPR and files it

the supervisory authorities concerned once the investigations have been completed

draft decision. Against this draft resolution, the affected

lodge an objection with the supervisory authorities pursuant to Art. 60 (4) GDPR.

In the event of irresolvable differences of opinion, the matter will be

EDPB in the consistency procedure according to Art. 63 DS-GVO for binding de-

submitted for divorce.

Case numbers and testing effort

The number of complaints, inquiries and

Art. 33 notifications declined in the reporting period and has returned to the

2019 level approximated. The number of legal proceedings

Term administrative assistance, on the other hand, continued to rise significantly in the reporting period.

Number 2019 Number 2020 Number 2021 Number 2022

633

European procedure

Art. 56 procedure

in total

Art. 56 procedure with

dismay

Art. 56 procedure with

leadership

Art. 61 procedure

(administrative assistance)

Table 1: European procedures

17

4

65

812

32

7

26

1419

47

16

92

645

11

2

155

45

During the reporting period, the Europe and International Office

a total of 645 Art. 56 procedures registered in the IMI system for a possible

whether they are affected or lead. In eleven of these proceedings

the European and International Office reported me as "affected",

subsequently dealt with the content of the matter and worked on the

decision making with. I have two methods of editing the

Complaint accepted as lead supervisory authority.

The decrease recorded in the year under review compared to the previous year

the Art. 56 procedure is explained i.a. in that meanwhile for a

Multitude of controllers and processors and a multitude

specific data processing constellations already have a case register (so-called

"Case Register") are created in IMI, on which new cases are built

can be set directly - for example as a new Art. 61 procedure - in IMI,

without a new Art. 56 procedure to clarify leadership and

concern is required. So the decline of the Art. 56 procedure goes

accompanied by an increase in Art. 61 proceedings. It is therefore to be expected

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

GMO will continue to increase in the future.

Approval of Binding Corporate Rules

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

There was another administrative procedure in the past reporting year

Main focus of the activities of the European and International Office in the

Review and approval of Binding Corporate Rules (German: binding

internal data protection regulations, in English: BCR) according to Art. 47 DS-GVO,

which - not least since the so-called Schrems II judgment of the ECJ of 16

July 2020 (Case C-311/18) and the invalidity of the EU-US Privacy Shield

– Growing as a transfer tool for data transfers to third countries

enjoy popularity.

BCR are complex contracts with measures to protect personal

personal data that a multinational corporation is committed to complying with

obliged to process personal data within the company

group in so-called "third countries" (i.e. countries outside the European

economic area), which in and of itself is not appropriate

provide a level of data protection.

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 the lead, as the so-called "BCR Lead", and coordinates

dines the procedure. One or two more regulators will be

supporting as a so-called "co-examiner". In addition, since the entry into force

of the GDPR and in departure from the previous so-called Mutual Recognition Ver-

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

established consistency mechanism to be included and opportunity

to review and comment on the BCR before the EDPB receives a

comment on this.

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

groups, I am very often involved in BCR approval processes as a spring

management within Germany or even Europe-wide as a BCR lead

in charge. In the year under review, I was in four BCR approval

responsible for the process as Europe-wide BCR Lead. Also have

I do the co-examination in five other procedures and in another six procedures

take over the inner-German leadership. Particularly gratifying

was that in the reporting period the approval process for the BCR for

Responsible persons (so-called Controller-BCR) of Fresenius SE & Co. KGaA and

Fresenius Kabi AG with a positive statement from the EDSA and mine

final approval decision could be completed.

Participation in committees 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 international transfers

Subgroup deals with international data transfers and all

common topics and questions that arise in this area. Next to the

Participation in regular subgroup meetings and BCR sessions

the European and International Office is involved in various draft

ing teams and task forces and reports together with colleagues

Colleagues from the LDA Bayern and the BfDI to the German supervisory authorities

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

of European and international data protection law. The feedbacks

I will then bring you from the German supervisory authorities as a country representative

re-entered the discussions at European level. This is how it works e.g. B.

influence on guidelines and recommendations to be adopted by the EDPB

take, 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 sends by e-mail,

but also electronically via the Confluence web platform and

to my responsible specialist department - be it for mere information and

Knowledge or, if necessary, further cause - be forwarded

must. This puts the specialist departments in a position to actively and

tend to be involved in the work at European level and e.g. B. through

Participation in ad hoc groups or early commenting on papers,

which are still in the draft stage, impact on the European

take the opinion-forming process.

Support of the DSK in questions of European data protection

Also at the national level, participation in working groups of the DSK

continued to support European data protection issues.

The staff unit will continue to take over the management of the nationwide work

working group organization and structure, which is responsible for the work of the DSK in important

organizational issues and concepts and processes

for better dovetailing of work at German and European level

developed. Another topic that the working group deals with intensively

busy, are questions arising from European cooperation after

Chapter VII of the GDPR, including the specific processing

of these procedures in the IMI system. In addition to organizing regular work

The European and International Office regularly has working group meetings here

monitor developments at national and European level

and evaluate to the colleagues of the other German

to report to supervisory authorities. In addition, the staff office

Europe and international affairs for me continue to attend the meetings of the

international data traffic working group, which deals with questions of cross-border

progressive data transmission in view.

48

Europe, International

4.2

Influencing the decisions of other supervisory authorities

In the reporting period, cooperation and coherence procedures were followed

Chapter VII DS-GVO a number of substantial measures and considerable

hefty fines against global IT corporations

I was able to influence by working in EDSA committees. example

Here are two legal proceedings against Meta Platforms Ireland Limited (short

hereinafter referred to as: Meta Ireland, formerly Facebook Ireland Limited),

in which the EEA supervisory authorities deal with key pillars of EU data

data protection law, namely with the lawfulness of the processing

Art. 6 DS-GVO and questions about the calculation of fines in the case of established

data protection violations.

Disclosure of children's data in Instagram

In a proceeding against Meta Ireland that the processing of personal

of data obtained from children through the Instagram service, the spring

the leading Irish data protection supervisory authority (Data Protection

Commission; short: DPC) after the intervention of the other EEA supervisory

hear a record fine of €405 million plus one

A series of further remedial measures imposed in accordance with Art. 58 (2) GDPR.

The fine imposed is the second highest fine

since the GDPR came into force.

The background to the measure was one ex officio by the DPC

study carried out by the Instagram service

Disclosure of Children's Personal Information. The social network
had allowed users between the ages of 13 and 17 to use the Instagram
to use a business account. With a change from a private to a
Business account was the contact information of the children concerned
(email addresses and phone numbers) publicly available. Also were
also children's personal Instagram accounts by default
Default "public".
As part of the investigation, Meta Ireland was heard and supported the
Publish the contact information of children using the feature
Use Instagram Business account, alternatively on Art. 6 as a legal basis
Paragraph 1 subparagraph 1 letter b DS-GVO ("contract performance") or Article 6 paragraph 1
Subsection 1 letter f GDPR (“legitimate interest”). The DPC had this
Practice initially not objected to and the other affected supervisory
authorities in the EEA (including me) submitted a draft decision in which they
found that Instagram relied on the legal bases mentioned for the
processing of the children's contact information.

A number of those affected appealed against this draft decision by the DPC
Supervisory authorities – including some German supervisory authorities –
objection. Not only the conclusions of the
DPC regarding the legal basis for processing, but also
the determination of the amount of the fine that was deemed inadequate. For
the German supervisory authorities received the objection from the Hamburg authorities
Coordinated by the Commissioner for Data Protection and Freedom of Information (HmbBfDI),

according to § 19 paragraph 2 BDSG due to a branch of Meta in Ham-

burg is in charge within Germany.

The DPC did not agree with the objections of the EEA regulators

and instead initiated a dispute pursuant to Art. 65 Para. 1 Letter a DS-GVO

settlement procedure at the EDPB.

The EDPB then issued a binding order on September 2, 2022

concluded that there was no reason for the DPC to believe that

processing by Instagram is necessary for the performance of a contract

and Meta Ireland consequently did not rely on Article 6(1)(1)(b).

GDPR as the legal basis for this processing. Also in

Reference to legitimate interest as an alternative legal basis for the

processing, the EDPB found that the publication of the email ad

ress or telephone numbers of children meet the requirements of Article 6

Paragraph 1 subparagraph 1 letter f DS-GVO not fulfilled. Processing was neither

necessary, nor, if deemed necessary, was it through

overriding legitimate interests of Meta are covered. The EDPB came

concluded that Meta Ireland used the personal data of

children had unlawfully processed without any legal basis and rejected the

DPC to amend the draft resolution and find therein a violation of

Art. 6 Para. 1 DS-GVO to determine. In addition, the EDPB instructed the DPC to

to check the planned fine in accordance with Art. 83 (1) and (2) GDPR and

to impose an effective, proportionate and dissuasive fine.

The DPC agrees with the determination of a data protection violation and the

now imposed fine of 405 million euros.

Insufficient consent in Facebook and Instagram

In a further proceeding against Meta Ireland in connection with the

The DPC has also provided the Facebook and Instagram services

after the intervention of the EEA supervisory authorities and a decision by the EDPB in

Dispute settlement procedure – fines of 210 million euros for

Violations of the GDPR in connection with the Facebook service

and 180 million euros for violations related to the

Instagram service imposed.

50

Europe, International

The reason for the proceedings was a complaint from a data subject

Austria (in relation to Facebook) and a complaint from a data subject

Person from Belgium (in relation to Instagram) already on May 25, 2018,

i.e. H. on the day the GDPR came into force.

In the run-up to May 25, 2018 and the GDPR coming into effect, Meta Ire-

land the terms of service for its Facebook and Instagram services

changed. Users have been informed that the legal basis

ge, on which both services the processing of personal data from

supported users, have changed. So far, Meta Ireland had opted for the

Processing of personal data of users of the Facebook and

Instagram services based on their consent. Now Meta Ireland tried

opt for most processing in connection with the Facebook

and Instagram services (including behavioral advertising)

on the legal basis of "performance of contract" from Article 6 Paragraph 1 Subparagraph 1

letter b DS-GVO. Wanted existing (and new) users

after the entry into force of the GDPR (continued) access to the services of

Facebook and Instagram have asked for their consent

with the updated Terms of Use.

Meta Ireland, at a hearing, took the view that by adopting

of the updated Terms of Use is a contract between Meta Ireland

and the users and the processing of user data in

in connection with the provision of their Facebook and Instagram services

is necessary for the performance of this contract, including the provision

of personalized services and behavioral advertising,

so that this processing according to Art. 6 Para. 1 Subparagraph 1 Letter b DS-

GMOs are lawful.

The complainants, however, argued that Meta Ireland

contrary to their assertion, still rely on consent as a legal

basis for the processing of user data and enforce it.

By allowing Meta Ireland to make access to its services conditional on the consent of the

make the user dependent on the updated terms of use,

effectively compel them to stop the processing of their personal data

Data for behavioral advertising and other personalized services

agree. This constitutes a violation of the GDPR.

After extensive investigations, the DPC submitted the affected EEA

hear (including me) two draft resolutions in which the DPC a

made a series of findings against Meta Ireland. In particular, the

DPC finds that Meta Ireland violated the transparency obligations

Article 5(1)(a) GDPR and Article 12 and Article 13(1)(c).

have violated the GDPR by not sufficiently informing the users

were formed, which processing of their personal data

carried out for what purpose and on what legal basis

became. The “forced

However, the DPC did not see consent as given, since Meta Ireland

does not rely on the consent of the user as the lawful basis for the

processing of their personal data and represented the

Position that Meta Ireland lawfully relies on the legal basis of the

Fulfillment of contract for the processing of personal user data

in connection with the provision of its personalized services

(including personalized advertising).

The supervisory authorities concerned agreed after examining the submitted

Draft resolutions to the DPC in determining the violation of

transparency obligations, but considered that in response to the Ver-

stoss the amount of the proposed fine too low. Also made

many supervisory authorities affected - including German supervisory authorities

Lead by the HmbBfDI - objections in relation to the legal basis

of the performance of the contract, which DPC had assessed as lawful.

The provision of behavioral advertising in connection

with the Facebook and Instagram services is not responsible for the fulfillment

significant obligations of Meta towards the users of Facebook

and Instagram required.

In these proceedings, too, the DPC joined the parties concerned

objections raised by the supervisory authorities and, since no con-

sens, both procedures to the EDPB for a decision

in the dispute settlement procedure according to Art. 65 Para. 1 Letter a DS-GVO.

In its binding resolution of December 5, 2022, the

EDSA many of those put forward by the regulators concerned

appeals and acknowledged Meta Ireland's breach of trans

parental obligations. The EDPB also instructed the DPC to pay the fine

to increase. Also in the question of the legal basis, the EDPB followed the

objections and concluded that Meta Ireland in principle

does not lawfully refer to the legal basis of "performance of the contract" for the

processing of personal data for the purpose of behavioral

can invoke advertising.

The DPC agrees with the EDSA decision with the determination that has now been made

data protection violations and the increase in fines.

5. Court and Fine Proceedings

court and fine proceedings

The GDPR leads to an increasing juridification of supervisory activities

(see Chapter 1). The number of court cases and fines is increasing

and this development is also having a greater impact on work

the supervisory authority. In the processing of complaints is always also

to be expected that the complainant or the person responsible

after the outcome of the proceedings for the opposing party of the supervisory authority

becomes. This leads to a formalization of supervisory activities and an additional

increasing need to document procedural steps - with the

corresponding additional work in the complaints procedure.

5.1

In court and on the high seas – evolution of court procedures in 2022

The trend of the last reporting years continued in 2022. The number

of court cases continued to increase significantly. Many procedures went in

the second instance, so that I am also repeatedly involved in appeals

drive in front of the Hessian Administrative Court (VGH) in Kassel.

Constitutional complaints against § 25a of the

Hessian Law on Public Safety and Order (HSOG)

and the analysis system hessenDATA before the Federal Constitutional Court

(BVerfG). Opinions were in two other proceedings before the BVerfG

and in three proceedings before the ECJ.

A total of 35 new court cases were recorded in the year under review.

These are distributed among various instances and courts. 18 of them are

at the Administrative Court (VG) Wiesbaden, ten proceedings at the Hessian

Administrative Court (VGH), three preliminary proceedings before the ECJ and

three proceedings before the Federal Constitutional Court in which I have to submit an opinion

was prompted.

court proceedings

Complaints pursuant to Art. 78 Para. 1 GDPR

Complaints pursuant to Art. 78 (2) GDPR

ECJ preliminary ruling procedure

Proceedings before the VGH in the 2nd instance

Proceedings before the BVerfG

expedited procedure

In total

Number

13

4

3

11

3

1

35

The court proceedings from the year under review have not yet been

se procedures from the previous reporting years. That was the number

a total of 45 pending court cases at the end of the year under review.

The thematic focus of the first-instance proceedings was above all

in employee data protection, in the rights of those affected (information according to

Art. 15 DS-GVO, correction according to Art. 16 DS-GVO, deletion of data

according to Art. 17 DS-GVO), in actions for failure to act according to Art. 78 Para. 2 DS-GVO,

in the data transmission to the processor, in the disclosure

of data to a financial service provider, in data processing

using private mobile devices within the framework of a contractual relationship and in the

video surveillance.

A look at the administrative litigation reveals that in the case of

Dismissals in the first instance, more often than last year, the

resolution of the appeal was requested.

failure to act

Actions for failure to act are a focal point of the lawsuits

according to Art. 78 Para. 2 Alt. 2 DS-GVO. Because of the very high number of

Complaints in individual specialist departments repeatedly led to delays

struggled in the processing of individual complaints. My employees

and employees showed a high level of commitment to coping with the

Complaints. In individual cases, however, the three-month period could be considered

of Art. 78 Para. 2 Alt. 2 DS-GVO are not complied with. Basically

there is an obligation to inform about the status of the procedure in three months

time intervals. If this information is not given, the process can continue

three months the right to sue for failure to act in court

be invoked. The three-month period is a rigid period that is not

can be shortened or lengthened. This also prevents me from

me, citing factual considerations, such as B. high complexity

court and fine proceedings

of the case to refer to an extension of the period. It's strong of the

Staffing levels in certain departments depend on how high the risk of

action for failure to act. In Art. 52 Para. 4 DS-GVO is also for this reason

expressly stipulates that each Member State must ensure that each

supervisory authority, among other things, with the human resources

is equipped with what they need to carry out their duties and powers

to be able to I hope to be here with the new posts assigned in 2023

to see an improvement.

I would like to single out two cases from the administrative court proceedings.

GPS tracking in the logistics industry

In the case of an order according to Art. 58 Para. 2 DS-GVO due to illegal

Use of a software tool for collecting and storing location

data of the vehicles of a logistics company were the orders

confirmed by my authority by the VG Wiesbaden and the rescission

Complaint dismissed (judgment of January 17, 2022, Az.: 6 K 1164/21.WI). The

The plaintiff had installed GPS systems in vehicles in its company fleet.
The software used made it possible to determine the live location
of vehicles via GPS and the storage of location data and measured
the fuel consumption. The plaintiff only had to track the vehicles
let, but so was the respective user (driver) about the assignment
identifiable for the assigned vehicle (cf. VG Lüneburg, partial judgment
of March 19, 2019 - 4 A 12719, juris para. 29). The plaintiff turned
against four orders from my authority - but without success. The court
came to the conclusion that there is a legal basis for the processing
personal data is not relevant, so the processing
was not lawful (Art. 5 Para. 1 Letter a DS-GVO). Neither
I have given my consent in accordance with Article 6 Paragraph 1 Subparagraph 1 Letter a GDPR
located, nor is the processing due to a legal obligation
according to Art. 6 Para. 1 Subparagraph 1 Letter c DS-GVO was required, nor
it was to safeguard the legitimate interests of the plaintiff pursuant to Art. 6
Paragraph 1 subparagraph 1 letter f DS-GVO required. The waiver of storage
of the data became lawful within the meaning of Art. 58 Para. 2 Letter d DS-GVO
arranged. The arrangement according to Art. 58 Para. 2 Letter g DS-GVO, the
data previously collected for GPS tracking purposes within two
week from the finality of the decision and the deletion
confirm, withstood. The arrangement of the comprehensive information of the
Drivers leading vehicles according to Art. 58 Para. 2 Letter c DS-GVO
also confirmed by the court. The court also ordered the

Submission of an updated processing directory according to Art. 58 Para. 1

Letter a DS-GVO considered lawful.

Medical billing office - billed in compliance with data protection?

In a further procedure, the VG Wiesbaden made it clear that the

administrative litigation is not a place for the preparation of claims for damages

claims according to Art. 82 DS-GVO (judgment of September 19, 2022, Az. 6 K

685/22.WI). The plaintiff complained to me that

a private medical billing office provides incomplete information

have. The check showed that no more data was saved for the invoice

chert because the plaintiff's consent had not been obtained. This one had them

Immediate deletion requested and the invoice was deleted immediately

been. In addition, the plaintiff also submitted a request for information

directed to the private medical billing office. I had after examining the

The plaintiff was informed of the situation with a notice that there was no violation.

Against this he brought an admissible obligation action. This considered

the VG Wiesbaden, however, inadmissible, since the right to sue according to § 42

Para. 2 VwGO was missing because the plaintiff did not violate a subjective

could speak right. There was also no legal basis on which

he has a pure determination authority without legal consequences for the person responsible

could support. The court found that there was no task of

is the supervisory authority, civil law claims for damages according to Art. 82

DS-GVO to facilitate and via the detour of the official investigation evidence

secure for the person concerned. The decision is not final. The

Plaintiff has applied for leave to appeal.

Oral hearing before the Federal Constitutional Court

The highlight of the court proceedings in the year under review was my

ment as an expert informant in the oral hearing

of the BVerfG on constitutional complaints regarding automated data

evaluation by the police in Hesse and Hamburg (Az.: 1 BvR 1547/19) on

December 20, 2022. Section 25a HSOG enables the Hessian police to

all data stored with her, e.g. for preventive control of

analyze serious crimes. Since 2018, Hesse has had the

Analysis software Gotham from the US company Palantir is used. that up

Analysis tool adapted to Hessian conditions is available in Hesse under the

designation hessenDATA (see also Chapter 6.1).

In response to the extensive questions asked by the court in the oral

development I have both answers to that of my employees and

given to employees of the established practice of using hessenDATA

court and fine proceedings

as well as data protection assessments. With regard to the

I have practice on the problematic reach of the analysis tool

pointed out. It takes u. to all data from radio cell queries

which is all persons who use a mobile device to communicate at a specific

Time spent in a certain spatial area recorded

become. It also evaluates all data from the police documentation system

even if they have nothing to do with serious crimes.

In this documentation system, all occurrences with which

the police has to do, documented, from criminal investigations, over

Witness statements, traffic accidents, reports of loss to neighbors

disputes and unsubstantiated suspicions. As a result, there is a risk

that many people are involved in police investigations that take place there

don't belong. Access to this analysis software in Hesse via

2,000 detectives working with her over 14,000 investigations in 2021

have performed.

One of the constitutional problems is that the dangerous

defensive provision of § 25a HSOG is very little defined. If

the scope is formulated so broadly, it is difficult in practice

drawing borders. Due to its depth of intervention, the analysis software

not become the standard tool for police work, but is for

reserve for very serious cases.

In the process I also related to another problem

with the topic of earmarking pointed out. When analyzing the at

the police stored data with hessenDATA are large amounts

included in data from "bystanders" who do not know about it and

who have no chance to arrange their lifestyle in such a way that they are not

are recorded. With hessenDATA, all data is stored with the police

Share a unified large data pool for analysis for far-reaching

future investigative purposes.

On the judgment of the Federal Constitutional Court of February 16, 2023 and the

I will have consequences for Hessian practice in the next activity report

make further explanations

5.2

Overview of the fine proceedings conducted

In 2022, the violations by the responsible authorities from the

diverse industries and areas. focal points

formed in the reporting year the proceedings against corona test centers and

Employee excesses in the public and non-public areas.

Fine procedures in numbers

In the reporting period, I initiated a total of 53 new fine procedures

directs. While the number of newly pending cases compared to

year-on-year, the number of sanctioned violations increased. There were

A total of 113 fines were waived, which were directed against natural persons

and against companies from various sectors.

The total amount of fines imposed was in the reporting period

at 44,350 euros.

The impact of the pandemic continued to be felt during the reporting period.

One focus of the processing in the fine office was the punishment

of violations by operators of corona test centers. Over and beyond

cases of staff excesses have been reported both in public and in

non-public area continues to be consistently pursued.

Violations by test center operators

Due to the ongoing corona pandemic, the health

area and in particular the operators of corona test centers more in

brought the focus. Here, after completing previous

several procedures for administrative offenses in the supervisory procedure

initiate (see also Chapter 15.3). This was mainly due to violations

against the principles for the processing of personal data (Art. 5

DS-GVO), legality (Art. 6 DS-GVO) and security (Art. 32

DS-GVO) of processing. Several procedures could already become final

be completed.

In one case, the fine proceedings were directed against a company
which operates several test centers mainly in the Rhine-Main area. sex
The subject of the procedure was the sending of an e-mail in the open mailing list
to approx. 100 people, whereby no sensitive data was affected. Although
the person responsible on the same day from an e-mail recipient
had been informed of the incident, they saw no reason to
to initiate further measures. Through the unlawful disclosure
of the numerous e-mail addresses, the company violated Art. 6
Para. 1 GDPR. In addition, it violated the documentation requirements
a data protection breach pursuant to Article 33 (5) in conjunction with Article 33
Para. 1 GDPR.
Based on the estimate made of the previous year's sales of the
company and taking into account the assessment criteria
Art. 83 Para. 2 DS-GVO were fines of 10,000 euros for
the first and 6,400 euros for the second violation. Significant

court and fine proceedings
the decision was due, among other things, to the constructive cooperation
with the supervisory authority and the expressed insight of the
company. In addition, the appointment of a data protection
commissioned in the aftermath of the incident and the fact that for the first
times data protection violations against the company became known
which is taken into account as a mitigating factor in the assessment of fines. Therewith
were the individual fines in the selected amount in the overall result
effective and proportionate in accordance with the requirements of the GDPR
and chilling. The company that, within the scope of the regulatory

was represented by a lawyer in the priority proceedings, accepted the decision

and made no objection.

In another Hessian test center, carelessness led to a

Error: An employee took an adhesive label due to lack of care

out of the trash, handwritten the email address of the testing center

on it and stuck the note to the plexiglass pane so that it was visible from the outside

at the test center. Unfortunately, the personally identifiable information

of a customer, such as name, birthday, date and time of the last test

and test ID, printed on the label. The note was only

tag removed from the disc. The data were therefore for a period of

approx. 24 hours visible to third parties. The test center turned during the

procedure that the employee involved did not perceive

that there was still customer data on the sheet of labels. She

I mistook the note for an empty sticky label and therefore labeled it with the

E-mail address of the test center attached to the pane.

By disclosing the above information, the responsible

makes his customer's data accessible to an unlimited group of recipients

and thus violated several principles for the processing of personal

83 para. 5 letter a in conjunction with Art. 5

Paragraph 1 letters a and f as well as Art. 6 Paragraph 1 DS-GVO. The plot was with

sanctioned with a fine of 1,800 euros. In this case, too

the operator of the test center showed understanding and paid the fine.

employee excesses

In the year under review, I had eight cases in the police force, with one

fine notice completed. The underlying actions of

Police officers referred to a wide variety of issues,

however, all took place for private reasons. Among other things,

Data queries about ex-partners, neighbors, family

relatives, acquaintances, colleagues and executives

police systems and systems available to the police in particular

out of curiosity, parental concern or lovesickness. Against it

according to § 170 Abs. 2 StPO in connection with § 46 Abs

Procedure from legal as well as another procedure from actual

reasons.

In a procedure against a police officer, a notice was issued

Fines totaling 7,380 euros plus expenses were waived.

The police officer had various police or police related

available databases for queries for own purposes.

The extent of the illegal data queries was exceptional: The

Police officers had received several hundred queries over three years

makes. The decision is not final.

In another case, a police officer questioned a female colleague several times

EWO off. In favor of this colleague, a ban on information in the registration

registered according to § 51 BMG. By entering different

However, the officer received more than 300 hits in query parameters in the system

displayed and thus extensive third-party data is provided. against

I imposed a fine of 800 euros on police officers. The

The fine notice is already final.

Several EWO queries about her ex-husband's new partner

by a police officer were the subject of another fine

monetary procedure. Among other things, the policewoman wanted to go through the queries

Bring experience where her ex-husband is with their children

stops. The procedure ended with a decision on a fine

300 euros that has not been attacked and paid.

In addition to the events described above, during the year under review I

also several cases of employee excess in the non-public area.

In one procedure it was due to concrete evidence of a

Criminal offense within the meaning of § 42 BDSG required a criminal complaint to the responsible

to provide public prosecution. The case was triggered by a report

of personal data breaches of a company

company, through which I have a breach of data protection law

former employee was informed. The retired employee

sent an e-mail to apply for a job for a new company that was founded in

competition to his former employer. He used 145

E-mail addresses from the customer base of his former employer.

Management assumed that the employee would have access

to the affected e-mail addresses, which are not general in the company

are accessible, abused, stored them on an external memory

and then used it for his own purposes.

court and fine proceedings

Because the employee's personal data from the business area

his former employer for the purpose of customer acquisition for his

stolen from a new employer or himself, passed under

other indications that the employee intends to enrich themselves

had traded. There was therefore a suspicion of a violation of Section 42

Para. 2 BDSG. According to Section 42 (3) BDSG, the offense can only be prosecuted upon request.

The competent public prosecutor's office saw in the investigation according to § 153

Para. 1 StPO due to the low level of guilt of the perpetrator and the lack of

from the prosecution in the public interest and gave up the procedure for

follow any administrative offenses on my own responsibility

authority. The fine proceedings that have been initiated have not yet been completed.

Violations by address dealers

During an unprovoked examination of a professional address dealer in

form of a small corporation, several data protection

problems identified. On the one hand, the data protection notices of the

Affected not adapted to the requirements of the GDPR and thus

outdated. The second was the contact form embedded on the website

unencrypted. There were therefore violations of Art. 13 DS-GVO and Art. 5

Paragraph 1 letter f in connection with Art. 32 DS-GVO.

During the company's data protection information for around four weeks

adapted to the current regulations after the intervention of my authority

had been in the oversight process for law enforcement

in relation to the TLS encryption of the contact form in accordance with the

Requirements of Art. 32 DS-GVO several threats of fines and one

Fixing of the fine in the amount of 2,500 euros necessary. Parallel

I had initiated proceedings for administrative offenses. Only as the

Enforcement of the imposed fine was imminent

the company is prompted to take the necessary steps

to encrypt transmissions of the contact form.

I ended the procedure for administrative offenses with a fine

decided on a total of 7,800 euros. Although the violations

could be clearly proven, the company appealed against the evidence

only filed an objection well after the deadline had expired and filed one

Application for reinstatement in the previous status. This was justified

with the fact that the manager was away on vacation and the

representatives commissioned by her did not inform her in good time about the received

informed of the fine. The representative should send her all mail

have handed over, only by means of a postal delivery document in the yellow

The fine notice sent to the envelope should be sent to the representative after the

driver's seat of the car may have slipped. This was several weeks later

been found.

I dismissed the request for reinstatement

unfounded and the opposition consequently inadmissible. Out of my sight

could not blame the managing director for missing the deadline

be cleared out. The representative was neither

appropriately instructed or trained, nor did he receive specific instructions

gene, as with official or judicial time-triggering notifications

was to be done.

The managing director filed an application against the rejection decision

court decision according to § 69 paragraph 1 sentence 1 and sentence 2 in connection with

§ 62 OWiG. My authority did not help the application and dropped the case

District Court of Wiesbaden for a decision. The district court closed

my legal opinion and confirmed my rejection notice

entirely lawful. According to Section 62 (2) sentence 3 OWiG, this decision

decision of the court incontestable. However, the victim objected

complaint. This was submitted to the district court of Wiesbaden

dismissed as inadmissible.

The fine proceedings have thus been concluded with legal effect. The fine

is filed against the company as part of the enforcement

drifted

5.3

EU guidelines for calculating fines

To understand the practice of calculating fines in the EU and EEA

standardize, the EDPB is working on guidelines for the calculation of

fines. To this end, the EDPB has submitted a first draft and

Consultation process carried out. These guidelines will be of great

authority for the future imposition of fines.

In the year under review, the EDPB submitted the long-awaited proposal on May 12, 2022

for guidelines on calculating fines under the GDPR (Guidelines

04/2022 on the calculation of administrative fines under the GDPR)

taken and published (https://edpb.europa.eu/system/files/2022-05/

edpb_guidelines_042022_calculationofadministrativefines_en.pdf). From the

From May 16 to June 27, 2022, a public consultation was held on the

draft done. The feedback to the public consultation was

published on the EDPB website.

court and fine proceedings

The guidance complements the previously issued guidance on application

and determination of fines within the meaning of the DS-GVO (WP 253), which

focus on the circumstances leading to the imposition of a fine. Goal

of the new guidelines on the calculation of fines is to provide a Europe-wide

strive to harmonize their determination. Harmonized output

points should be a common alignment, on the basis of which

Fines can be calculated on a case-by-case basis. With that comes the

EDSA its legal mandate from Art. 70 Para. 1 Letter k DS-GVO

after, after which he has uniform guidelines for supervisors in relation

to the application of measures according to Art. 58 Para. 1, 2 and 3 DS-GVO

and the determination of fines according to Art. 83 DS-GVO.

These guidelines take precedence over the national guidelines of the DSK. you concern

both cross-border and non-cross-border cases.

However, the assessment of the individual case is not omitted. According to Art. 83

Para. 1 DS-GVO it must be ensured that each individual fine is effective,

is proportionate and dissuasive.

The developed method of calculating the amount of the fine is divided into

five steps that "climb along" Art. 83 DS-GVO:

Step 1

In a first step, the processing operations of the individual case are closed

determine and evaluate the application of Art. 83 Para. 3 DS-GVO (Chap. 3

the guideline). It is important to first check on what behavior

(actual circumstances of the behavior) and which violations (abstract

legal descriptions of what is sanctionable) the facts

based. First of all, it must be clarified whether the case stems from a criminal offense

whether there are separate sanctionable forms of conduct

act. Do the behaviors give rise to a classification of

a violation and there is no agreement, this is the reason for

any violation will result in a fine up to the maximum legal limit

impose violation. Give the sanctionable action or

the separately sanctionable forms of behavior cause for the punishment of

more than one violation, then it must be checked whether the violations are mutually exclusive

exclude or whether the infringements apply simultaneously. So here it comes

on the assessment according to the principles of specialty, of subsidiarity

and consumption.

step 2

This is followed by setting the starting point for further calculations

the amount of the fine (chapter 4 of the guideline). The EDPB is of the opinion

that the calculation of the fine is based on a harmonized

point should begin. The starting point is defined by three elements:

a. the classification of the violation in accordance with Article 83 (4) to (6) GDPR,

b. the severity of the violation according to Art. 83 (2) letters a, b and g GDPR,

c. the company's turnover as an important element in terms of

the imposition of an effective, dissuasive and proportionate

Fine within the meaning of Art. 83 Para. 1 DS-GVO.

step 3

In a third step, the aggravating and mitigating

related to past or present behavior

of the person responsible and the corresponding increase or decrease

of the fine (Chapter 5 of the guideline). After evaluating the

The nature, severity and duration of the violation and its intentional or

negligent character and the categories of data concerned in step 2

are now the aggravating or mitigating factors under Article 83(2).

GDPR to take into account.

step 4

In the fourth step, the relevant statutory maximum amounts

determined for the processing operations. Those in previous or next

Calculations made in increments may not exceed this maximum

(Chapter 6 of the guideline). The GDPR follows with these maximum

amounts to the general tradition of Union law on sanctions. The

Amounts in Art. 83 Para. 4 to 6 DS-GVO represent legal maximum amounts

and thus prohibit the supervisory authorities from imposing fines

that end up exceeding the applicable maximum amounts. The

Maximum amounts are divided into static maximum amounts and dynamic

cal maximum amounts. According to Art. 83 Para. 4 DS-GVO, fines of up to

to an amount of up to 10 million euros due to violation of Art. 83

Para. 4 DS-GVO are imposed. against

sees Art. 83 Para. 5 and 6 DS-GVO in the event of violations of those mentioned there

obligations fines of up to 20 million euros. In the

Case of a company can increase the range of the fine towards

a sales-based maximum amount. This revenue-based

The maximum amount is dynamic and individualized for the respective company

aligned to the principles of effectiveness, proportionality and

deterrence from Art. 83 Para. 1 DS-GVO. In this context is

it is important to understand how the term "company" within the meaning of Art. 83

DS-GVO is to be understood. Recital 150 GDPR is based on
Concept of company according to Art. 101 and 102 TFEU. Accordingly, a
so-called functional company concept based on the German
administrative offense law is alien. This is based on the so-called legal
principle on. After the Bonn Regional Court, in its decision of
November 11, 2020 (Az.: 29 OWi 430 Js-OWi 366/20-1/20) in favor of
European approach, KG Berlin decided on December 6
About 2021 (Ref.: 3 Ws 250/21 – 161 AR 84/21) the ECJ in German matters
Living submitted this question for decision. A decision of
CJEU (C-807/21) is eagerly awaited.

step 5

The fifth and last step is to check whether the calculated final amount
the requirements of effectiveness, proportionality and deterrence
from Art. 83 Para. 1 DS-GVO. The fine can be in this step
if necessary, be adjusted accordingly with regard to Art. 83 Para. 1 DS-GVO,
however, without exceeding the applicable statutory maximum
(Chapter 7 of the guideline). Anything in excess of this maximum amount will
cut.

In the five steps, at all times it must be borne in mind that the calculation
a fine is not just a mathematical exercise. Rather, they are
Circumstances of the specific individual case are the determining factors that
lead final amount.

Even if the structure of the guidelines gives the impression that they are
could, the calculation of the fines is purely mathematical, should the
Calculating fines doesn't have to be a math exercise. Therefore
In principle, there are also approaches to programming fine calculators, im

result fails.

outlook

The next step is now for the EDPB and the responsible working group to

incorporate the feedback from the consultation phase into the guidelines.

This work has already started. Hesse is next to the federal government and

Berlin involved in this working group.

Whether the fine guidelines of the EDPB lead to significantly higher fines

lead remains to be seen. Because it finds Art. 83 Para. 1 DS-GVO as cor-

Reactive application after which the fine is effective, proportionate and

should be intimidating. It is certainly true that the fines already

are significantly higher today than they were under the BDSG, and as a result

lead to irritation at the local and regional courts. Because the national

judicial fine practice does not know these high amounts, the react

Courts initially rather reserved. It already follows from

the fine framework that the fines are designed for other amounts

are. Here, too, a practice will first have to be developed.

However, this also means that fine proceedings end up before the courts.

6. Police, protection of the constitution and judiciary

Police, the Office for the Protection of the Constitution and the Judiciary

The police, the Office for the Protection of the Constitution and the judicial authorities have far-reaching

Information on the processing of personal data leading to deep interventions

lead to the informational self-determination of the persons concerned

can. However, precisely because of this, these powers are always specific

linked to legal requirements. To protect fundamental rights

informational self-determination, it is therefore important that these powers,

their requirements and their limits are proportionate and with regard to

be monitored for compliance. The proportionality of the legal

powers was the subject of constitutional complaints in the reporting period

against the authority in § 25a HSOG to use the existing data in police

to evaluate collections with the help of analysis software (Section 6.1), and from

parliamentary hearings on the amendment of the Hessian law

on public security and order (Section 6.2). Compliance with

The prerequisites and limits of these powers were the subject of

at the State Office for the Protection of the Constitution (Chapter 6.3), at the police authorities

(Section 6.4) and at public prosecutor's offices (Section 6.5). Difficult demarcations

of powers under the right of assembly and the law of criminal prosecution

themselves during “walks” by corona deniers (Section 6.6).

6.1

HessenDATA before the Federal Constitutional Court

Due to several constitutional complaints, the BVerfG examined i.a. the

Constitutionality of § 25a of the Hessian Security and Ordinance

ungsgesetzes (HSOG), which allows automated data evaluation by the

Police allowed in Hesse. In this case, the court asked me to

Written statement requested and for oral hearing on 20.

December 2022 (see Chapter 5.1).

In the procedure for the constitutionality of the automated data

Evaluation by the police in Hesse and Hamburg (file number: 1

BvR 1547/19, 1 BvR 2634/20) I submitted a statement to the BVerfG

on my experiences with the application of § 25a HSOG and mine

constitutional assessment. This provision allows the

Hessian police, the personal data stored with them

also to be analyzed to prevent serious criminal offenses

ren. In Hesse, the Gotham analysis software has been used for this purpose since 2018

US company Palantir for use. The adapted to Hessian conditions

Analysis tool bears the name HessenDATA.

67

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

§ 25a HSOG

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

process generated data using an automated application for data analysis

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

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

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

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

damage to the environment is to be expected.

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

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

ations, objects and things produced, insignificant information and knowledge

excluded, the incoming findings assigned to known facts

and stored data are statistically evaluated.

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

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

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

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

the hearing must be made up for.

Essentially, in my statement on the concept of danger and

the term "justified individual case" used in the regulation

increased intervention quality of certain data sources and earmarking

as with data from the transaction processing system and data from radio

cell queries, access options and user numbers within the framework

of proportionality, the design of the rights of those affected and the

procedural protective measures expressed.

First of all, constitutionally problematic is that the

legal provision of § 25a HSOG with regard to intervention thresholds

is not definite enough. The design of the scope for

preventive combating of criminal offenses mentioned in § 100a StPO

so far into the danger zone that it is difficult to

practice to set limits that reflect the encroachment weight of the measure

Sufficient account and security from law enforcement

demarcate For circumstances with a sufficiently specific risk

for weighty legal interests and in the area of serious crime

the use of the analysis software may be justifiable, but it must not

become standard tools for police work.

Furthermore, § 25a Para. 1 HSOG with regard to the "justified

Individual case" does not apply to any specifications such as this wording in practice

understand is. In any case, it is essential that the justification for the

concrete application of the data analysis with hessenDATA in each individual case

is sufficiently documented to enable verification.

Police, the Office for the Protection of the Constitution and the Judiciary

With regard to the data sources, the interim report of the study

Committee of the Hessian State Parliament (Hessian State Parliament: Inter-

Technical report of the investigative committee 19/3 on printed paper 19/6574,

LT Drs. 19/6864, p. 18f.) an overview of the in hessenDATA aktuell

included data sources, with data from seven different data

sources can flow in. These include the three Hessian police

Databases POLAS, Crime (ST) and ComVor, data from the Hessian

System for telecommunications surveillance (TKÜ) according to § 100a StPO and

the nationwide interface for traffic and connection data

TKÜ operator according to § 100g StPO, forensic extracts (from IT evidence objects

extracted contact and connection lists), telex and manual

imported data from publicly accessible social networks. All of

of the police and the data sources included in the data analysis

stored data becomes part of the analysis software

a virtual data pool for analysis for far-reaching future investigations

lung purposes.

In the police case processing system ComVor, all occurrences

facts that the police deal with are documented, from investigations to

Criminal offenses, witness statements, traffic accidents, loss reports up to

to neighbor disputes and unsubstantiated suspicions. consequently

personal data of any kind from ComVor

evaluated and according to § 20 paragraph 9 HSOG for the data analysis according to § 25a

HSOG the principle of strict earmarking for data of transaction

administration to be breached.

§ 20 HSOG

(...)

(9) The security and police authorities can process management or

temporary documentation of official actions personal data exclusively

further process for this purpose or for the purpose specified in paragraph 10 sentence 1. Paragraph 1

to 7 do not apply in this respect. The personal data according to sentence 1 can

also be further processed for the purposes specified in Sections 13a, 13b and 25a."

(...)

The range of the analysis tool when accessed is also problematic

of data from cell queries, thereby personal data of all

People who log in with a mobile device at a certain time

have stayed in a certain spatial area can be recorded.

When analyzing the data stored by the police with hessenDATA

This means that large amounts of data from "uninvolved" people are also collected

included, those who don't find out about it and who don't have a chance to share theirs

Arranging a lifestyle in such a way that they are not recorded. A further

processing of such data according to § 25a HSOG is not included in the standard itself

subject to special conditions.

The wording of § 25a HSOG does not result in any limitation of the

options and use of hessenDATA, so that the question arises

according to proportionality. Access to this analysis software

currently have over 2,000 detectives in Hesse who deal with her a year

Conducted over 14,000 investigations in 2021. The depth of engagement

Data analysis, the complexity of the research activity and the sensitivity of the
obtained analysis results make it necessary to use the actual
Accesses and users of such an application to the absolutely necessary
limit measure.
Furthermore, in my written statement I have the inadequate
corresponding legal anchoring of the rights of data subjects and legal protection
Possibilities regarding § 25a HSOG discussed. On the one hand, there is
Danger that the right to information is only related to the source systems
and therefore not specifically to hessenDATA. Lack of recognition of one
such a right to information specific to § 25a HSOG, it is one affected
Person hardly possible to find out whether personal data under
have been analyzed by hessenDATA, and subsequently legal
to seek protection and, if necessary, to take legal action. On the other hand, § 25a
HSOG neither from the special logging obligation with undercover and
intervention-intensive procedure according to § 28 HSOG nor from notification
obligation to provide under Section 29 (5) in conjunction with Section 28 (2) HSOG.
Finally, I pointed out that § 25a HSOG does not have the necessary
agile and effective procedural protective measures.
This is how the project, which is intended as a safeguard from a data protection perspective,
hearing of my authority in § 25a Abs. 3 S. 2 HSOG currently practically empty, since
my authority in the general phenomenon-related orders
of the Hessian police authorities was included (see small inquiry
and answer, LT-Drs. 20/660, p. 1, as of July 2019: In the answer to the question
1 five general phenomena-related arrangements are mentioned). But
since 2019 it has no further orders and consequently none
hearings of my authority, since this is not intended,

as long as hessenDATA no major change from a technical point of view
experienced and without significant innovations with the same source systems
and databases is used. Furthermore, the obligation to data
protection control by my authority in § 29a HSOG not to § 25a HSOG
and there are no specific judge caveats or reporting requirements.

70

Police, the Office for the Protection of the Constitution and the Judiciary
As a result, I stated in my statement that
the regulation § 25a HSOG constitutional in several respects
Is exposed to doubts, also by a possible constitutional
Ultimately, interpretation cannot be eliminated.
On the judgment of the Federal Constitutional Court of February 16, 2023 and the
I will have consequences for Hessian practice in the next activity report
make further explanations.

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

In the year under review, the state government submitted a draft law for amendment
safety regulations and the reorganization of the Hessian
Riot police dated March 22, 2022, LT-Drs. 20/8129, before. As part of
of the legislative process, I gave a written and oral
lung decrease, about which I report below. The Legislative
driving was not yet at the time the activity report was prepared
completed.
As part of the public hearing in the Interior Committee, I had the opportunity
heit, on the draft law to amend safety regulations and

on the reorganization of the Hessian riot police of March 22, 2022,

LT-Drs. 20/8129 to comment. Unfortunately I didn't have the opportunity

my data protection concerns at an early stage within the framework of the

to contribute to the drafting of the law.

My comments focused in particular on the proposals to amend

amendment of the Hessian law on public safety and order

tion (HSOG). The bill also had amendments to the

Hessian Constitutional Protection Act (HVSG). But he had

not yet the new requirements of the judgment of the BVerfG, 1 BvR 1619/17, dated

April 26, 2022 on the Bavarian Constitutional Protection Act, which as part

was classified as unconstitutional, implemented with regard to the HVSG.

Therefore, the hearing was also limited to the proposed changes

to the HSOG.

My full opinion can be found in the INA committee proposal

20/53 Part 1 of July 1, 2022 on pages 79 ff., which is also the basis

for my statements in the public oral hearing of the

committee of the Hessian state parliament on July 15, 2022.

Regular review of applicants

In the statement I have u. critical to the proposed

Change of § 13a Abs. 2 HSOG-E expressed. The

seen supplement, officials who work in an authority with

Aim for enforcement tasks, regularly also on the basis of databases

Checking the LfV Hessen is understandable, but contains due to

the special nature of the databases of the Office for the Protection of the Constitution

legal risks.

First of all, it is already problematic to designate such a standard

designed review, which in the result due to "soft" findings of the

Protection of the Constitution exclude people from certain professional groups

can, to enshrine in a police law. Basically it is here

an obstacle to admission to civil service, for mostly civil servants

legal activities, and should therefore be in the relevant laws

be anchored.

In addition, there are no regulations in § 13a Para. 2 HSOG-E, such as the applicant

or the applicant in the event of a rejection, for example on the basis of knowledge

of the Office for the Protection of the Constitution can seek legal protection. In contrast to this

makes about § 7 Aviation Security Act for background checks

concrete statements on the design of the procedure.

In addition, there is the special feature that the rejection of an information

According to § 26 Para. 3 HVSG no justification is required. So it is conceivable that

the persons concerned for their work as employees of a public authority

with enforcement tasks based on findings of the Office for the Protection of the Constitution

be rejected without, however, being told which findings are involved

acts in this regard and how they can specifically check such a rejection if necessary

can let.

Video surveillance without crime analysis

I also commented on the proposal regarding video surveillance

14 Para. 3a HSOG-E. The bill has

a supplement provided in such a way that the conditions for a

Video surveillance according to paragraph 3 sentence 1 "in the publicly accessible areas

range from airports, passenger stations, sports venues, shopping malls

and packing stations are to be regarded as fulfilled". Consequently, at these local

In the future, crime analysis and video surveillance will no longer be possible

regularly be allowed.

First is the norm in terms of spatial limitations of the enumerated

Localities problematic, since there is a sufficient certainty of the

72

Police, the Office for the Protection of the Constitution and the Judiciary

"public areas" of these locations in the proposed

there is no regulation. Regarding the major airport Frankfurt am Main

there are also specific spatial demarcation problems, such as where

exactly the area of the airport begins and ends.

It is also incomprehensible from a data protection point of view that each

Packstation in Hesse to be classified indiscriminately as a crime focus

to. It is also unclear to what extent a preventive video surveillance crime

in publicly accessible areas of packing stations.

In addition, the justification for the law did not explain why

such a measure is considered necessary there at all. Regarding the

I think publicly accessible areas of all sports facilities in Hesse

an extended scheme for dispensable because of the crime occurring there

not triggered by the location. Rather, they are happening there

Events - sporting as well as social and cultural - that take place in the

cause exceptional crime risks. These may according to individual

prognostic assessment also based on the current regulation

§ 14 Para. 3 HSOG are video-monitored for crime prevention purposes.

The qualification of all shopping centers as crime hotspots is

also not appropriate.

Automated processing of license plates

The changes to § 14a HSOG-E proposed in the draft law for

automated processing of license plates now included

Clarifications and restrictions that the Federal Constitutional Court made in its judgment of March 11

2008 (1 BvR 2074/05) and by resolution of December 18, 2018 (1 BvR

3187/10) for such a regulation. However, they stay in

one essential aspect behind these requirements: The BVerfG

calls for the term "manhunt inventory" to be specified, with which the

Vehicle license plates are to be compared. A sufficient

However, there is no specification of this term in the draft law.

Continued data storage with no negative prognosis

Finally, I also have critical comments on the proposed

Legislative amendment to § 27 Para. 4 HSOG-E made, which is a significant

extension of the segregation test periods. Thus, with "continue

suspicion" regarding the categorized criminal offenses an extension

tion of storage for ten years, in the case of other criminal offenses

of significant importance (Section 13 (3) HSOG) for a further five years.

A fundamental personal negative prognosis as a legal

The previous version is a requirement for storage by the police

of the HSOG as well as in the present draft in § 20 Para. 6 HSOG

provided - such a regulation, such as § 18 para. 1 No. 3 and

2 No. 2 BKAG, missing. Against the background of the expanded

Storage options appears as a requirement for storage in

police information system POLAS-Hessen an individual personal

related negative prognosis is now even more urgent.

The current wording of the draft law ultimately becomes one

Rule storage of 15 or 20 years for categorized or classified

ten offenses without requiring an examination at the time of renewal

or checking whether factual indications justify the assumption

that the person will commit such crimes must be made. a

Speaking review is now only at a further extension

provided (§ 27 Para. 4 Clause 5 HSOG-E). The justification effort for

the corresponding encroachments on fundamental rights are thus reduced by five or ten

years in the future. In this context, I would like

In order to illustrate the explosive nature of this problem, it should be pointed out that in

Distinction from the data from the federal central register in the police

criminal offenses can also be recorded and stored in the information system,

who have not been charged or convicted.

It now remains to be seen to what extent the legislature will respond to the not only

me in the public hearing in the interior committee of the Hessian state

will respond to criticism expressed during the day and revise the draft law.

6.3

Complaints against the State Office for the Protection of the Constitution

Information from the State Office for the Protection of the Constitution in Hesse (LfV Hessen)

according to § 26 HVSG regularly contain a reference to the fact that the

data subject can contact my authority. A complaint about

a refusal to provide information triggered a review of the information procedure

from the LfV Hessen. Here data protection law and

technical and content-related questions.

The right to information vis-à-vis the LfV Hessen is a special law

Hessian Constitutional Protection Act (HVSG). The regulation of

§ 26 HVSG sees in paragraph 2 possibilities to restrict the information

right and refers in paragraph 3 to the fact that the person concerned

my authority can contact.

74

Police, the Office for the Protection of the Constitution and the Judiciary

§ 26 HVSG

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

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

points to a specific fact and a special interest in information

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

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

not up

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

2.

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

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

the effort required to provide the information is not disproportionate

on the interest in information expressed by the data subject.

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

at due discretion.

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

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

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

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

3. jeopardizes public safety or otherwise the welfare of the federal or state government

would cause a disadvantage or

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

Legislation or its essence, in particular because of the overriding

legitimate interests of a third party must be kept secret.

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

worker or an employee specially commissioned by her.

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

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

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

data protection officer. Notifications from the Hessian data

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

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

(...)

If a recipient is informed about a

partial or complete refusal to provide information appears

the opportunity to contact my authority, subjectively often than

an opportunity to still get the withheld information.

Furthermore, those affected also contact me in order to

to arrange for deletion of storages.

First of all, it should be noted that a technical examination of the content of the legal

moderation of storage at the LfV Hessen by my authority

is not provided for by law. The legislature has in § 26 paragraph 3 sentence 1
HVSG regulated that in the event of a total or partial rejection
the information without justification on the possibility of contacting my authority
to turn, must be pointed out.
My authority can confirm the information procedure at the LfV Hessen in
check from a data protection point of view. The validity of data protection
However, according to § 15 HVSG, legal regulations are restricted.
§ 15 HVSG
When fulfilling the tasks according to § 2 by the state office, the Hessian data
Data Protection and Freedom of Information Act of May 3, 2018 (GVBl. p. 82) in the respective
current version applies as follows:
1. § 1 paragraph 8, §§ 4, 14 paragraphs 1 and 3, § 19 and the second part do not apply,
2. §§ 41, 46 paragraphs 1 to 4 and §§ 47 to 49, 57, 59, 78 and 79 apply accordingly
apply.
Such an examination extends to the question of whether the LfV Hessen
with the data of the data subject in accordance with the rights of the data subject
has dealt with, so it is a comprehensibly documented, personal and
Factual handling of the specific request for information and
a complete or partial refusal to provide information. This
A data protection check differs from a technical and content-related one
Examination of the relevant storage and the assessment of whether this
related information may be refused. For a disclosure
to obtain information that has been refused so far and also in order to
If necessary, to arrange for individual deletions, the person concerned must against the
proceed in a timely manner with the notification of information from the LfV Hessen
(Objection and lawsuit). Only in this way can the

be effected. By excluding the applicability of § 14 para. 3
HDSIG in § 15 No. 1 HVSG are my authority to issue orders formulated there
not applicable to data processing at LfV Hessen. Think
restrict the supervisory authority's options vis-à-vis the LfV Hessen
refer to the powers according to § 14 para. 2 HDSIG, d. H. the complaint
to the competent supreme state authority as well as the warning
intended processing operations, insofar as these are likely to
violate applicable data protection regulations.
As far as in the data protection complaint procedure by my
authority decides that the information behavior of the LfV Hessen
is not to be criticized in the specific individual case, this does not mean that

Police, the Office for the Protection of the Constitution and the Judiciary
individual storage or refusal of information by the LfV Hessen
have been evaluated by my department in terms of content, but only
that there is an appropriate handling of the
request for a future has taken place. A lawsuit against my decision
However, the administrative court cannot delete the LfV Hessen
nor provide information on previously refused storage.
In this respect, it is important for those affected to oppose a decision by the LfV Hessen
to lodge an objection to information pursuant to Section 25 HVSG, if necessary, in a timely manner,
insofar as they require the provision of information in the case of previously rejected information or
want to achieve deletions.

6.4

Data protection controls at police authorities and the protection of the constitution

In various areas, legal regulations stipulate that I

certain data protection controls at the Hessian police authorities and at

State Office for the Protection of the Constitution (LfV Hessen). In 2022

was the data protection control carried out for the first time in 2021

Second generation Schengen Information System (SIS II).

In addition, the anti-terrorist database (ATD) and covert measures

checked.

An examination of the tenders began for the first time at the end of 2021

according to § 17 HSOG and § 163e StPO in connection with Art. 36 Para. 2 SIS

II resolution. This data protection control has been implemented across Europe and also at

Federal and state governments designed by the data protection authorities.

The police authorities use the possibility of alerting people

and items for both security and law enforcement purposes. In the

In the course of the tenders, the state and federal police

carry out covert or targeted controls and the results obtained from them

personal data by means of hit reports to the advertiser

forward job.

In the run-up to the examination, together with the Federal Commissioner for

Data Protection and Freedom of Information (BfDI) by the SIS II Supervision

Coordination Group (SIS II SCG; the group consists of representatives of

national supervisory authorities of the Member States and the European

data protection officer) compiled an extensive catalog of questions

and to the needs of the German supervisory and police authorities

speaking adapted. This was determined by the respective police authorities

Questionnaire answered as part of the control activity. Content could

This is how working methods and courses of action relating to SIS II are experienced

brought and questioned.

For the data protection control itself, my authority also worked out

from a test scheme, which also includes the data

protection supervisory authorities of the federal states and the federal government

became. The control activity was carried out by eleven supervisory authorities

and a total of 27 bodies were audited by these. The results of

Questionnaire and the test were then compiled

and communicated to the SIS II SCG.

As part of my data protection control, 26 were randomly checked

Tenders initiated by the Hessian police authorities were examined. have

I found some deficiencies: For example, the documentation requirements were increased

various police measures are not sufficient in all cases

Fulfills. This is how § 17 paragraph 4 sentence 4 HSOG looks at police observations

or targeted controls that no later than after the expiry of three

Months to check whether the requirements for the arrangement still

consist; the result of this examination is to be put on record.

Further possible regulatory measures are currently being considered

checked.

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and

the use of the second generation Schengen Information System (SIS II Decision)

Art. 36 SIS II Decision

(...)

(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.

(...)

78

Police, the Office for the Protection of the Constitution and the Judiciary

According to the legal requirements from § 10 Abs. 1 S. 1 ATDG found

there are also data protection controls for storage in the ATD. This

has to take place and has taken place every two years in accordance with legal requirements

in 2022 at the LfV Hessen and the police headquarters in Frankfurt am

Main to new saves of people within the years 2020 and

2021. The focus of this examination was on storage according to § 2 and

Section 3 (2) ATDG.

The storage in such a compound file, the information for the

Police and constitutional protection authorities of the federal states and the federal government

makes available represents a particularly deep one for the persons concerned

encroachment on fundamental rights. As a rule, the person concerned does not know that

it is stored in it.

The basis of my data protection control of ATD was initially the

File content for the stored person. Based on the submitted personal

ten and the underlying facts, my authority checked whether the

Prerequisites for storing the relevant person were met

and have been adequately and comprehensibly documented.

There are no data protection concerns against the storage

of the persons examined in the ATD.

§ 2 ATDG

The authorities involved are obliged to provide data that has already been collected in accordance with Section 3 (1) in the

Keep anti-terrorist file if they are in accordance with the legislation applicable to them

have police or intelligence findings (intelligence).

which there are actual indications that the data relate to

1. People who

a) a terrorist organization according to § 129a of the Criminal Code, which has an international

has a national connection, or a terrorist organization according to § 129a in connection

tion with § 129b paragraph 1 sentence 1 of the Criminal Code with reference to the Federal Republic

belong to or support Germany,

b) belong to a group that supports an association under letter a, or

c) a group according to letter b willingly with knowledge of the terrorism

support group activity,

2. Persons who unlawfully use violence as a means of enforcement internationally

any political or religious interests or such use of force

support, prepare or through their activities, in particular through endorsement

such acts of violence, intentionally provoke, or

(...)

§ 3 ATDG

(1) The following types of data, if available, are stored in the anti-terror database:

1. to persons according to § 2 sentence 1 numbers 1 and 2

a) the surname, first names, previous names, other names, alias personal data,

different spellings of names, gender, date of birth, birth

place, the country of birth, current and previous nationalities, current and

previous addresses, special physical characteristics, languages, dialects, photographs,

the designation of the case group according to § 2 and, unless other legal

contrary to moods and this is necessary to identify a person,

Information on identity papers (basic data),

the following additional data types (extended basic data):

b)

(...)

oo) Contact persons for the respective persons according to § 2 sentence 1 number 1 letter a or

No. 2,

(...)

(2) Contact persons according to paragraph 1 number 1 letter b double letter oo are

Persons for whom there are actual indications that they are related to the persons listed in § 2 sentence

1 number 1 letter a or number 2 not only fleetingly or in

accidental contact and through them further information for the

reconnaissance or combating of international terrorism are to be expected.

(...)

§ 10 ATDG

(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. The records entered by the countries in the anti-terror database

can also be obtained from the respective state representative for data protection

are controlled with the performance of their examination tasks in the federal states, insofar as

the federal states are responsible according to § 8 paragraph 1. The Federal Commissioner for the

Data protection and freedom of information works in this respect with the state representatives for

data protection together.

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

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

(...)

Another data protection control required by law is that of the

covert measures according to § 29a HSOG. This year checked my

Authority therefore telecommunications surveillance measures (TKÜ measure

taken) according to § 15a HSOG at the Hessian State Criminal Police Office (HLKA).

TKÜ measures are carried out by police authorities both as classic

eavesdropping measures and for locating a telecommunications device.

Police, the Office for the Protection of the Constitution and the Judiciary

The basis of the test were the telephone and mobile phone numbers

on the part of the HLKA in the period 2018 up to the deadline of November 14th

2022 were covered by a TKÜ measure. As focal points for these

Data protection control, the arrangements for the individual measures,

Documentation of the start and end of the respective measures,

notification of data subjects and deletion of old data.

At the time this activity report went to press, this was

Control activity not yet completed.

§ 15a HSOG

(1) The police authorities can use a service provider that commercially operates telecommunications

provides communication services or is involved in them, demand that he take note of them

Allows monitoring and recording of the content of telecommunications and the closer ones

Circumstances of telecommunications including the location of activated non-stationary

Telecommunications systems transmitted if this is to avert an urgent danger to life,

life or liberty of a person or for such goods of the public whose threat the

Foundations or existence of the federation or a state or the foundations of existence

touching people is essential. The measure may be directed against a person

1. who is responsible according to §§ 6 or 7,

2. in which the requirements of § 9 are met,

3. where certain facts justify the assumption that

a) they are intended for or originate from a person under No. 1

receives or forwards or

b) a person according to no. 1 uses their telecommunications connection or end device

will, insofar as the measure is essential for the prevention of terrorist offenses, or

4. which is named in Section 15 (2) sentence 1 no. 2 or 3, insofar as the measure is for prevention

terrorist offenses is essential.

The measure may also be carried out if other people are unavoidable

be affected. Section 15 (4) sentences 4 to 8 applies accordingly.

(2) Under the conditions of paragraph 1, the police authorities can also provide information about

Traffic data according to § 96 paragraph 1 of the Telecommunications Act (...), in a

current or a future period and about content that is within

of the telecommunications network are stored in memory devices. (...) Information

about inventory data according to §§ 95 and 111 of the Telecommunications Act

the police authorities from the person providing telecommunications services for business

provides or participates in it, under the conditions of § 12 paragraph 1 sentence 1, paragraph 3

and 4 require (Section 113 (1) sentences 1 and 3 of the Telecommunications Act). relates

The request for information according to sentence 3 relates to data by means of which access to end devices
or on storage devices that are in these end devices or physically separated from them
are used, is protected (section 113 (1) sentence 2 of the Telecommunications Act),
the information may only be requested if the legal requirements for the
use of the data are available. The information about inventory data based on one to one
Internet Protocol address assigned at a specific point in time may only be used to ward off a
significant risk are required. Section 29 paragraphs 5 to 7 apply to sentences 4 and 5 accordingly.
81
The Hessian Commissioner for Data Protection and Freedom of Information
51. Activity report on data protection
(2a) Under the conditions of paragraph 1, the police authorities may
who commercially have their own or third-party telemedia ready for use or the
Provide access to usage, information about usage data according to § 15 paragraph 1 of the Tele-
media law (...) demand. The information can also be about future usage data
be required. Under the conditions of § 12 paragraph 1 sentence 1, paragraphs 3 and 4
the police authorities information about inventory data according to § 14 paragraph 1 of the Telemedia Act
demand. The service provider has the data immediately on the by the police authority
to transmit in a specific way.
(3) The police authorities can use technical means under the conditions of paragraph 1
to determine the location of an activated mobile radio terminal and the
insert council and card numbers.
(4) The police authorities can ward off an imminent danger to life and limb
or freedom of a person or for such public goods, the threat to which the
Foundations or stock of the federation or a state or the foundations of
Existence of people affected, telecommunications connections through use
technical means interrupt or prevent. (...)

6.5

scrutiny of a public prosecutor's office on notifications

covert measures

In spring 2022 I have an on-site inspection at a Hessian

public prosecutor's office, which focuses on covert measures

according to § 100a StPO. Here legality, documentation

as well as notifications of those affected and the omission or final

Taking a closer look at ignoring notifications.

Monitor within the scope of Directive (EU) 2016/680 (JHA Directive).

I in accordance with § 13 para. 1 and 2 no. 1 HDSIG the application and enforcement

of the regulations on data protection in Hesse. According to §§ 14 paragraph 4 and

63 HDSIG, § 500 StPO in connection with § 68 BDSG are mine

Employees are granted investigative and control powers.

A telecommunications surveillance according to § 100a StPO constitutes an ordered

particularly intrusive measure of criminal prosecution. In the course

of surveillance measures according to § 100a StPO are regularly

processed personal data on a larger scale. This does not

ben data on the circumstances of the communication processes above all

actual content data. The subsequent notification according to § 101

Para. 4 S. 1 No. 3 StPO is a basic requirement for the protection of

Rights and freedoms of data subjects and any third parties affected.

Notification is also required for the exercise of data subject rights

necessary precondition. The legislator has in § 101 paragraph 6 StPO

therefore high requirements on deferrals of notification

Police, the Office for the Protection of the Constitution and the Judiciary

tied. Under the conditions of Section 101 Paragraph 4 Sentence 3 and 4 StPO

a notification of those affected is also omitted.

Responsible for carrying out the notification of actions after

§ 100a StPO is the respective public prosecutor's office. Because of this, mine

Authority in spring 2022 a review based on case files

carried out on site at a Hessian public prosecutor's office.

A two-digit number of files was requested as a sample. All

of the requested files related to investigations, during which measures

ordered to monitor telecommunications in accordance with § 100a StPO

had been. With the exception of one file that was in the court,

to be provided. Care was taken to select as many as possible

Cover departments and local areas of responsibility. Within the

available time frame, a total of ten files could

be subjected to more detailed scrutiny.

Particular attention should be paid to the presence of the court order

for the respective measure and the implementation of the notification

affected persons.

As a result, the basic documentation including the correct

teral resolutions available. It could, however, provide additional information

regarding the handling of notifications from third parties against

be practiced What the verifiability of weighing decisions at

As far as no notifications go, I have a more extensive one

Documentation requested. With written documentation, the

Increased legal certainty for the authority issuing the order and the comprehensibility

possibility of legality in the event of subsequent complaints from those affected

secured. In addition, in one case, a court order for the

Deferring the notification by the person responsible.

According to Section 101 (8) StPO, the personal data obtained through the measure

to delete the data immediately as soon as they are subject to any legal action

Verification or action is no longer required. erasure logs

regarding the personal data collected within the meaning of Section 101 (8).

StPO were in random controls in the intended cases

available and part of the files. The notification of the execution of the

Deletion was included in the notifications.

The departments of the public prosecutor's office are following up on the subject

Notifications as a result of measures for telecommunication

on monitoring by the person responsible. The

On-site data protection officers have also been involved.

83

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

§ 101 StPO

(1) For measures according to Sections 98a, 99, 100a to 100f, 100h, 100i, 110a, 163d to 163g

Unless otherwise specified, the following regulations apply. (...)

(3) Personal data collected through measures pursuant to paragraph 1,

are to be marked accordingly. After a transmission to another body, the

to maintain labeling by these.

(4) Of the measures referred to in paragraph 1, in the event (...)

3.

of § 100a to notify those involved in the monitored telecommunications (...)

gen. The possibility of subsequent legal protection according to paragraph 7 and

indicate the deadline for this. You will not be notified if you

there are overriding legitimate interests of a data subject.

In addition, the notification of a person referred to in sentence 1 numbers 2 and 3

person against whom the measure was not directed, stay away if

was only marginally affected by the measure and it can be assumed that they

not interested in notification. Research to determine the

The identity of a person referred to in sentence 1 is only to be made if this is

Consideration of the encroachment intensity of the measure against this person, the

Effort to determine their identity and the resulting for them or others

people with the following impairments.

(5) Notification takes place as soon as this is done without jeopardizing the purpose of the investigation,

of a person's life, physical integrity and personal freedom and

of significant assets, in the case of Section 110a also the possibility of further

Use of the undercover cop is possible. Will the notification after set

1 deferred, the reasons are to be put on record.

(6) If the notification deferred according to paragraph 5 is not made within twelve months

after completion of the measure, further deferrals require the judicial

Approval. The court determines the duration of further deferrals. It can dem

agree to definitively refraining from notification if the conditions

for a notification with a probability bordering on certainty also in the future

will not occur. If several measures are to be taken at a close time

been carried out, the period specified in sentence 1 begins upon termination

the last measure. For measures according to §§ 100b and 100c, the amount in sentence 1

said period of six months.

(7) Court decisions pursuant to subsection 6 are made for ordering the measure

competent court, otherwise the court at the seat of the competent public prosecutor's office. The

Persons named in subsection 4 sentence 1 may go to the court having jurisdiction pursuant to sentence 1

even after completion of the measure up to two weeks after notification

reviewing the legality of the measure and the manner in which it was implemented

apply for. An immediate appeal against the decision is permissible. Is the public

A lawsuit has been filed and the accused notified, decides on the application

the court dealing with the matter in the decision concluding the proceedings.

(8) Are the personal data obtained through the measure for criminal prosecution

and no longer required for any judicial review of the measure, so

they must be deleted immediately. The deletion must be documented. So far the

Deletion only postponed for a possible judicial review of the measure

is, the data may only be used for this purpose without the consent of the data subjects

be used; their processing is to be restricted accordingly.

84

Police, the Office for the Protection of the Constitution and the Judiciary

6.6

Photographs taken at meetings

In connection with public criticism of the do's and don'ts during

the corona pandemic, like-minded people appeared in the

public space. The assessment of whether these are "walks"

or "assemblies" is also for the legal possibilities

important for producing images.

During the corona pandemic, the regulations issued for

Containing the incidence of infection in the population is controversial

recorded. The possibilities for gatherings were increased by the

temporary contact bans, distance rules and the obligation to wear masks as a

perceived as limiting. This led to it also in Hessen

People came together for so-called "corona walks". The

Evaluation of whether it is a meeting or a meeting in the individual case

Walk is also with a view to the protection of personal rights

the participant relevant.

Walk versus gathering

Art 8 GG

(1) All Germans have the right to peacefully and peacefully move about without registration or permission

without assembling weapons.

(2) For assemblies in the open air, this right may be granted by law or by

be restricted by law.

A meeting within the meaning of Art. 8 GG is a local gathering

several people for the common, on the participation in the public

discussion or demonstration aimed at forming opinions. After

This definition distinguishes a meeting from a "walk"

possibly like-minded people hardly differ in individual cases.

The possibilities of state intervention for the production of images and

Recordings at meetings are defined in § 12a in conjunction with § 19a of the

Law on meetings and elevators (VersG) regulated. Furthermore

however, § 100h StPO can also come into consideration. Crucial to the

Assessing which standard can be applied is the purpose of the

Measure. This can be preventive on security or repressive

aimed at prosecuting criminal and administrative offences.

§ 12a VersG

(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.

(2) The documents are after the end of the public meeting or timely and

materially directly related events to be informed immediately

not if they are not required

1.

2.

for the prosecution of criminal offenses by participants or

in individual cases to avert danger because the person concerned is suspected of committing criminal offences

or prepared or committed in connection with the public meeting

to have, and it is therefore to be feared that it poses considerable dangers for future people

going out at public gatherings or elevators.

Documents that were not destroyed for the reasons listed in sentence 1 number 2

in any case to be destroyed no later than three years after their creation,

unless they are now needed for the purpose listed in sentence 1 no. 1.

(3) The powers to collect personal information in accordance with the

Code of Criminal Procedure and the Law on Administrative Offenses remain unaffected.

§ 19a VersG

For video and audio recordings by the police at open-air gatherings

and lifts, § 12a applies.

§ 100h StPO

(1) Even without the knowledge of the persons concerned, outside of apartments

1. Photographs are taken,

2. other special technical means intended for observation purposes are used

become,

when investigating the facts or determining the whereabouts of a

accused would be less promising or more difficult in any other way. One

Measure according to sentence 1 number 2 is only permissible if the subject of the investigation is a

crime is of major importance.

(2) The measures may only be directed against one suspect. Against others

people are

1. Measures pursuant to paragraph 1 number 1 are only permissible if the investigation of the facts

or determining the whereabouts of an accused in any other way

would be less promising or much more difficult,

2. Measures according to Paragraph 1 No. 2 are only permissible if they are based on certain facts

it can be assumed that they are connected to an accused or a

such a connection is made, the action to investigate the facts

or will lead to the determination of the whereabouts of an accused and this

would be hopeless or significantly more difficult in any other way.

86

Police, the Office for the Protection of the Constitution and the Judiciary

(3) The measures may also be carried out if third parties are unavoidable

be hit.

(4) Section 100d paragraphs 1 and 2 apply accordingly.

Image and sound recordings according to the Assembly Act

(security)

The assembly law regulations for the production of images and

Sound recordings by the police are subject to certain

tied. According to Section 12a (1) VersG, “actual indications of the

justify accepting that significant dangers from the assembly

go out for public safety or order", so that on the part of the

Police image and sound recordings can be made. is important in

In this context, that the police have a valid prognosis for

the danger emanating from the assembly is demanded and not one against

initial suspicion directed at individual persons regarding the commission of

unlawful acts (i.e. security vs. prosecution).

From this it follows that at a meeting there is no room for criminal

nal preventive video surveillance according to § 14 paragraph 3 HSOG. The rule

allows video surveillance by the police and the security

security authorities, even if this danger is not considered significant

hazard is to be qualified. On the other hand, § 12a requires a significant risk

Paragraph 1 VersG. The intervention threshold is thus clear at meetings

higher. There is also the option of making video and audio recordings

took in the context of assembly law only for the police and not

for other security authorities.

The permanently installed video surveillance of the Hessian municipalities

Basis of § 14 HSOG, regardless of whether they are from the police or

be operated by a municipal danger prevention authority, must therefore

be turned off at meetings. By case law

in this respect, a recognizability or perceptibility of the shutdown for the

Meeting participants required (OVG Münster (15th Senate), decision

of July 2, 2020 – 15 B 950/20; VG Cologne (20th chamber), decision of 1.

July 2020 – 20 L 1149/20; Cologne Administrative Court (20th chamber), decision of May 29th

2020 – 20L 968/20).

87

Image and sound recordings according to StPO (prosecution of criminal offenses and

administrative offenses)

According to § 12a Para. 3 VersG, the powers to collect personal

related information according to the provisions of the StPO and the OWiG unaffected.

The regulation of § 100h StPO, which permits the production of

Represents image recordings outside of apartments is therefore also inside

assembly law context applicable. Furthermore, § 100h StPO

through the regulation in § 46 OWIG also in the pursuit of regulatory

adversities apply.

In the context of assembly law, consideration of the necessary

the production of images and thus the proportionality

eligibility principle of particular importance, since in contrast to a

Walk through state action not only in the right to information

mational self-determination, but also in the freedom of assembly

is intervened.

The production of image and sound recordings is according to § 100h paragraph 1 sentence 1

StPO therefore only permissible if the investigation of the facts or the

Determining the whereabouts of an accused in another way

would be less promising or more difficult. In the right of assembly

It is therefore necessary to examine the context, for example, whether there is an immediate

Determination of personal details of illegal acts or omissions

of persons in the same way a prosecution of administrative offenses

enables us to take pictures.

It is therefore of great importance, first of all on the part of public authorities

to assess in a comprehensible manner whether to assume an assembly character

is. As far as z. B. banners presented by several people or pa-
roles are chanted, this clearly points to a communal, to which
Participation in the formation of public opinion or discussion
Rally and thus towards a meeting. If such obvious
relevant information is not available is due to the circumstances of the individual case
to make an understandable decision. When in doubt, it appears
against the background of the constitutionally guaranteed freedom of assembly
and the associated restrictions on government action
preferable to accept a meeting.
Then it must be clarified for what purpose images are created
should. Specifically, it must be asked whether this is a measure by
averting danger or for the prosecution of criminal offenses and
things. In the case of averting danger, the police are responsible
the requirements of § 12a Para. 1 VersG for the production of image recordings
accepted legitimately. Section 14 (3) HSOG is enforced at meetings by the

Police, the Office for the Protection of the Constitution and the Judiciary
special legal regulation of § 12a Abs. 1 VersG superseded. does it
on the other hand, it is a measure of the prosecution of criminal offenses or
breaches of law, § 100h StPO applies. Besides the police
According to § 46 paragraph 1 OWiG, the responsible administrative offense
business authority to take action.
Due to the individual assessment, the present legal basis
lay for the production of images thus taking into account the
principle of proportionality and the respective norm addressees
to be chosen. For reasons of traceability and transparency

the procedure should be documented.

89

7. General administration, municipalities

General administration, municipalities

The work of the state administration and the administrations of the districts, Cities and municipalities in Hesse consists mainly in processing personal data. This affects all citizens of Hesse. It is therefore particularly important that the administrative activities comply with data protection regulations. This is largely the scope of the case. Still, I need both the legal, technical and organizational framework of the digital transformation keep an eye on and accompany the administration (chapter 7.1) as well as the explain data protection regulations for this process (chapter 7.2 and 7.4). In individual cases there are always questions that need to be answered and require regulatory intervention – how with regard to impermissible data queries (chapter 7.3), the creation of photo graphics (Section 7.5) and conflicts of interest of data protection officers (Section 7.6).

7.1 Digital transformation of public administration and data protection

For a successful modernization of administration in the context of the OZG implementation tion is – in addition to the qualitative improvement in administrative action by providing digital, efficient and user-friendly administrative services – necessary that the citizens using them

the employees involved in the digital service provision on the

Data protection-compliant design of the means and procedures used

can trust. An essential component of a data protection-compliant environment

implementation of digitization projects is digital sovereignty.

More appropriate than the Federal Constitutional Court in its decision

census, the importance of data protection as a

suspension of trust in state action can hardly be formulated:

“Anyone who cannot survey with sufficient certainty which

relevant information in certain areas of his social

environment are known, and who has the knowledge of possible communication

onspartner is not able to estimate to some extent, can in his

Freedom are essentially inhibited, out of one's own self-determination

to plan or decide. With the right to informational

Self-determination would be a social order and a social order

enabling legal order incompatible, in which citizens no longer

know who, what, when and on what occasion about them

white. Anyone who is unsure about deviant behavior at any time

noted and permanently stored as information, used or

will try not to use such behavioral

stand out. Anyone who expects that about participating in

an assembly or a citizens' initiative is officially registered

and that risks may arise for him as a result, will possibly

to an exercise of his corresponding fundamental rights (Art. 8, 9 GG)

waive. This would not only increase the individual development opportunities

affect the individual, but also the common good, because

Self-determination an elementary functional condition of a

ability of its citizens to act and participate

free democratic community" (Federal Constitutional Court, judgment of

December 15, 1983 – 1 BvR 209/83 and others).

Even if the 2023 census verdict is already its fortieth birthday

celebrates, the statements and evaluations are due to the advancing

gitalization of all areas of life – including public administration

– today more relevant than ever. This was also reflected in the fields of activity

which was an essential part of my work in the past reporting period

The focus was on the digitization of administrative services

the Online Access Act (OZG), the question of digital sovereignty as

essential success factor for the data protection-compliant implementation of

IT projects (see also Chapter 2) and the expansion of information,

training and advisory services from my authority.

On the need for supplementary regulations in the OZG

Already in my last activity report (50th activity report, Chapter 8.1)

I had pointed out the data protection challenges that

it in connection with the digitization of administrative services

the OZG using the so-called "One for All" (EfA) principle

to solve. I mentioned the following topics:

– What 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)?

92

General administration, municipalities

– How can the legal consequences linked to this be efficiently implemented

become? Is there a need for new legal bases or are there contracts?

complete?

– Must for the processing of personal data in the OZG context

new legal bases are created or are they already sufficient

existing legal basis?

Practice has shown that the data protection issues of digital

administrative services according to the OFA principle

Circumstances, even without further legal regulations by the

the instruments for action provided by the GDPR (e.g. the conclusion

of order processing contracts according to Art. 28 DS-GVO). The

However, the associated expenses can hardly be overestimated and

entail considerable difficulties for those responsible for implementation

itself. As part of my advice on individual OZG implementation projects in

In particular, I encountered the following problems:

– The large number of potential actors (federal government, 16 federal states, 294

Counties and approx. 11,000 municipalities) may lead to the need for the

conclusion and the maintenance of a plethora of - on data protection law -

legal legitimacy - necessary contracts.

– In order to counteract this problem, individual federal governments have

different legal opinions and "data protection law

tive implementation models" emerged, some of which are incompatible with each other

are compatible – such as the conclusion of administrative agreements or

the municipal representative model.

The complex situation creates considerable legal uncertainty

ties that ultimately lead to a loss of trust among citizens

and citizens can lead. Because if already for those responsible

Actors themselves the legal situation is difficult to survey, as should

then citizens in availing of digitized

administrative services can determine with legal certainty who does what, when and

on what occasion knows about them?

Both the problem and the solution are obvious: additional ones are needed

Regulations in the OZG, which deal with both the question of data protection

accountability between the actors involved as well as additional

Provide legal bases for the processing of personal data.

The DSK had already pointed this out in autumn 2021 and issued a statutory

Reorganization of the OZG until the beginning of the III. quarter of 2022 required

(Protocol of the 102nd DSK from November 24th and 25th, 2021, Top 10, https://www.

datenschutzkonferenz-online.de/protokolle.html). About the proposed legislation

to support, the DSK set up a contact group in spring 2022

OZG 2.0 set up, in which employees of my authority also participate.

The contact group OZG 2.0 should, according to the will of the DSK, hold talks and

Consultations with the Federal Ministry of the Interior and Homeland (BMI)

and the Federal IT Cooperation (FITKO) and data protection

introduce certain requirements into the legislative process for the OZG

(Protocol of the 103rd DSK from March 23rd to 24th, 2022, Top 14, https://www.
datenschutzkonferenz-online.de/protokolle.html).
Unfortunately, it was not possible in the reporting period to provide the urgently needed
to create new regulations. This was already evident in September 2022
away. The DSK therefore already determined at this point in time that the legal
General conditions for a data protection-compliant implementation of the
EfA principle in the OZG were still not created and by the
inevitable recourse to various transitional arrangements for allocation
the responsibility under data protection law, significant data protection
al risks and doubts about the legality of administrative action
arise. A rapidly growing number of people are potentially affected
citizens, since in the foreseeable future numerous
cher OZG services are to be expected (minutes of the 3rd interim conference
on September 21, 2022, Top 8, https://www.datenschutzkonferenz-online.
de/protocols.html).
I am currently confident that the necessary
agile new regulations of the OZG are passed, since in the meantime
a draft of the OZG is available (draft of the BMI from 20.
January 2023, draft of a law amending the OZG and others
Regulations, https://www.onlinezugangsgesetz.de/SharedDocs/downloads/
Webs/OZG/DE/ozg-2-0-referential draft-ozgaendg.html).
Pending the adoption of the necessary regulations, my authority will
stand by the OZG implementation managers in Hesse in an advisory capacity
and in finding pragmatic transitional
support solutions.
Importance of digital sovereignty for data protection in

digitization projects

In the past reporting period, I also referred to the special

Importance of digital sovereignty for data protection-compliant implementation

of digitization projects and a focus here

the case law of the ECJ on the transfer of personal data

placed in third countries (50th activity report, Chapter 3). The DSK also has it

Recognized and established the importance of digital sovereignty for data protection

provides that the lawful fulfillment of state tasks freedom of choice

and full control of those responsible over the means used

and procedures for the digital processing of personal data

required (resolution of the DSK, digital sovereignty in the public

Establish administration – better protect personal data, 2020,

https://www.datenschutzkonferenz-online.de/entschlussungen.html).

In the spring of 2022, the DSK – against the background of the increasing

Outsourcing of IT processes to the cloud, also in the public sector -

set up a Sovereign Cloud task force in which my

Authority also cooperates (protocol of the 103rd DSK from March 23rd to 24th

2022, Top 9, https://www.datenschutzkonferenz-online.de/protokolle.html).

The aim of the task force is to break the concept of the "sovereign cloud" from others

Delimit cloud offers and essential requirements for “Sovereign

to formulate clouds”. In November 2022, the Sovereigns

Cloud" presents their first work results (minutes of the 104th DSK from 22.

to November 24, 2022, Top 11, https://www.datenschutzkonferenz-online.

de/protokolle.html), work on this topic is currently ongoing

however still on. But I hope that the results of the task force

future support for Hessian digitization projects

can offer.

For my advice on the data protection-compliant implementation of IT projects

in the field of the Hessian state administration and the achieved here

For progress in digital sovereignty, see also Chap. 3.4.

Information, awareness and advice

In order to ensure that data protection as an elementary component of a successful

rich digitization is understood, it is necessary to the different

Inform contributors about data protection law, for new developments

to sensitize lungs and to solve complex problems

to advise you in a cooperative and trusting manner. I have my information and

Consultancy for the public sector of public administration

therefore expanded again in the past reporting period. So became 2022

for example together with the state commissioner for data protection

and freedom of information in Rhineland-Palatinate and the professional association of the

Data protection officer of Germany e. V. (BvD) of the “1. Privacy Day

Hesse & Rhineland-Palatinate” (see Chapter 18), the municipal

zen associations were informed about new data protection regulations on a case-by-case

developments with an impact on their fields of activity (on operation

from Facebook pages and to use Microsoft 365) and it became a

regular exchange on data protection issues

the service providers for information and communication technology in the

schen Landesverwaltung (Hessian Center for Data Processing) and

of the municipalities (ekom21) initialized.

7.2

Data protection in municipalities

During the reporting period, I received inquiries and complaints regarding

various areas of local government. Hereinafter

several selected topics from supervisory practice are discussed

closer illuminated. Although the extensive data protection law

Requirements by the Hessian municipalities in daily practice

are mostly complied with, individual violations of the

record data protection.

No data processing without a legal basis

The processing of personal data is according to Art. 5 Para. 1 Letter a

and Art. 6 DS-GVO only lawful if for the respective processing

a legal basis is relevant. This central data protection law

This principle must also always be taken into account in the municipal sector.

In the course of the reporting period, I received several such messages

Violations noted:

Art. 5 GDPR

(1) Personal data must

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

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

and faith, transparency")

(...)

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

a) The data subject has given their consent to the processing of data relating to them

personal data given for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the party concerned

fene person is, or necessary to carry out pre-contractual measures, the

be made at the request of the data subject;

c) the processing is necessary for compliance with a legal obligation imposed by the

Controller is subject to;

96

General administration, municipalities

d) the processing is necessary to protect the vital interests of the data subject

or to protect another natural person;

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;

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.

Point (f) of the first subparagraph shall not apply to public authorities in the performance of their duties

processing carried out.

(...)

Transfer of personal data between

(district) municipality and district

For a transmission of personal data between (district

riger) Municipality and district (e.g. between the assembly authority

of a municipality and the regulatory and municipal supervisory authority

district) always requires a legal basis under data protection law.

The position of the district administrator as a supervisory authority according to Section 136 (3) HGO

and § 86 Para. 1 No. 3 HSOG does not in itself justify an authorization for a

data transmission.

§ 136 HGO

(...)

(3) The supervisory authority for the other municipalities is the district administrator as the authority of the state

administration, upper supervisory authority of the District President.

(...)

regulators are

§ 86 HSOG

(1)

(...)

3.

for the local regulatory authorities in the other communities the district administrator, the re-

Government Presidency and the responsible ministries.

(...)

97

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

Data transmission from a municipal authority to the chairperson of the

municipal council

The data transmission by the authority of a municipality or a

district to the chairman of the municipal council or the district council

ges always requires a legal basis. This can be, for example, Section 22 (1) HDSIG

be. For this, however, the transmission must on the one hand fulfill the

Responsibility of the transmitting body (here the authority of a municipality

or a district) or the third party to whom the data is transmitted,

(here chairmen of the municipal council or district council) lying

tasks may be required. On the other hand, the conditions must

lie, which would allow processing according to § 21 HDSIG (e.g. if

Information provided by the data subject must be verified because actual

There are indications of their incorrectness, or the processing of the

exercise of supervisory and control powers).

§ 22 HDSIG

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

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

or the third party to whom the data is transmitted

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

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

for the fulfillment of which they are transmitted to him. Processing for other purposes is

permitted under the conditions of § 21.

(...)

§ 21 HDSIG

(1) The processing of personal data for a purpose other than that

for which the data was collected, by public authorities within the scope of their

performance is permissible if

1. It is obvious that it is in the interest of the data subject and not a reason

to the assumption that they have given their consent in knowledge of the other purpose

would refuse

2. Information from the data subject must be checked because there are actual indications

there are points for their incorrectness,

3. they to ward off significant disadvantages for the common good or a danger to the

public security or order, defense or national security, for

Protection of significant interests of the common good or to secure the tax or

customs revenue is required,

4. they for the prosecution of criminal or administrative offences, for enforcement or

for the execution of penalties or measures within the meaning of Section 11 (1) No. 8 of the Criminal Code

98

General administration, municipalities

code or of educational measures or disciplinary measures within the meaning of the youth

required by court law or for the enforcement of fines,

5. to ward off a serious impairment of rights and freedoms

another person is required or

6. they exercise supervisory and control powers, auditing

or serves to carry out organizational investigations of the person responsible;

this also applies to processing for training and examination purposes by the

Controller, insofar as the interests of the person concerned are not worthy of protection

oppose

(...)

Statements in meetings of municipal bodies

In the case of statements made in meetings, in particular by municipal councils and

District councils must (especially if they are not related to the work in the committee

directly related) may be questioned as to whether a name

designation of the member is necessary or it is not sufficient,

to designate this or that person as a “member of faction x”. If-

also personal (exaggerated) statements within the framework of the

political battles of opinion are permissible, it must be borne in mind that

as a result of the principle of openness to meetings of a large

effect of such statements - possibly also in the media and via the

Internet - is to be assumed and the person concerned with any

confronted with negative consequences outside of municipal activities

could be. Such personal statements can therefore

infringe the privacy rights of the data subject.

Administrative assistance is not a legal basis

The regulations on administrative assistance, for example in §§ 4 et seq. HVwVfG, do not provide any

suitable legal basis for a transfer of personal data

This is already the case because this one data processing is not

regulate and do not meet the requirements of Art. 6 Para. 3 DS-GVO.

§ 4 HVwVfG

(1) Each authority shall provide additional assistance (administrative assistance) to other authorities upon request.

(2) Administrative assistance is not available if

1. Authorities provide each other with assistance within an existing instruction relationship;

2. the provision of assistance consists of actions which the requested authority has as its own task

incumbent.

Art. 6 GDPR

(...)

(3) The legal basis for the processing pursuant to paragraph 1 letters c and e

set by

a) Union law or

b) the law of the Member States to which the controller is subject.

The purpose of the processing must be specified in this legal basis or with regard to

the processing pursuant to paragraph 1 letter e is necessary for the performance of a task

which is in the public interest or in the exercise of public authority which

responsible has been transferred. This legal basis may contain specific provisions

contain genes to adapt the application of the provisions of this regulation, under

other provisions on what general conditions governing the regulation of

Lawfulness of processing by the controller apply what types of data

are processed, which persons are affected, to which institutions and for which

Purposes the personal data may be disclosed, which purpose limitation

they are subject to how long they may be stored and which processing operations

and procedures may be applied, including safeguards

lawful and fair processing, such as for

other special processing situations in accordance with Chapter IX. Union law or that

Member State law must pursue an objective in the public interest

and proportionate to the legitimate purpose pursued.

(...)

Transmission of personal data by municipalities

lawyers

A transfer of personal data by a municipality

a lawyer as a non-public body

can in particular be admissible if an element of § 22 para. 2

HDSIG is relevant.

§ 22 HDSIG

(...)

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

Posting is allowed if

1. to fulfill the tasks for which the transmitting body is responsible

is necessary and the prerequisites for processing according to Section 21

would allow

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

knowledge of the data to be transmitted credibly and the data subject does not

has a legitimate interest in the exclusion of the transmission or

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

and the third party has made a commitment to the transmitting public body

to process the data only for the purpose for which it was transmitted to him

become. Processing for other purposes is permitted if a transmission

would be permissible under sentence 1 and the transmitting body has agreed.

(...)

In this regard, it should be expressly pointed out that the transmission is not

is permissible solely because lawyers according to § 2 of the professional code

for lawyers (BORA) are bound to secrecy.

§ 2 BORA

(1) The lawyer is obliged and entitled to secrecy. this is also valid

after the end of the mandate.

(...)

Data transmissions by the registration authorities

In the period under review, I received – as in previous years

– multiple inquiries and complaints that data transfers through

concern registration authorities.

The registration authorities may process personal data in many case con-

process statements. Nevertheless, affected persons are several

Rights to have data transmission blocked or restricted.

Affected persons can find out more about the regulations on my website

genes (blocks of information and more, rights of those affected

registration authorities; available at https://datenschutz.hessen.de/datenschutz/

municipalities/rights-of-those-concerned-at-registration-authorities).

Although data protection violations by the registration authorities in my

legal practice can only rarely be determined, it came up in individual cases

unlawful transmissions. The following case should illustrate this as an example:

A lawyer requested an extended information on the register of residents

Tenant of his client, in particular with regard to the residential address

the tenant's separated wife. The tenant had rent claims

not settled. The wife herself was not a contractual partner of the

rental agreement.

According to § 45 BMG, an extended information from the register of

Various personal data are provided, "as far as a legitimate

interest is made credible". This may also contain “Family name

and first name as well as address of the spouse or life partner”.

§ 45 BMG

(1) Insofar as a legitimate interest can be credibly demonstrated, the

1 specified data of individual specific persons an extended information from the register of residents

be granted via

earlier names,

1.

2. Date and place of birth as well as the country in the case of birth abroad,

3. Marital status, limited to whether married or a civil partner

leading or not

previous adresses,

4. current nationalities,

5.

6. move-in date and move-out date,

7. Last name and first name as well as address of the legal representative,

8. Surname and first names as well as address of the spouse or life partner

as well as

9. Date and place of death and, in the case of deaths abroad, the state.

(...)

A “legitimate interest” is anything permitted by law

interest of a legal, economic or ideal nature.

After consideration, this must be the opposite for each individual date ("to the extent")

legitimate interests of the data subject in non-disclosure

of reporting data predominate (Schwabenbauer, in: Engelbrecht/Schwaben-

bauer, BMG § 45 para. 6).

The word "so far" makes it clear that there is a legitimate interest

must refer to each individual date about which information is requested.

If the name and address of the spouse of the person concerned are required, Section 45

Para. 1 No. 8 BMG, it must be checked particularly carefully whether a calculated

legitimate interest exists (conceivable, for example, due to spouse liability according to § 1357

BGB) (Schwabenbauer, in: Engelbrecht/Schwabenbauer, BMG § 45 Rn. 15).

In this case, the registration authority considered a "legitimate interest".

given and issued an extended population register information, which all

contained the personal data mentioned in Section 45 (1) BMG. Included

was misunderstood, however, that although a legal and economic

interest regarding the personal data of the defaulting tenant

existed, such interests related to the personal data

but were not visible to the wife. In this respect, the discretion

incorrectly exercised by the registration authority.

102

General administration, municipalities

The information provided, including the name and address of the wife, had to

the noticeable effects. Several people appeared in person

the wife's apartment, demanded the outstanding rent of the separately

living husband and thus penetrated her personal

personal sphere of life.

Data protection at recycling centers

Recycling yards (recycling yards) are often owned by local authorities

organized. In this regard, it should be noted that according to § 2 para. 2

HDSIG are considered non-public bodies to the extent that they are public bodies

companies to take part in the competition.

The consequence of this is that the provisions of the HDSIG are predominantly

are closed and instead those applicable to non-public bodies

regulations of the BDSG apply.

§ 2 HDSIG

(...)

(2) Public bodies are considered non-public bodies insofar as they are

companies to take part in the competition. In that regard, find the non-public

Place applicable regulations of the Federal Data Protection Act and §§ 5 to 18 and

23 application.

(...)

In particular, the processing of the

Vehicle registration number and identity card of the residents

Resident.

The recycling center of a municipality is regularly only for the disposal of the

Waste from the residents of the municipality concerned

constant. A relevant regulation can often be found in a municipal

Statute, for example in § 3 of the Waste Statute of the Wetteraukreis.

"§ 3 waste statute of the Wetterau district

(1) To use the waste disposal facilities of the Wetteraukreis

the district municipalities except Bad Vilbel are entitled

unless otherwise provided in these bylaws.

(2) The owner, his/her waste from collection

and transport by a municipality belonging to a district excluded

sen are entitled, in accordance with these articles of association, to

waste incurred by him/her directly with the Wetteraukreis

the approved waste disposal facilities for the purpose

of handling, storing and depositing. This

Regulation does not apply to waste according to § 2 of the disposal

excluded are.

(3) The Wetteraukreis participates in the recycling yards in Echzell,

Friedberg/Bad Nauheim and Niddatal Waste from private households

ments of the Wetteraukreis except for Bad Vilbel. About the

Use of the recycling yards, the types of waste and the survey

The district council issues a separate statute on fees.

(4) If waste is not sorted according to the specifications of § 1

Paragraph 4 sentence 2 delivered, the Wetterau district decides

about the further utilization or disposal of the waste."

Employees of the recycling center can read the license plate number of the delivery

to ensure that only waste from residents

and residents of the municipality concerned. At

It is permissible under data protection law for non-district license plates

Check the driver's identity card to determine whether

it may be a resident of the county in question

acts. The processing has regularly reduced to a mere visual

to restrict trolls. Storage, for example by means of a copy or photo of the

Vehicle license plate or identity card, on the other hand, is fundamental

not permitted. An exception is only in the case of special occurrences

are permitted. An example is the enforcement of a house ban for

to name a specific driver (see also Chapter 7.5 on garbage disposal).

Guidelines for data protection in municipalities

In order to support the implementation of data protection, I have

Information for municipalities made available on my website

(available at https://datenschutz.hessen.de/datenschutz/kommunen/daten-

protection-in-municipalities). There municipal data protection officers and

Employees get an initial overview of various topics

(e.g. on the processing of personal data; rights of those affected

Persons, information according to Art. 15 et seq. GDPR; Order processing, Art. 28

DS-GVO, and joint responsibility, Art. 26 DS-GVO).

104

General administration, municipalities

7.3

Excess employees due to data queries in the motor vehicle register

After several times in the past in the media about illegal

queries by police officers is shown by the following

ing facts that the problem also in local government

can exist.

Illegal queries in file systems were in the past few years

primarily in the police context, the subject of data protection law

supervisory or fine proceedings. Automated retrieval options

Data from the central traffic information system ZEVIS, which is

fahrt-Bundesamt is operated, but also exist at the municipal ones

public order offices. ZEVIS is used in particular to

Procedures to determine who is the holder of a traffic offense

motor vehicle ("owner data"). The ZEVIS file system is subject to this

the regulations for logging in accordance with Section 36 (6) of the Road Traffic Act

(StVG). All access to the data records stored in ZEVIS

logged and are therefore traceable.

§ 36 paragraph 6 Road Traffic Act

(6) The Federal Motor Transport Authority or the registration authority as the transmitting body has about

to make the retrievals records used in carrying out the retrievals

Data, the day and time of the retrieval, the identification of the retrieving agency and the

retrieved data must contain. The logged data may only be used for the purposes of

Data protection control, data backup or to ensure proper

Operation of the data processing system are used. Those logged according to sentence 1

Data may also be used to provide the data subject with information

grant which of them are contained in Annex I, Sections I and II of Directive (EU) 2015/413

personal data to bodies in other member states of the European Union

for the purpose of tracking those listed in Article 2 of Directive (EU) 2015/413 there,

traffic safety endangering offenses were reported. The date of

request and the competent body pursuant to sentence 1 to which the transmission took place

also communicated to the data subject. Section 36a applies to the procedure according to the sentences

3 and 4 accordingly. Are there any indications that without their use the

Prevention or prosecution of a serious crime against life, limb or

Freedom of a person would be hopeless or significantly more difficult, the data may also

used for this purpose unless requested by law enforcement

using owner data of a specific person or vehicle data

specific vehicle is provided. The log data are by appropriate provisions

to protect against improper use and against other misuse and after

six months to delete.

51. Activity report on data protection

A citizen complained to me that according to his assumption

a former love interest an owner request for his motor vehicle

triggered. The relationship between those involved was about a

ting platform came about and - at least on the part of the complainant

deführers – not designed to last. For "data protection reasons" waived

the complainant therefore also to the disclosure of his actual

Name, especially since he has a steady relationship with a partner

existed, according to the will of the applicant through the love affair

should not be charged.

The relationship that came about via the dating platform was

apparently not ended amicably and thus triggered the

disappointed expectations and, above all, reactions. After exam

of the possible alternative courses of action - this may be assumed at this point

be - was taken on the part of the abandoned lady the decision that

the complainant's permanent partner about the activities

to inform their partner.

This was in view of the complainant's reticent dealings

not an easy task with his personal data. As an approach

for the "determination" of the actual name served the indicator of

Vehicle with which the complainant to the amorous adventures

had appeared. An immediate opportunity to obtain the coveted data

hold was not an option for the lady due to lack of access to ZEVIS. she knew

but a person who is in good position for local government (first

City Council) was active and asked them to give her the personal data of the

vehicle owner to obtain. Due to the request of the first city council

an employee of the local government then arranged for the holder festival

position and transmitted the data of the complainant. The disappointed

Lady used the information obtained to the complainant

and to locate his partner on social networks

and to inform the latter of their partner's infidelity. Few

surprisingly, the complainant was told by his partner

confronted, which once again disappointed the respective expectations and

ultimately resulted in the complaint to my authority.

Since official license plates as personal data contain the data

subject to protective regulations would be - the principle of

Lawfulness according to Art. 5 Para. 1 Letter a in connection with Art. 6 DS-

GVO accordingly - for retrieving the data of the vehicle owner one

Legal basis or the consent of the complainant required

have been.

106

General administration, municipalities

By checking the log data for retrieving the holder data of the

Complainant was able to carry out the query carried out in the time window in question

the local government determined and demonstrated that the retrieval

spatially and factually not in the context of a competent referral, e.g. B.

the prosecution of traffic violations. The query was

therefore unlawful, since the data processing pursuant to Art. 5 Para. 1 Letter a in

Connection with Art. 6 Para. 1 DS-GVO took place without legal reason.

Furthermore, the first city councilor, who apparently received the request out of favour,

triggered and the personal data of the complainant

had passed on to be identified. He admitted at the hearing

the violation in the fine proceedings. Against the first city council was a

A fine of €350 was issued. The decision is final.

7.4

Requirements for document collection boxes

In several Hessian cities and communities are in the past

So-called “document pick-up boxes” were set up two years ago. There can

Citizens various documents (e.g. identity cards

and passports, civil status documents, lost property) also outside

pick up during the opening hours of the citizens' office. This as fundamental

However, the offer that is to be classified as citizen-friendly must comply with data protection

fully meet legal requirements.

The first document pick-up box in Germany was opened in 2019 in the

City of Ludwigsburg in Baden-Württemberg. Meanwhile also in

Hessen installed several boxes, for example in Wiesbaden, Hanau and Bensheim.

Functionality and process of the document collection box

In Wiesbaden, next to the citizens' office at Marktstrasse 18, it has been standing since March

2021 the so-called "WI-Box" as a pick-up station for the Wiesbaden regulatory office. I

I learned how it works and the process, starting with the reservation

tion to the collection of documents by employees of the citizens' office

can be demonstrated at an on-site appointment in August 2022.

The "WI-Box" consists of two separate boxes, their functionality

Pick-up stations of delivery services is similar. The boxes are under video surveillance

and specially secured. For example, if you have an identity card in the office

gerbüro, it can be picked up at the Bürgerbüro during

can be picked up 24 hours a day at the "WI-Box" during opening hours.

The manufacturer of both the boxes and those designed for their use

Software is the Swiss Kern AG.

In one box, which has 46 compartments, ordered personal

ID cards and passports can be collected. To do this, you must first
Fingerprint scanned in the citizens' office and other data (name, first
name, address, e-mail address) are given. The fingerprint
is scanned using the Bundesdruckerei device, which is also used for the
Taking fingerprints for the identification documents is used. The
used software application developed by the manufacturer of the box
is independent of the fingerprint scanning software
for the identity card.
The personal data is processed by the software
of the manufacturer of the box, which is distributed locally on the servers of the city of Wiesbaden
will lead. The data is not transmitted to third parties. All data
will be deleted no later than seven days after the documents have been made available
(see below). After registration, a confirmation email will first be sent to the
specified email address will be sent. The filing of the documents in the
"WI-Box" is carried out by appropriately trained employees of the Citizens'
offices according to the four-eyes principle. They authenticate themselves via
an RFID/NFC card. As soon as the ID is in the "WI-Box" for collection
ready, the applicant will receive a second email
TAN code as a number and QR code.
As a further method, the manufacturer offers the function of entering the code via
to send SMS. The e-mail does not contain any further data, but only
The information that a document (ID) is ready to be picked up.
At the "WI-Box" you can either scan the code or
enter manually and scan the fingerprint (two separate
factors for authentication).
In the other box, civil status documents and other documents can

documents and lost property can be picked up. For that, the fingerprint

not required. The TAN code sent by email is sufficient for collection

receives. The documents or lost property remain for a maximum of seven

Days in the "WI Box". Provided the documents within this period

If they are not picked up, they will be picked up by employees of the Citizens Advice Bureau

removed from the "WI-Box" and taken back to the citizens' office. the one

Scanned fingerprint and other data of the citizens

Citizens become citizens upon collection of the document or at the latest after expiration

of seven days deleted.

In the case of a further collection, the fingerprint and the further

data is recaptured.

According to the City of Wiesbaden, the "WI-Box" is being

and citizens already frequently used. Since the installation in March 2021

used the system to collect around 1,200 ID documents

been (as of August 2022). The documents offered for collection

should also be continuously expanded. Also many other Hessian ones

Municipalities showed interest and would

inquire about experiences.

Data protection issues

Although document pick-up boxes such as the "WI-Box" in particular before the

Background to the advancing digitization of administration as a citizen

are kindly welcomed, must meet the requirements of data protection

be fully complied with. Also for any later additional costs

to avoid, the data protection regulations should be met from the start

carefully considered and continuously checked. To that end, in particular

consider the following guidelines.

Processing of fingerprints as biometric data

If during the application and collection process (as with the "WI-

Box") where fingerprints are taken are biometric

data processed. According to Art. 4 No. 14 DS-GVO, these are "with special

technical procedures obtained personal data on the physical

physical, physiological or behavioral characteristics of a natural

natural person who uniquely identifies that natural person

enable or confirm". The processing of "biometric data for

unique identification of a natural person" as processing

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

(See DSK, Briefing Paper No. 17 – Special Categories of Personal

Data, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.

pdf) always requires the express consent of the person concerned

person in the processing of the fingerprint for a specified purpose

(Identification of the person concerned to collect the identity card)

according to Art. 9 Para. 2 Letter a GDPR.

Art. 4 GDPR

For the purposes of this Regulation, the term means:

(...)

14. "biometric data" personal data obtained with special technical

Genetic data on the physical, physiological or behavioral characteristics

a natural person who uniquely identifies that natural person

enable or confirm, such as facial images or dactyloscopic data;

(...)

Art. 9 GDPR

(1) The processing of personal data revealing racial and ethnic

Origin, political opinions, religious or philosophical beliefs or the

trade union membership, as well as the processing of genetic data,

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

health data or data relating to the sex life or sexual orientation of a natural person

person is prohibited.

(2) Paragraph 1 does not apply in the following cases:

a) The data subject has consent to the processing of said personal data

expressly consented for one or more specified purposes, unless after

Union law or the law of the Member States can enforce the ban in accordance with paragraph 1

the consent of the data subject is not revoked,

(...)

Requirements for the declaration of consent

The declaration of consent must also meet the requirements of Art. 7

Comply with DS-GVO (see EDSA, guidelines 05/2020 for consent in accordance with

Regulation 2016/679, version 1.1, https://edpb.europa.eu/sites/default/files/

files/file1/edpb_guidelines_202005_consent_en.pdf; as well as DSK, short paper

No. 20 - Consent according to the DS-GVO, https://www.datenschutzkonfe-

renz-online.de/media/kp/dsk_kpnr_20.pdf). In this regard, in particular

the extent to which the data subject is informed, the revocability at any time

as well as the voluntariness of the consent given. Further

has a clear separation between the processing of a fingerprint

and the processing of other "simple" personal data (name,

e-mail address etc.).

Art. 7 GDPR

(1) If the processing is based on consent, the person responsible must prove it

can that the data subject in the processing of their personal data

has consented.

110

General administration, municipalities

(2) If the data subject gives his/her consent in the form of a written declaration

still concerns other matters, the request for consent must be intelligible

and easily accessible form in clear and simple language so that it

clearly distinguishable from the other circumstances. Parts of the explanation are then

not binding if they constitute a violation of this regulation.

(3) The data subject has the right to revoke their consent at any time. Through

the withdrawal of consent will up the legality of the consent given

the processing carried out for the revocation is not affected. The person concerned will be informed before delivery

informed of the consent. Withdrawal of consent must be so easy

how to give consent.

(4) When assessing whether the consent was given voluntarily, the circumstance

be taken into account to the greatest extent possible, whether, among other things, the fulfillment

of a contract, including the provision of a service, from consent to

is dependent on the processing of personal data necessary for the fulfillment of the

contract are not required.

Duty to inform

According to Art. 13 DS-GVO, the persons concerned are informed about the data

work (see Art. 29 Data Protection Group, Guidelines on

transparency under Regulation 2016/679, https://ec.europa.eu/newsroom/article29/redirection/document/51025, as well as DSK, short paper no. 10 - In-information requirements for third-party and direct collection, https://www.datenschutz-konferenz-online.de/media/kp/dsk_kpnr_10.pdf). to the information content include in particular “the purposes for which the personal data are to be processed and the legal basis for the processing”.

In this regard, between the processing of fingerprints (Art. 9 DS-GVO) and the processing of other personal data such as name and e-mail address (Art. 6 DS-GVO). For the Processing of further data is a "simple" consent accordingly Article 6 paragraph 1 subparagraph 1 letter a and Article 7 GDPR required.

Since the document pick-up box is an additional, not legally regulated constitutes an offer is neither a "legal obligation" within the meaning of Art. 6 Paragraph 1 subparagraph 1 letter c DS-GVO still requires processing for the performance of a task in the public interest Article 6 paragraph 1 subparagraph 1 letter e GDPR to be accepted. The information should be posted at the document pick-up box on site as well as available on the municipality's website.

Art. 13 GDPR

(1) If personal data is collected from the data subject, the responsible verbatim to the data subject at the time such data was collected:

a) the name and contact details of the person responsible and, if applicable, his representative;

b) where applicable, the contact details of the data protection officer;

c) the purposes for which the personal data are to be processed, as well as

the legal basis for the processing;

d) if the processing is based on Article 6 paragraph 1 letter f, the legitimate

Interests pursued by the controller or a third party;

e) where applicable, the recipients or categories of recipients of the personal

gene data and

f) where applicable, the intention of the person responsible to process the personal data

to a third country or an international organization, as well as the existence

the existence or absence of an adequacy decision by the Commission or

in the case of transfers pursuant to Article 46 or Article 47 or Article 49(1).

the second subparagraph, a reference to the appropriate or reasonable guarantees and

the possibility of how to obtain a copy of them or where they are available.

(2) In addition to the information pursuant to paragraph 1, the person responsible shall provide the data subject

person at the time this data was collected, the following further information on the

necessary to ensure fair and transparent processing:

a) the duration for which the personal data will be stored or, if this

is not possible, the criteria for determining this duration;

b) the existence of a right to information on the part of the person responsible about the

relevant personal data as well as correction or deletion or on

restriction of processing or a right to object to processing

and the right to data portability;

c) if the processing is based on Article 6 paragraph 1 letter a or Article 9 paragraph 2

letter a, the existence of a right to withdraw consent at any time

call without affecting the legality of the consent until its withdrawal

processing that has taken place is affected;

d) the existence of a right of appeal to a supervisory authority;

e) whether the provision of the personal data is required by law or contract

Written or is necessary for the conclusion of a contract, whether the data subject

is obliged to provide the personal data and which possible

Consequences of non-provision would have and

f) 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.

(...)

112

General administration, municipalities

Data Protection Impact Assessment

The need to carry out a data protection impact assessment

35 GDPR is not entirely clear, but it is fundamental

to accept This is supported by Art. 35 (1) and (3) (b) GDPR

the large volume of data processing (potentially all residents

residents of the respective municipality), the processing of the

Data of data subjects in need of protection (imbalance of power between

the municipality and the residents; minors),

the processing of special categories of personal data

in accordance with Art. 9 GDPR and with the processing of fingerprints

associated risks of misuse (see below) (see Art. 29 Data Protection Working Party,

Data Protection Impact Assessment (DPIA) Guidelines and Response

the question of whether processing within the meaning of Regulation 2016/679

apparently entails a high risk", in particular p. 9 ff., https://www.

datenschutz-bayern.de/technik/orient/wp248.pdf; as well as DSK, short paper

No. 5 - Data protection impact assessment according to Art. 35 DS-GVO, https://www.

datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf).

Art. 35 GDPR

(1) Has a form of processing, especially when using new technologies,

based on the type, scope, circumstances and purposes of the processing

obviously result in a high risk for the rights and freedoms of natural persons,

the person responsible carries out a preliminary assessment of the consequences of the intended processing

processing procedures for the protection of personal data. For the investigation

several similar processing operations with similarly high risks can be a single one

assessment to be made.

(...)

(3) A data protection impact assessment pursuant to paragraph 1 is particularly required in the following

cases required:

a) systematic and comprehensive assessment of personal aspects of natural persons,

which is based on automated processing, including profiling, and which in turn

serves as a basis for decisions that have legal effect over natural

develop persons or impair them in a similarly significant way;

b) extensive processing of special categories of personal data

pursuant to Article 9 paragraph 1 or of personal data on criminal law

Convictions and offenses under Article 10 or

c) systematic extensive surveillance of publicly accessible areas.

(...)

Technical and organizational measures

Furthermore, suitable technical and organizational measures

according to Art. 32 DS-GVO (in particular with regard to the processing of

fingerprints as a biometric date) to take a risk

appropriate for the rights and freedoms of the data subjects

to ensure a level of protection (see DSK, Brief Paper No. 18 - Risk for the

Rights and freedoms of natural persons, https://www.datenschutzkon-

ferenz-online.de/media/kp/dsk_kpnr_18.pdf).

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.

(...)

When collecting civil status documents and other

documents and lost property as a result of the media discontinuity

Safety factor welcome if residents die

Be given the opportunity to provide their mobile phone number in order to – in addition to

an e-mail – also to be able to receive an SMS.

The collection of ID cards - in addition to the required acceptance

me of the fingerprint - possible procedures e-mail or SMS transmission

are to be qualified as equivalent.

Since, due to the easy accessibility to e-mail inboxes and finance

do not depress any abuses in the domestic family environment

114

General administration, municipalities

are to be excluded, according to Art. 32 Para. 2 DS-GVO a

Risk analysis and assessment are based on realistically possible

Abuse scenarios based.

The processing of fingerprints as biometric data should be

a level of protection appropriate to the risk (e.g. through a

IT security concept and a role and authorization concept) and

according to Art. 24 and Art. 5 Para. 2 DS-GVO can be proven.

In this respect, even if the process is one for the citizens

user-friendly method represents - not be misunderstood that the

Taking fingerprints is quite susceptible to counterfeiting.

In this respect, two aspects are relevant: on the one hand, the unauthorized one

Collection of ID documents from the document collection box using
a fake fingerprint. For this, the protection level of the finger
fingerprint scanners at the document pick-up box against counterfeit fingerprints
press significantly (especially with regard to recognizing and defending against
of common and easy-to-perform attacks).
On the other hand, the compromise in the sense of a disclosure of the stored
certified fingerprints to unauthorized third parties or the public
honesty. In this respect, it is relevant which fingerprint data is recorded exactly and
stored (a graphical representation of the fingerprint that
used for counterfeiting or use in other systems
can, or extracted fingerprint features that are not readily available for
other purposes can be misused (see DSK, position paper on
biometric analysis https://www.datenschutzkonferenz-online.de/media/
oh/20190405_oh_positionspapier_biometrie.pdf).
Regarding the e-mails sent by the municipality to citizens
and citizens is the orientation guide of the DSK "Measures for protection
personal data when transmitting by e-mail" (available at
https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientie-
ungshilfe_e_mail_verschluesselung.pdf) must be taken into account. This represents
high demands on the e-mail dispatch of personal data,
which usually includes the recipient e-mail address. The Ver-
E-mails sent should contain as little information as possible and no further
contain personal data (e.g. with the "WI-Box", with the
only the information is given that a document - e.g. B. an ID – to
available for collection).

7.5

Photographs of bulky waste by a municipal waste company

Processes are also used in everyday waste disposal
increasingly automated and digitized. So e.g. B. to the management of
Logistics processes or customer relationships are increasingly becoming digital solutions
used, which are subjected to a data protection analysis
must.

A complaint situation often goes through the communication of my service
transition smoothly into a counseling situation with the person in charge who
to increase the level of information and data protection in particular
can lead to the establishment and further development of digital processes.

During the reporting period, I received a complaint against a waste
disposal company, which in terms of bulky waste disposal for a
public waste management company operates.

The field staff took photographs as part of a pick-up order
of bulky waste and then linked them in the customer management system
with the pick-up order of the client. In the context of a complaint
case the complainant found out about the photographs and doubted the
legality of this action. In this regard, he stated
that he had not received any information about the taking of photographs.

In order for the scope of the General Data Protection Regulation to be open,
it is first necessary that the procedure described is
is a "processing of personal data". According to Art. 2 Para. 1
DS-GVO, it depends on whether personal data is completely or partially

wise be processed automatically or whether in the case of a non-automated one

Processing a storage in a file system is to take place.

The terms "personal data" and "processing" are defined in Art. 4

No. 1 and 2 DS-GVO defined.

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 identical

tifiable is a natural person who directly or indirectly, in particular

by assignment to an identifier such as a name, an identification number, a status

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

the expression of the physical, physiological, genetic, psychological, economic,

cultural or social identity of that natural person can be identified;

(2) "Processing" means any process carried out with or without the aid of automated processes

or any such series of operations involving personal data such as that

Collection, recording, organization, ordering, storage, adaptation

or modification, retrieval, retrieval, use, disclosure by

Transmission, distribution or any other form of provision, matching or

linking, restriction, deletion or destruction;

(...)

While a digital photograph is unproblematic in the technical sense

falls under the processing concept, but it was questionable whether with a view to

the bulky waste personal data are processed. For bulky waste

it is a collection of objects. A photograph

of bulky waste initially contains only information related to

these items. Acts without connection to a natural person

it is therefore so-called factual data in which initially no personal

according to Art. 4 No. 1 DS-GVO (Taeger/Gabel/Arning/Rothkegel,

4th edition 2022, GDPR Art. 4 para. 10). A personal reference can, however

only arise in the course of further processing of the data. so can

various data with a factual reference are brought together and combined in this way

that the person becomes identifiable, i.e. a personal reference is made

(Taeger/Gabel/Arning/Rothkegel, 4th edition 2022, DS-GVO

Art. 4 para. 13). This is even more the case if exclusively factual

data is linked to other personal data.

Therefore, linking the photograph to it changes the quality of the data

the pick-up order in the customer management system, since there is a connection here

of information with identification data of a natural person

becomes. In other words: at the moment when the image of the objects

assigned to the sales order and linked to it, receives that

Material date a personal reference within the meaning of Art. 4 No. 1 DS-GVO.

I have contacted the disposal company as part of the complaints procedure

process to comment and to answer various questions

regarding the fulfillment of the information obligations, for the purposes and the

Background of the procedure as well as the actual and technical

processing prompted.

In its opinion, the disposal company has the basics

and processes related to the photographic recording of bulky waste in detail

set out. In particular, it explained that the photographs of the blocking

müll's documentation purposes and used in the event of a complaint

become. They are only made in the following cases:

- if there is more bulky waste at the collection point than announced or free

can be picked up free of charge

– if there is no bulky waste at the collection point,

– if garbage that does not belong to the bulky waste collection is at the collection point.

In this regard, it was stated that after the relevant

Waste Management Statute the disposal of bulky waste only under certain conditions

Prerequisites is free:

Excerpt from the waste regulations:

"(...)

(2) Any property owner and household of to the

Land connected to waste disposal in the association

area is entitled to charge up to twice a calendar year

to request the disposal of bulky waste. (...)

(4) The total amount is limited to 2 m² per collection. (...)

(5) Only rubbish that is accepted at the time of registration will be taken away

were specified. (...)"

The photographs should therefore ensure that the statutory

according requirements are met in the context of disposal

and, should there be any inconsistencies, the garbage and the amount of garbage

can be assigned to the right person. As in the underlying

In the event of a complaint, the processing of complaints is made possible

light or relieved, e.g. B. if not (only) the bulky waste of the applicant,

but someone else's bulky waste has been disposed of or left behind.

The legal basis for data processing is Article 6 Paragraph 1 Subparagraph 1

Letter e DS-GVO into consideration.

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

(...)

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; (...)

118

General administration, municipalities

According to § 20 Para. 1 KrWG, the public waste management authorities have

the waste that has accumulated and been left in their area from private sources

Households and waste for disposal from other areas of origin

to eliminate.

The legal entities obliged to waste disposal under state law

(Municipalities, towns and districts or associations as special purpose

de) regulate according to § 1 Abs. 6 Nr. 2 HAKrWG by statute, under which

Prerequisites, in what way, at what place and at what time

they are to be left with the waste.

In the statutes of the relevant public-law pension provider

is regulated that this third party to fulfill its tasks, in particular

special private companies, of which in the present case

use has been made.

The disposal company acts when carrying out the bulky waste

consequently, in fulfillment of his obligations to the public
legal waste disposal authorities. To the citizen it appears as a so-called
administrative assistants and processes their data in connection with this
with the processing of the free bulky waste contingent thus fulfilled
public duties and therefore on the basis of Article 6 Paragraph 1 Subparagraph 1
Letter e GDPR.
Photographing the bulky waste and linking it to the collection order
therefore, under the respective conditions, constitutes a lawful data transfer
processing within the meaning of Article 6 Paragraph 1 Subsection 1 Letter e GDPR. Incorrect
the disposal company had Art. 6 in its data protection information
Paragraph 1 subparagraph 1 letter b DS-GVO (contract-related data processing)
listed as the legal basis for data processing. In this regard
I have given a notice to that effect.
The examination of the data protection information has also shown that
already explanations for the creation and linking of photographs of the
bulky waste were included. To provide the data protection information
assured the person responsible, in addition to the possibility of retrieval on the
website, upon transmission of the telephone, electronically or by post
the agreed collection date, the corresponding data protection information
to transmit. The pick-up date is sent by e-mail or
in writing by post. The establishment of an automated transmission is
initiated.
The examination of the processing processes themselves has also shown that
the technical and organizational measures in accordance with Art. 32 GDPR
ensure an adequate level of security.

Since the disposal company currently has an internal audit and

adjustment process has been initiated in the area of data protection

I, in addition to information on the legal basis and the data protection declaration,

some notes on technical improvements in data transmission,

the backup of the software on the end devices and to secure the

End devices themselves, which represent an additional optimization.

7.6

Conflicts of interest of the data protection officer in a municipality

Personnel or technical management functions and responsibility for

Relevant data processing operations in municipalities usually lead

to a conflict of interest with the function of data protection officer

within the meaning of Art. 38 Para. 6 S. 2 DS-GVO, § 7 Para. 2 S. 2 BDSG and § 7

Paragraph 2 p. 2 HDSIG.

The existence of conflicts of interest is one of the most common questions raised

asked me about the position and the tasks of the data protection officer

becomes. When appointing data protection officers, there is often the

Tendency to delegate this position to an already trusted manager.

Apparently, it is assumed here that the exercise of the function

of the data protection officer by trusted executives gently and im

in the sense of the mayor. However, such a transfer

inadmissible because the existing conflict of interest involves personal and professional

Executives and those responsible for data processing

excluded from the function of data protection officer.

In a case to be examined by me, the function of the data protection

assigned to a person who simultaneously held the functions

Main office manager with responsibility for IT system administration and

Digitization, Head of Tax and Real Estate Management, Head of

security service, IT security officer, digitization officer,

Anti-corruption officer and complaints office according to the AGG.

There was a conflict of interest within the meaning of Art. 38 Para. 6 S. 2 DS-GVO,

Section 7 (2) sentence 2 BDSG and Section 7 (2) sentence 2 HDSIG.

Although the activity of the data protection officer does not have to be exclusively

be practiced. The data protection officer can also have other functions

perceive. However, there must be no conflict of interest. When exactly

The law does not define a conflict of interest. In general is

acknowledged, however, that Data Protection Officers do not exercise any functions

which they monitor themselves in the role of data protection officer

would. Therefore, members of the top management level cannot

be a data protection officer in good time. The same applies to people who

to a significant extent for data processing in an organization

responsible or responsible.

Controls a person below senior management because of their

Function or responsibility already the content and scope of

Processing of personal data, it can be used to monitor their

own function are not used. This applies, for example, to

Those with managerial responsibility within the IT department. is recognized

a conflict of interest also for the head of the marketing department or for

Sales manager, because they are responsible for processing customer

data are. Within a commune, the management of an office, which in

processes citizen data to a significant extent, roughly comparable to

the head of a marketing department or a sales manager. Also in

In this function of a municipality, leaders are responsible for content

and extent of the processing of personal data.

All of the management functions mentioned above therefore include the function of the

data protection officer a conflict of interest. Every single one of these

Functions would already have been suitable due to the data subject

an existing conflict of interest from the function of the data protection officer

to exclude commissioners.

The functions in the representative system can also create a conflict of interest

include. The digitization officer primarily has an interest

in digitization and thus the simplified processing of personal

related data. The IT security officer is usually on

processing large amounts of personal data

interested in being able to monitor IT security. Both functions

therefore contain a conflict of interest in the function of the data protection officer

wore The same applies to the anti-corruption officer, who also

similar to a money laundering officer, involved in the processing of as many as possible

is interested in data in order to be able to identify corruption when in doubt. The three

therefore also include the aforementioned functions in the officer system

a conflict of interest with the function of data protection officer.

It was no longer necessary to check with the complaints office

there is a conflict of interest according to the AGG, as this is no longer relevant.

However, there is no obvious conflict of interest.

In the case to be processed, the municipality was referred to the existing

Conflicts of interest pointed out, an exchange of the data protection officer

However, this did not happen despite several reminders. This exchange

took place only after the municipality pursuant to Art. 58 Para. 2 Letter b DS-

GMO was warned and the local authority was called in.

8. School and colleges

school and colleges

The Hessian Ministry of Education is implementing several major digitization projects

for the Hessian schools, leading to a major digitization push

for school instruction and school communication. For this

include not only the Hessian school portal, the school administration network,

the teacher and student database, other teaching programs and the

uniform school access. This has recently also included a data protection

fair, sovereign video conferencing system (see Chapter 3.2). Also in

higher education was the establishment of data protection-compliant video conferencing

systems is an important task (see Chapter 3.3). In the reporting period

succeeded in these digitization projects in terms of data protection

to accompany and advise successfully.

8.1

Uniform access to schools (ESZ)

The digitization project "Uniform School ID" aims to provide access to

the now diverse digital tools that the Hessian cultural

Ministry (HKM) makes available, can be facilitated. For this a

established a uniform authentication procedure. The objective of the HKM

is understandable and the project makes it easier for users to access

the diverse offers. However, the data protection regulations also apply

issues to be taken into account in an appropriate manner.

The digitization offer is becoming more complex

Teachers, students, guardians and others

People and groups of people use digital offers in the school environment

different providers. This includes digital applications of land

of Hesse such as B. the Teachers and Students Database (LUSD) or the

School portal Hessen (SPH). Also offers from the school authorities such as the

Education platforms I-Serv, SchulCloud or wtk.edu are used. Added

come commercial providers such as WebUntis, which u. a. a digital one

Timetable planning or the use of digital class registers. It

So there is a wide range of digital tools used in school

used in different contexts. To these tools

to be able to use, private end devices as well as those via the digital pact

end devices procured by the school authorities.

For many accesses to the digital procedures are currently their own

Registration methods and data required. Furthermore, for the processing of

sensitive data further protective measures, such. B. a particularly safe

Registration procedure via a two-factor authentication, necessary. The-

ses is used, for example, in the official e-mail addresses for teachers

used. In addition, the HKM calls for the use of other applications

(e.g. online grade entry, individual and special needs

tion) also in terms of additional data protection measures

a strong authentication. With the project “Uniform School ID”

the integration of the various applications into a unified and

secure registration process are implemented.

Goals of the Ministry of Education

The HKM is currently implementing the "Digital School Hessen" program, in which

The aim is to achieve the following goals:

– All persons who are active in the school environment can use a uniform

Get access (school ID Hessen). This includes state, church and

School authority staff, pupils, legal guardians,

but also other persons or institutions with a school connection.

– A central access page is to be set up from which all

Applications can be reached without having to log in again (single sign-on).

- In addition, access should also be decentralized in existing procedures, such as

e.g. B. school board portals can be implemented. Here serves the

Uniform school access (ESZ or Schul-ID Hessen) as central

authentication service.

- All school systems in the state of Hesse should be accessible, but

systems of third parties (particularly the school authorities) should also be integrated

can become.

– Existing networks (e.g. the Hessian school administration network –

HSVN) are to be transformed or completely through the uniform access

be replaced.

The implementation of data protection is particularly important

challenging

The core element of the project is a uniform authentication procedure.

This results in various advantages for the users. So

are i.a. the login procedures are just as uniform as the password rules.

Passwords and authentication paths are managed centrally. for

Applications with a high protection requirement have a secure login

ready. The user name and an ID are sufficient for the registration itself.

It follows that a powerful public cloud service is chosen

had to become. That at the end of the HKM a Microsoft product (Azure) to

school and colleges

implementation was used, I came across with regard to the case law

of the ECJ (Schrems II judgment) (see 50th activity report, Chapter 3) and the

DSK's criticism of Microsoft cloud products (see Chapter 2) to strong reservations,

which I have repeated to the Minister myself. Because a judgment

technical solution that takes into account the use of micro

soft products makes it problematic if personal data is included in the

transferred to and processed in the USA or access to it from

US intelligence services insist on personally identifiable information was one

Understanding based on the chosen technical solution complex.

It was only possible because I was able to make it clear that using the

MS-Cloud can at best have a temporary character, as far as Microsoft in

not implement adjustments itself in the foreseeable future that would lead to a data protection

lead to conformity. In the other case, the migration of the logon service

to a sovereign and data protection compliant cloud in 2023.

The ministry therefore has to acquire the necessary licenses

Microsoft has chosen a very limited period of use.

The authentication procedure for the ESZ provides for the official e-mail address

resse of the teachers, who e.g. made up of first and last names,

to use. A possible use of pseudonymization methods

the teacher email addresses in the cloud service to avoid disclosure

of the real name, which I initially preferred, would have in reality

ment requires a disproportionately high amount of time

taken and the timing of a possible migration to the sovereign

Management cloud exceeded in 2023. That's why it wasn't

leader to insist on pseudonymization, even if initially

consequently appeared. Rather must now through appropriate organizational

measures are ensured

– that those affected by the data processing in an appropriate manner

informed about the service and the transmission of telemetry data

become and

- Showed the teachers the possibility of an alternative registration

becomes.

Further agreements with the HKM

I have also agreed with the ministry that I will be in regular meetings

time intervals about the desired migration procedure in a

to have the veräne management cloud informed. I also appreciate that

HKM is a future cloud provider from SAP, Arvato and Microsoft

advertised pilot project (Delos Cloud) endeavors to e.g. questions

to solve the problem of migrating data to a data protection-compliant cloud.

In addition, the HKM stands with the state state service provider

Hessian Center for Data Processing (HZD) in a regular

exchange as part of efforts to create a sovereign national cloud

to also bring cult-specific aspects into the process.

In the extensive discussions at the specialist level and abroad, I

exchange with the Minister of Education got the impression that the Ministry

my concern for a legally compliant solution, also and especially in

meaning of the teachers, can understand and supports. the realization

that the process for the most timely production of data protection

conformity has a high priority, the prerequisite for a foreseeable

safe and sovereign use of the uniform school ID.

8.2

Advice on data protection law on the Hessen school portal

The Hessen school portal (SPH) is a successful example of how digital

sovereignty can be practiced. It is remarkable that in the

SPH integrated applications basically use open source software

use comes. A part of the applications was expanded and on a

scalable cloud environment migrated to as a user-friendly platform

to be available to all Hessian schools. The HKM as the supreme

School supervisory authority and the HZD as the central IT service provider for the

The Hessian state administration works with external service providers

together who are active in the scope of the GDPR.

I already reported in my 50th activity report that I

Central consulting task in the areas of school data protection

zes, the digitization of schools and in particular the SPH (see

50th activity report, chap. 9.7). I am also responsible for this task in the year under review

complied.

The HKM has comprehensive data protection documents on the SPH

created and presented to me for a first viewing. These also included

Applications due to the ongoing digitization of schools

were newly integrated into the SPH. Based on these documents,

my first impression confirms that the SPH is a platform

acts, which can be operated in compliance with data protection.

After the documents have been handed over to my employees by the HKM

were started, a phase of comprehensive consulting services of my house

ses to the individual departments of the HKM. Both in writing

as well as in several rounds of talks, the different

school and colleges

Data protection aspects of the SPH discussed. For example, was

suggested by my employees to sign some contracts with individual departments

Contribute to the SPH for a number of years, to new legal

adapt to requirements. Another result of the deliberations was that

the submitted data protection documents in some places

are to specify the various aspects of data protection law

even more transparent to the users of the SPH like

also present to my authority. For example, in the

Role and authorization concept used categories of affected

persons to those of the main document on the data protection concept

match or to clarify the use of the global role “Employees”.

Another example is the omission within the data protection consequences

assessment the evaluation of the procedures with regard to necessity and

purpose to carry out. This is also to be done by the HKM.

A review of the IT security concept from a technical point of view allowed only

identify minor supplemental needs. It was positive to emphasize

that the HKM has already carried out an IT baseline protection check in accordance with the

protection publication series 200 of the Federal Office for Information Security

onstechnik carried out and thus an easily accessible and verifiable

method had chosen.

A next step must now be that the HKM accepts the submitted documents

gene revised according to the advice of my house, so that a

final check of the SPH can take place.

8.3

Verification of school access authorizations

school management network

Repeated complaints have prompted me in the year under review

a random sample of Hessian schools, the process of access management

direction of school management and other officials on the teachers and

Student Database (LUSD) and school administration mailboxes to

test. The test results prompted me to contact the HKM

to include a sustainable and data protection compliant change of the

process to achieve.

What the LUSD includes

The teacher and student database is a school administration procedure. The

web-based system manages student, lesson, performance and input

records of teachers, checks course enrollments through to approval for

Abitur, Hauptschule and Realschule degrees, prints certificates and delivers them

Basic data for planning and statistics. The LUSD stores the data centrally

ral at the HZD and provides the schools with a common, always up-to-date

database available.

information request

I wrote to the selected schools and asked them to

1. to send me an overview related to the LUSD from which

shows why which people have access due to which function

for the surveyed school on the LUSD. In addition, I should

of the individual schools the corresponding role and authorization

concept to be sent to the LUSD application. This one should too

include when which persons will have their access rights revoked.

2. With regard to the school administration mailboxes, the schools should

determine who has access to the individual mailboxes and why. Besides that

should also in this regard on the part of each individual school a role and

authorization concept should be transmitted, which should also include

when which persons lose their respective authorizations.

From the documents sent to me, it appears that the schools

Overview of the roles in the LUSD and also related to the school

manage administrative mailboxes. However, only one of the 26 schools was able to

present a role and authorization concept that also includes withdrawal

of authorizations guaranteed by organizational measures. One

another school has a role and authorization concept

was created on the LUSD and the school administration mailboxes

however, the withdrawal of authorizations is not regulated.

The evaluation of the documents gave the impression that many

School management and their teams do not know that role and

authorization concept, both for the LUSD and for the school administration

mailboxes, are created and maintained from a data protection point of view

must. The following quote, for example, underscores my impression

a letter from a school board:

"Because it's a little unclear to me what a role and authorization concept

should contain - in addition to the already existing distribution of rights,

which results from the respective function at the school -...".

school and colleges

A role and authorization concept is mandatory for schools

necessary

With a role and authorization concept, schools can ensure

that only those persons processed by the schools

have access to personal data who are authorized to do so. It

serves to simplify internal school organization and communication.

With such a concept, the allocation of access authorizations

easily be organized. However, it should always be noted

that only absolutely necessary access authorizations are distributed.

It is therefore imperative that the schools in Hesse in the future

full role and authorization concepts related to the LUSD like

also implement the school administration mailboxes. It would be from the perspective of

Privacy welcome if a central body, such as

the HKM as the competent technical supervisor, in this regard requirements for the

schools would impart. This could be in the form of a pattern a

role and authorization concept.

The following contents are of importance, whereby the

responsible bodies in methodological terms also based on this
laid module "Control access to data, systems and processes" of
standard data protection model:
– Based on functions within the school organization (e.g. school
management, secretariat), function-related roles must be defined that
to be implemented in the IT systems and services.
– It must be specified for each role which authorizations are used to obtain it
on the respective IT system and the IT service. One should
Orientation towards the elementary processing operations of personal
drawn data (reading, writing, deleting).
– Provision should be made as to when authorizations are granted to persons
(e.g. entry into a functional position).
– Provision must be made for when authorizations are revoked. This must
be both general (e.g. “Resignation of a teacher from the
school service”) and – if foreseeable – for specific persons (e.g.
"End of Ms. Mustermann's legal clerkship on December 31, 2022").
– It must be recorded which authorizations are assigned to which persons
are. This documentation must always be kept up to date.
– The withdrawal of authorizations is possible through organizational measures
ment (e.g. as part of an offboarding checklist that
e.g. the return of service keys is also logged). This
Specifications are to be documented in the concepts.

– If authorizations cannot be assigned to individuals

(e.g. collective mailboxes), it must be stated by name which person

group is assigned a shared role. It is to be specified as with

a change in the composition of this group of people

unauthorized further use is excluded (e.g. changing the password).

– Regular reviews and, if necessary, adjustments are part of the concepts

of these concepts to changed circumstances (e.g. new functions in

school organization or new technical configurations).

The principle of minimizing assigned authorizations is included

to consider.

– The concepts are with the date of the last made to them

change and the name of the person(s) responsible for changes

to provide.

Result

In summary, it can be stated that it is necessary for the

len a role and authorization concept both in relation to the LUSD and

also create and maintain the school administration mailboxes. From this

Reason I approached the HKM in the first half of 2022,

so that models and orientation aids for the schools on this topic can be

be worked. At the end of the reporting year, the HKM gave me a first

Submitted draft of adapted documents for the schools that stand

be coordinated between the HKM and myself by the editorial deadline.

9th Census 2022

2022 census

My employees have carried out the 2022 census in Hesse

accompanied intensively and with great effort. In doing so, it was found
that it is part of the procedures in the 33 collection points of the
state and in connection with the involvement of private companies
responsible for sending the survey documents and preparing them
no irregularities have occurred that would have affected the project
can ask.

Scope of work as part of the testing activity

To get an idea of the scope of the test and the associated
wand to get for my agency is the representation of some numerical values
helpful: It took around 18 man-days to complete the 33 Hessian
check collection points. In addition, the evaluation of the test
results about eight person days. There were also two exam dates
external service providers with locations in Baden-Württemberg and Schles-
wig Holstein. In this regard, my staff have about 6,000
kilometers covered and a large number of test reports written,
Interview notes made and written correspondence with the
audited facilities. After all, it was the Hessian
State Statistical Office (HSL) and the other supervisory authorities
practice regular exchange of experience to each other
to inform about new developments and findings. More than a dozen
Appointments for this took place in 2022.

Online-first strategy of the statistical offices

Like the 2011 census, the 2022 census was primarily one
register-based survey. In the process, the federal authorities
(e.g. Federal Agency for Cartography and Geodesy) and municipalities (e.g.
Register of residents, property tax offices) stored addresses and personal

related data are necessary for the specific statistical purpose

Data filtered out and sent to official statistics. Next to one

Survey of the approx. 2.14 million building and apartment owners in the

As part of the building and housing census (GWZ) was an additional

Household survey provided in Hesse about 850,000 people

comprised. The surveys should be carried out online if possible, which is why the

Building and apartment owners with a personal cover letter

also the access data for an online platform were mentioned, which

operated by a service provider of the Federal Statistical Office (ITZBund).

131

became. The advertising campaign for "Online-First" was evident in the episode

risen because the demand for paper-based documents in the

was significantly lower compared to the 2011 census. was in Hesse

the online rate at GWZ is 89.7%. This was shown e.g. also at

external service provider Rhenus Docs to Data, which is responsible for digitizing the

Bogen was responsible. The workload there remained below the general

new expectations.

collection points

In the 21 Hessian districts, the big cities and the towns with

Special status (e.g. Bad Homburg, Rüsselsheim) were already granted at the end of the

Year 2021 statistical offices set up. The legal basis for this was

§ 19 Census Act 2022 of November 26, 2019 (BGBl. I p. 1851 ff, last

amended by law postponing the census to 2022

of December 3, 2021, Federal Law Gazette I, p. 2675) and § 3 of the Hessian implementation

2022 Census Act of March 25, 2020 (GVBl. No. 15 p. 228).

For the establishment and operation of these bodies responsible for settlement
responsible for the household survey and the additional surveys
had to organize were from the Hessian State Statistical Office
(HSL) Minimum requirements and recommendations have been developed. The
Implementation of these requirements in terms of personnel, administrative
and organizational handling of the 2022 census was my testing interest.

Separation from other administrative units

In § 6 of the Hessian census implementation law it was regulated that the
Collection points for the duration of the processing and storage of
Individual details spatially and organizationally from other administrative
units were to be separated. This requirement was implemented by the
responsible bodies very differently. While there is a
A number of districts and municipalities announced the spatial separation
ensure the establishment of autonomous collection points (e.g. the
Cities of Darmstadt and Frankfurt, the districts of Bergstraße, Main-Kinzig or
the Werra-Meißner district), other administrative bodies were "more generous".
In the district of Groß-Gerau, the collection point was divided into three rooms "com-
primed", which were located in the facility management department. In
in another case (Main-Taunus-Kreis) the collection point was in a
housed upstream vaccination center. From the vaccination center could
you can enter the collection point unhindered. Another example: At the
City of Wiesbaden became the social space located in the survey point
the employees of the survey agency and those of the office for elections and

Statistics shared. In short, the interpretation of the legislature

The required spatial separation was partly generous.

There was no shortage of curiosities either. The city of Fulda, for example, judged

their collection point at the municipal cemetery. The building was

used by the employees of the cemetery administration; some rooms have been

assigned to the census collection agency. You could do the separation requirement

nevertheless implement it appropriately. The district of Fulda was also able to

claim a unique selling proposition for his collection point. This was

housed on the 11th floor of an administration building, which is the highest

location of the city.

Spatial accommodation

As expected and the experiences from the 2011 census

confirming that the spatial accommodation was exemplary in many cases,

on the other hand also borderline. This does not only concern matters

of data protection, but also the working conditions to which the

lifting point personnel was exposed. Considering also at least in

in the initial phase of inadequate technology it appears to a particular degree

to be difficult to meet the claims in terms of statistical

Confidentiality and temporal as well as content requirements always in the necessary

to be taken into account. Where to look for an external

Accommodation away from the actual administration had decided were

the spatial conditions and usually also the working conditions

appropriate. However, if one had decided to use the collection point

to accommodate in the town hall or in the district administration, resulted in

some cases, calamities that at least raise doubts about it

whether statistical secrecy can be guaranteed at all times

could. This applies e.g. B. for the separate visitor area or for the

Reception of the survey officers.

It was found that a large number of survey points on the visitor

area and the so-called "Communication PC" (the possibility for citizens to

survey office to enter his data online) have waived, since one

assumed that the citizens' interest in making contact would increase

locally would be limited. In almost all cases this calculation worked

on too. The contact with the survey officers also went very well

differing. Some of the survey documents were collected as part of external

Handed out training events, sometimes also to the officers

delivered or handed over at the collection point, although a separate one

Space for visitors and survey officers was not available.

HSL minimum requirements and sample documents

The HSL had a catalog of measures for setting up survey points

created, who deals with the topics of IT and information security and the establishment

and foreclosure of the collection point. Additionally were

Recommendations and advice, e.g. for regular hardware testing

at the collection point. In addition, the HSL had a model service

instruction, the model of a data protection impact assessment (DPIA) and

Examples of required records of processing activities

(VVT) that the collection agencies should use.

The service instructions, DSFA and VVT could be used as part of the tests

be submitted by all survey agencies.

The technical measures considered necessary by the statistical office for

IT and information security were also assessed by the survey agencies

largely implemented.

A comprehensive technical examination of most of the positions could

driving reasons, however, not made.

survey management and staff

According to § 4 of the implementation law, a service

management and their deputy. This important legal

Requirement was with the formal assignment of the task and order

by the mayor or the district administrator in all survey offices

been spoken. With regard to the requirement profile, it had to be guaranteed

be that the management function, insofar as this is carried out by employees from the administration

was perceived, belonged to "uncritical" administrative units.

In 2011, the legislature had expressly ruled out that

certain areas such as B. enforcement, the building authorities, the

Registration offices and the immigration authorities staff in the collection point

is used. This requirement was in the implementation law for the census

no longer included in 2022. Nevertheless, all bodies tried to staff

to use from areas of administration that the claim from the year

2011 satisfied. In a few cases was for the management function

external staff recruited.

Almost without exception, the heads of the survey offices and their

representative with competent answers. Also the submission of the documents

such as B. the appointment as a manager, the service instructions and other documents

documentation was complete with a few exceptions. A multitude of

Lines, but also the staff, some of whom are only hired temporarily

in the survey office were characterized by high commitment and a good

Also knowledgeable about data protection issues.

In some cases, collection agency staff took over as far as it was necessary

the administration recruited, temporarily also tasks of their actual

chen area of responsibility. The legislature has not ruled out

but whether this is actually in the sense of the separation requirement of census and

administration was acceptance-promoting remains to be seen.

survey officer

According to Section 20 of the Census Implementation Act, the municipalities could

Recruit survey officers (EB) to carry out the survey.

These were then active in the field of household sampling. This

initially included the "existence determination", i.e. the determination of the in

people living in a household. In a second step, a

Subset included in an extended survey. The answers could

either online (the EB then handed over the access data and identifiers

to the portal) or in writing with a questionnaire that you

received from the survey officer. According to my information I

received from the survey agencies, there was a “good online rate”.

Paper was still in demand, which was then done by the contract processor Rhenus

Docs to Data prepared in Schwarzenbek in Schleswig-Holstein, that is

has been digitized (see below).

Compared to the 2011 census, none were sent to the survey officers

Specifications regarding the exercised profession made, insofar as this in a

employment relationship. Only the EB should not be in his immediate

living environment are used. Complaints about EB went to me

only a few. However, in a few cases the reliability of the

EB not guaranteed (see below).

visitor

The survey agencies have found across the board that there are hardly any

there was visitor traffic. Quite a few survey points had

no visitors at all to report, others only in single-digit numbers. The

Spatial and technical resources stayed where they were

had made available, largely unused. Some collection points

therefore opted out of this service. As far as there is one

Respondents moved to the collection point, e.g. B.

when filling out the questionnaire with a pragmatic approach.

This finding also points to an increased online response rate.

In this respect, the experiences that were made with the census are repeated

made in 2011.

In addition, the interest of the population may be other issues

applied. War in Ukraine, inflation, energy crisis: people faced problems

who did not make the 2022 census a relevant public

let become an event.

IT and information security

In contrast to the 2011 census, the technical design of the

2022 census largely determined by a centralized approach. The

The Federal Statistical Office and its processor "ITZBund" were for

responsible for large parts of the technical processing of the 2022 census. The
The task of the federal states was therefore reduced to the specifications for the facility
and the technical operation of the collection points. The implementation of this
Specifications were then made by the cities and districts.
In connection with setting up the survey agency, the
those responsible for operation the following, non-exhaustive
to implement the requirements:
– appointment of an information security officer,
– Access control at the operating system level in the form of a user
administration and a role and authorization concept,
– Isolation of the IT systems from the rest of the administration,
– Encryption of data storage,
– no software on the IT systems that is required for the operation of the application
gene is not required
– Use of current virus scanners,
– Setting up an interface protection and
– Monitoring of the relevant IT systems.
Only a few shortcomings in implementation
As part of the test series, my employees have no serious problems
Implementation deficits identified. Occasionally there was software on the computers
installed, which was not required for the census. In one case there was none
Antivirus software on the EHU PC (PC with the survey support
programs for the census) installed. There were also survey points
who had not regularly updated the virus scanner. In
of a survey office was the location of the printer for the receipt

druck not known, as far as a person obliged to provide information uses the information PC for

intended to use his online entries at the collection point and

should receive an acknowledgment for the input made at the end. in one

other case, three printers were activated for the survey office, from

whose location was unknown.

All deficiencies were immediately turned off by the intervention of my employees.

With regard to the technical quality of the defect, it is surprising

that in particular z. B. the inadequate virus protection was not an isolated case,

but had to be ascertained repeatedly.

Census questionnaire gone astray

As part of a large census, even if a key

If a test has been carried out, data breaches are bound to occur.

Whether this concerns the loss of survey forms or the non-submission of

Records by Survey Officers: Against human error

the survey offices were not immune. In order not to give the wrong impression

awaken: Thousands of Hessian survey officers have in

in the sense of official statistics, they have done their job in an exemplary manner. To that extent

these were unfortunate isolated cases, e.g. B. in Darmstadt one

Survey officers collected the completed questionnaires in a block of flats in the

forgot to leave the house and the documents were then stolen. Or when

in Frankfurt, some survey officers did not hand in their documents and

the collection agency management had to take legal action. In all

cases known to my authority, a

proper notification of the violation of personal protection

submitted data according to Art. 33 DS-GVO.

complaints

The number of complaints (at the time of writing approx

70) was limited and slightly lower than in 2011 (about 100). in a

In many cases, the legitimacy of the census was called into question. In many

Cases concerned undelivered documents or unavailability

the hotline operated by an external service provider. also gave

there are isolated problems with survey officers who supposedly do not

could identify or with a boyish speech to the

persons required to provide information occurred. More than once my employees had to

carry out educational work by telephone in matters of the census, a task

which was actually assigned to the telephone hotline.

In a number of cases, direct contact with the competent authorities

Make the HSL workaround, especially if it is

to supposedly or actually wrong addresses of the persons obliged to provide information

acted.

As in 2011, the telephone calls made amounted to a three-digit number

in the area, but clearly did not reach the volume of 700 at the time

talks.

In summary, it can be stated that massive protests against the census,

as far as data protection issues are concerned, have not materialized.

No doubt it came in connection with the settlement of the census

in some cases to problems. Sheets not recorded, received receipts

Training documents for non-existent real estate within the framework of the GWZ or

but unreliable survey officers in the household survey: Sun

there was something on a case-by-case basis. Nevertheless, this is compared to

the total volume of more than 2.4 million building and housing

owners who wrote to them, and nearly 850,000 residents who

As part of the household survey were contacted to a low rate.

dunning procedure

In the data processing process it was planned to use a dunning procedure

lead, as far as building and apartment owners or individual households

did not comply with their statutory obligation to provide information. Both the

procedure as well as the number of those involved in such a procedure

were transferred was regulated differently in the collection agencies.

Entries could still be made in the central procedure until the end of November 2022

of the federal government. In that regard, it was required from early autumn, defaulters

Encourage respondents to submit their data by dunning procedure

transmit the official statistics. In many cases, the associated

Threat of a penalty payment successfully, so that the personal

data were still delivered. However, not a few intended

Places, dunning procedures or even a threatened penalty or fine

not enforce because of the reason for this with the end of the inputs and

the closure of the collection points on December 31, 2022.

order processing

In the 2011 census, were some supervisory authorities responsible for data

protection nor legal concerns regarding the commissioning of external

service providers, this was basically no longer an issue in 2022. In the

For the rest, the GDPR opened up leeway, which e.g. with a contract about

order processing in accordance with Article 28 (3) could be used.

For three areas, external companies were included in the official statistics

claimed:

- Telephone hotline,

– Sending of personalized questionnaires and

– Digitization of the questionnaires.

Telephone hotline

After the experiences of 2011, the interest of the statistical

schen offices great not to manage the telephone hotline themselves, but

engage an external service provider for this. The data protection law

The question was to what extent services are also provided

could, who via telephone information or the initiation of the

dispatch of questionnaires to those obliged to provide information. The

concerned i.a. the case constellation that a person obliged to provide information

gen wanted to fill out directly with the hotline employee. I have at this

Body made it clear that I do not derive from the census law for this

resulting legal basis and the statistical confidentiality

of the personal data applies. Rather, here was the HSL with a

Second level support requested to include the data.

With the service provider tricontes360 GmbH, a contact center specialist,

I have repeatedly addressed data protection aspects with regard to the

Order processing process exchanged and relevant questions

discussed the data protection concept for the census.

Personalization and dispatch of the GWZ survey forms

My employees also exchanged ideas intensively with the Ricoh

Document Center in Brackenheim near Heilbronn. The company has the
Printed sheets of the GWZ and the household survey, the sheets of the GWZ
personalized (i.e. provided with addresses) and sent. This happened
if a person obliged to provide information does not use the online procedure for answering
had chosen, but wished to receive a paper questionnaire.
Among other things, the talks were about transport encryption
the address data to be transmitted by the statistical office and their deletion
after the documents have been printed. A meeting at the company as well
the processing procedures were also checked.

139

Digitization and transmission of the questionnaires to the ITZBund
The questionnaires completed by the person obliged to provide information were sent to the
company Rhenus Docs to Data forwarded. The Processor
scanned the sheets and sent the digital copies to the ITZBund. The
Data protection issues arose with regard to the
processing of the documents after the incoming mail in the company itself.
So were the input documentation, i.e. the logging of the
Receipt of the sheets, their registration as part of the scanning process, the
encrypted transmission and the required client separation
important topics of repeated preliminary discussions. As well as the other
Rhenus was given a questionnaire to external service providers in advance
which was to be answered. In addition, my employee made his way
to Schleswig-Holstein to hold further talks on site and the
to control processing.

Ultimately, it was also about the storage and, later on, the
filing of the documents with the scan service provider. As in 2011, there were none
complaints. The census documents of the federal states were based on the
video-monitored premises in a hall separate from others there
stored documents. The destruction of the bows took over
a subsidiary under a subcontract. The documentation
this final data processing process was also exemplary
properly regulated. So there was no reason for my employee to have one
to criticize the manufacturing processes taking place in Schwarzenbek.
On the other hand, there were probably shortcomings at the ITZBund. The transmission
the data there has meanwhile stalled because the process of
Acknowledgment of receipt of the digitized questionnaires did not work.
The result was an interim transmission backlog, which the company
men but mastered.
Cooperation with the Hessian Statistical Office
Smooth cooperation with the responsible technical supervisor for
Large-scale surveys such as the 2022 census are data protection-
legal issues evident. Cooperation with the responsible
employees of the HSL was as cooperative as it was trusting. In particular
with regard to order processing, my employees were always up to date
informed. All necessary documents were available in advance
placed. Regular meetings prior to the survey were aimed at
directed to identify data protection issues and for this
to find solutions. This is not a matter of course, but in Hesse it is
established for many years.

2022 census

Cooperation with the other supervisory authorities

From the Federal Commissioner for Data Protection and Freedom of Information (BfDI)

An ad hoc working group on the 2022 census was set up.

This facility had already proven itself in 2011. The group consisting

from the federal government and the states of Hamburg, Saxony-Anhalt and Hesse,

dealt with individual statistical and data protection issues

statements, which are then submitted to the responsible federal statistics working group

and the countries were further processed and reached a decision.

The cooperation was suitable, scarce human resources

to be used in a concerted manner and for as uniform a language as possible

of the supervisory authorities to take care of the official statistics.

Preliminary conclusion

For a huge data processing project like the 2022 census, the

data protection requirements. From the cities and counties

sen these are within the scope of the operation of the collection points on a large scale

and whole implemented.

Unsurprisingly, it always came as each phase progressed

once again to complaints or inquiries that my employees

pursued. There were no serious violations. shortcomings

gen the misconduct of individual employees or had organizational

Backgrounds. This assessment applies both to the collection agency

nization, the processing of the building and apartment census as well as for

the household survey. The commissioning of external service providers led to

a higher complexity of the data processing processes and meant

a considerable increase in effort for my employees. Nevertheless succeeded

to constantly accompany the processing in this area and also to

check.

To control data processing by the federal government, i.e. in particular

the ITZ-Bund, which acts as a processor for the Federal Statistical Office

is active, however, was the responsibility of the BfDI.

A register-based procedure in the future

The census method is being further developed. The official statistics want this to be the case by 2031

gradually switched to a purely register-based procedure (register census)

in which no additional surveys are necessary. The data

should largely come from existing administrative or statistical sources

be obtained automatically. The guiding principle is the once only principle:

Citizens only have to transfer their information once

average and no longer provide information themselves for reliable census results

give. In some cases, new registers must be created for this in accordance with the relevant legislation

basis can be built up. For the building and apartment details

in the register census, for example, it is necessary to

Establishment register (GWR) as an administrative register. The GWR delivers

thus also information that politics, administration and science for their

need their own tasks.

In this project, too, data protection issues arise

be clear. To name just a few examples: The transmission of personal

Son-related data to a central register is per se with the question

connected, who has access to the databases and the updates

makes. There are also requirements regarding deletion

and logging. The supervisory authorities for data protection will

also closely monitor the process for a register census.

142

Advice to the Hessian state parliament

10th consultation of the Hessian state parliament

Advice to the Hessian state parliament

At the request of the President of the Hessian State Parliament, I advised the State

tagsverwaltung in updating the guide to data protection

the provision of personal data in parliamentary initiatives for

Members of the Hessian state parliament.

The guide is intended as a working aid for members of the Hessian state parliament

for the question of how personal data - here in particular names

men – to be dealt with if they are mentioned in parliamentary initiatives

are intended to be used and thereby end up in public materials that

are visible to the person. This guide should adapt to the amended new

Data protection law and the new data protection regulations of the Hessian

State Parliament (DSO) to be adjusted.

The starting point is § 9 Para. 1 DSO, which protects the right to information

functional self-determination of natural persons formulated the principle

that personal data is not published in parliamentary documents

and may not be dealt with in public sessions of the Landtag.

From this principle, the DSO looks to the perception of parliamentary

Tasks, however, provide certain exceptions. On the one hand, according to § 3 para. 1

No. 2 DSO allow relevant consent, personal

to name data. On the other hand, § 9 Para. 2 DSO also provides for

Exceptions exist if the state parliament's control task allows the right

on informational self-determination of the person concerned prevails. In

In this case, the provision of personal data in parliamentary

nical initiatives a balance between the right to informational

Self-determination of the person concerned and the control task of the

to do in the state legislature. Section 9 (2) provides the framework for this consideration

S. 2 No. 1 to 3 as well as Para. 3 and Para. 4 DSO. The guide gives concrete

Hints, like these abstract and value-filling exceptions

are to be understood in typical cases.

In particular for the balancing of the control task of the state parliament

and the right to informational self-determination of the data subject

the guide provides information for MEPs:

According to § 9 Para. 2 S. 2 No. 3 DSO, persons of the

are mentioned in public life if their public work is affected

is. A consideration of their right to informational self-determination

is not required in this case. are public figures

in particular political mandate holders (e.g. Bundestag and state parliament

Orderly, members of the district council, city councillors), officials (e.g.

ministers, state secretaries, mayors) as well as people from contemporary history

(e.g. King Charles III, Nobel Prize winner, Olympic champion).

If these requirements are not met or if there are any doubts,

according to § 9 para. 2 sentence 2 no. 1 DSO, you are entitled to be named

waive. If personal characteristics to deal with the facts

are required, the function, service or professional title of the

person concerned and, if necessary, the surname

abbreviated (e.g. President B., Prosecutor A.).

If, according to § 9 Para. 2 S. 2 No. 2 DSO, a treatment of the facts

only be possible by stating the name and data of the person and

the interests of that person would be material through a public discussion

affected, the facts should be discussed in a non-public meeting

committee or working group.

According to § 9 para. 4 DSO, data of a data subject can be

a significant impairment of their interests, exceptionally public

discussed when parliamentary control requires it. This

is z. B. in a final report of a committee of inquiry or

the parliamentary debate on this conceivable, which is based on this

concrete person decisively arrives.

The decision on the form of parliamentary treatment as well

the publication of names in parliamentary initiatives meets in

disputed cases, the President.

144

Employee data protection

11. Employee data protection

Employee data protection

The conditions of data protection for employees are being massively enforced

the digitization of working life, the virtualization of work contacts

and work processes and the spread of smart devices as work tools

or changed in the work environment. This allows behavior and

to record the performance of employees more easily, more deeply and more comprehensively

(on camera surveillance chapter 11.2). At the latest through this is a comprehensive
Send regulation of employee data protection overdue (chapter 11.1).
Also in the run-up to the application or employment relationship
Processing operations for data of potential employees take place (Section 11.3).

11.1
Changes in employee data protection

The advancing digitization of the working world is changing the conditions
genes of personal rights protection in the employment relationship. Through
an IT-supported organization and performance of the work fall
more and more and more precise personal data of employees
at. At the same time, algorithm-based decision support
tion systems (AI) new possibilities of data analysis and thus easier,
deeper and more comprehensive controls of employees. It is time,
to regulate employee data protection in a new and comprehensive manner.
In 2009, against the background of the data scandals of a number of large
company for the first time an independent regulation on employee data
created protection (§ 32 BDSG old version). At that time it was already clear
the legislator aware that the employee data protection law
requires further development (BT-Drs. 16/13657, 20). Despite a declaration of intent
ments in coalition agreements, legislative initiatives and the possibility of
New regulation in connection with the entry into force of the GDPR in 2018
- the regulation on employee data protection exists as § 26 BDSG bis
largely continued today without any major changes to the content.

§ 26 BDSG

(1) Personal 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. In order to uncover criminal offences, personal

Employee data is only processed if actual facts to be documented

evidence justify the suspicion that the person concerned in the employment

has committed a criminal offense, the processing is necessary for detection

and the legitimate interest of the employee in the exclusion of

Processing does not predominate, in particular the type and extent with regard to the occasion

are not disproportionate.

(2) Is the processing of personal data of employees based on

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

or the dependency of the employed person in the employment relationship

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

In particular, voluntariness can exist if the employed person has a legal

cher or economic advantage is achieved or employer and employed person

pursue similar interests. Consent must be in writing or electronically

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

The employer has informed the employee about the purpose of the data processing and

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

to clear up.

(3) Deviating 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
outweighs the exclusion of processing. Paragraph 2 also applies to consent to the
Processing of special categories of personal data; the consent must
expressly refer to this data. Section 22 paragraph 2 applies accordingly.
(4) The processing of personal data, including special categories
personal data of employees for employment purposes,
is permitted on the basis of collective agreements. The negotiating
partner Article 88 paragraph 2 of Regulation (EU) 2016/679.
(5) The controller must take appropriate measures to ensure that
in particular the principles set out in Article 5 of Regulation (EU) 2016/679 for
the processing of personal data is complied with.
(...)
ECJ proposal on the provisions of employee data protection
This could possibly change soon as the question of Union
legal conformity of the almost identically worded Hessian regulation for
employment data protection, § 23 HDSIG, the ECJ in case C-34/21
currently available for examination. The decision of the ECJ will therefore not
not only affect § 23 HDSIG, but also § 26 BDSG.
146
Employee data protection
§ 23 HDSIG
(1) Personal data of employees may be used for employment

be processed if this is necessary for the decision on the justification of a
Employment relationship or after establishing the employment relationship for
its implementation, termination or processing as well as for the implementation of internal work
planning, organizational, social and personnel measures is required. This
shall also apply to the exercise or fulfillment of obligations arising from a law or a collective agreement,
rights resulting from a company or service agreement (collective agreement).
and duties of employee representation. To detect criminal offenses
personal data of employees may only be processed if
documented factual indications justify the suspicion that the affected
ne person in the employment relationship has committed a criminal offense, the processing for
disclosure is required and the legitimate interest of the employee
does not outweigh the exclusion of processing, in particular the nature and extent of
are not disproportionate to the occasion.
(2) Is the processing of personal data of employees based on
of consent, for the assessment of the voluntary nature of the consent, in particular
or the dependency of the employed person in the employment relationship
as well as the circumstances under which the consent was given.
Voluntariness can exist in particular if a legal
or economic advantage is achieved or employer or employer and employees
person pursue similar interests. The consent must be in writing, insofar as
another form is not appropriate due to special circumstances. The servant or
Employer informed the employee about the purpose of the data processing and about her
To clarify the right of withdrawal according to Art. 7 Para. 3 of Regulation (EU) No. 2016/679 in text form.
(3) Deviating from Art. 9 Para. 1 of Regulation (EU) No. 2016/679 is the processing
special categories of personal data within the meaning of Art. 9 Para. 1 of the Ordinance
Regulation (EU) No. 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

outweighs the exclusion of processing. Paragraph 2 also applies to consent to the

Processing of special categories of personal data; the consent must

expressly refer to this data. § 20 paragraph 2 applies accordingly.

(4) The processing of personal data, including special categories of personal

personal data of employees for employment purposes

permitted on the basis of collective agreements. The negotiating

partner Art. 88 Para. 2 of Regulation (EU) No. 2016/679.

(5) The controller must take appropriate measures to ensure that

in particular the principles set out in Article 5 of Regulation (EU) No. 2016/679 for

the processing of personal data is complied with.

(...)

147

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

This was preceded by the order for reference by the VG Wiesbaden of 21

December 2020 (23 K 1360/20.WI.PV, ZD 2021, 393) a legal dispute between

the main staff council for teachers and the Hessian

Ministry of Education on the question of whether the introduction of a live stream company

courtesy of the consent of the respective teacher through video conferencing systems

required or whether the data processing that takes place here is based on Section 23 (1) sentence 1

HDSIG is covered.

The Administrative Court of Wiesbaden expressed doubts in its order for reference

because Section 23 (1) sentence 1 HDSIG is a more specific one

Regulation within the meaning of the opening clause of Art. 88 Para. 1 and Para. 2

GDPR acts. On the other hand, the court had concerns as to whether the provisions in § 23

Para. 5 HDSIG contained regulation, according to which the person responsible suitable

must take measures to ensure that, in particular, the

Art. 5 of the GDPR set out principles for the processing of personal

related data are complied with, adequate implementation of the

Art. 88 Para. 2 GDPR.

Art. 88 GDPR

(1) Member States may through legislation or through collective agreements

more specific rules to ensure the protection of rights and freedoms across

regarding the processing of personal employee data in the context of employment,

in particular for the purpose of hiring, including the fulfillment of the employment contract

the fulfillment of obligations stipulated by law or by collective agreements

Duties, management, planning and organization of work, equality

and diversity in the workplace, occupational health and safety, protection

the property of employers or customers and for the purposes of claims

individual or collective rights related to employment and

Provide benefits and for termination of employment purposes.

(2) These provisions include appropriate and special measures to safeguard the

human dignity, legitimate interests and fundamental rights of those concerned

Person, in particular with regard to the transparency of processing, the transmission

personal data within a group of companies or a group of

companies engaged in joint economic activity and the surveillance

systems in the workplace.

(...)

The decision of the ECJ stands at the end of the reporting period

still pending, both the European Commission and the Advocate General

but have already agreed with the opinion of the VG Wiesbaden

and expressed that Section 23 HDSIG does not meet the requirements of

opening clause of Art. 88 Para. 1 DS-GVO, since it is - in relation

to the regulations of the DS-GVO - not to specifying national ones

148

Employee data protection

Regulations act and the reference in § 23 Para. 5 HDSIG and § 26 Para. 5

BDSG no adequate implementation of "special measures" in mind

of Art. 88 (2) GDPR (opinion of the Advocate General of 22

September 2022 in Case C-34/21, paragraphs 58, 72, 75).

New regulations on employee data protection

It is therefore to be welcomed that the federal government in its coalition agreement

has already announced that “regulations on employee data protection

create in order to achieve legal clarity for employers and employees

and to protect personal rights effectively" (coalition agreement between

SPD, Bündnis90/Die Grünen and FDP, 20th legislative period, p. 17).

The DSK has also been calling for legal standards for several years

the employment relationship (DSK resolution of March 27, 2014

"Employee data protection now!" and from April 29, 2022 "The time for a

Employee Data Protection Act is "Now"!", https://www.datenschutzkon-

ferenz-online.de/entschlussungen.html).

As far as possible new regulations for employee data protection are concerned,

Is it therefore convenient that in the last legislative period

de by the Federal Ministry of Labor and Social Affairs (BMAS) with the

Advisory Council on employee data protection convened an expert commission

was to provide recommendations for action on the question of the need for a
to develop an independent law on employee data protection and
to examine initial content-related proposals for such a law. The Advisory Board
published its report on employee data protection in January 2022
(https://www.denkfabrik-bmas.de/focus/beschaeftendatenschutz/
report-of-the-independent-interdisciplinary-advisory-board-on-employees-
data protection).
He comes to the conclusion that the general clause-like regulation
of § 26 BDSG often no accurate statements about the admissibility
of specific processing in the employment relationship, but
leave this up to the case-by-case analysis of the courts, and demands concrete
regulations (report of the advisory board on employee data protection
from January 17, 2022, p. 5, https://www.denkfabrik-bmas.de/focus/
employee data protection/report-of-the-independent-interdisciplinary-
ren-advisory-board-on-employee-data-protection).
According to the DSK, § 26 BDSG is not sufficiently practicable,
clear and appropriate (statement of the DSK on the evaluation of the
Federal Data Protection Act of March 2, 2021, p. 8, https://www.datenschutzkonferenz-online.de/
statements.html) and therefore lists both employer and
Employee side on legal uncertainties ("The time for an employee

Data Protection Act is "Now!", 1 https://www.datenschutzkonferenz-online.
de/resolutions.html).
First suggestions for the content design

Both the advisory board for employee data protection and the DSK give
first indications of possible regulatory complexes of a new employment
tendatenschutzgesetzes and show parallels, e.g. B. what
the need to clarify employee data protection law
essential guiding principles of the design of any regulations and the
pertains to regulatory complexes that are mandatory in terms of substantive law.
In addition, the German Trade Union Confederation will have its own in February 2022
Draft on employee data protection submitted (https://www.dgb.de/uber-
us/dgb-heute/recht/++co++82a3178c-88c4-11ec-b434-001a4a160123).
Because in the area of employee data protection I have to deal with a large number of
Inquiries and complaints are reached, I stand by any new regulation
regulation of employee data protection law in Hesse will be happy to provide advice
available.

11.2

Driver surveillance by cameras

Permanent performance and behavior controls of employees
Potential for significant violations of data protection law and are
moderately unlawful. This also applies to the monitoring of female drivers
and drivers of a haulage company through dashcams. Filming in particular
of the driver by one aligned in the driver's cabin
Camera has to stop.

complaints from employees

I received several anonymous complaints from drivers
a forwarding agent. The employees stated that during their work
so-called "dashcams" to be monitored. This is it
video cameras that are installed in or on the vehicle and that

record driving events. The recordings created are about

Clarification of the course of traffic accidents and as evidence in court

procedure used.

In their complaints, the employees stated that the dash cams

had two camera angles, one of which showed traffic

hen filmed on the street (outdoor) and the other shots of

employees in the driver's cabin (interior).

150

Employee data protection

I took the complaints as an opportunity to contact those responsible

to hear about the processing procedure. It turned out that the

information provided by the employees was correct. My investigations

that the records made are kept for a period of 60 days without cause

Hours were stored in a closed system (so-called

ring memory). On certain occasions such as B. sudden steering,

hard braking, failing to notice traffic signs, or being distracted

Drivers of more than four seconds - were out of the

Records of the ring memory automatically creates video clips and in

uploaded to a cloud. A certain group of people in the forwarding agency had

then the opportunity to view the created video clips. The video clips

were in the cloud instance for a period of up to six months

saved.

To justify the data processing procedure, the data subjects should

sign a consent form but did not have the opportunity to do so

to reject, but only to "revoke" them. The explanation was how

follows (excerpt):

"I agree that the with the installed in the company vehicle

Combined dash cam with personal recordings related to events

Data of my person, in the context of the prosecution of criminal offenses or

Administrative offenses, in compliance with the General Data Protection Regulation

Regulation (DS-GVO) of the Federal and Hessian Data Protection Act

(BDSG and HessDSG) to authorized third parties (these were specifically

called) are transmitted.

I have also been informed that the use of my

data on a voluntary basis. Furthermore, that I give this consent

revoked at any time in accordance with Art. 7 DS-GVO with effect for the future

can call. I address my declaration of revocation to (Here was the

E-mail address of the data protection officer of the person responsible

called). I hereby declare that I am in this way of proceeding

of my own free will."

At the time the informed consent was presented to the workers

was installed, the cameras had already been installed and put into operation.

In addition to the consent, the person responsible asserted that the vi-

deomonitoring of traffic on the one hand as a countermeasure

me with regard to self-inflicted accidents of employees and

on the other hand, to collect evidence in the event of accidents caused by third parties.

Consent?

The principle of the lawfulness of data processing from Art. 5 Para. 1

Letter a DS-GVO in connection with Art. 6 DS-GVO requires for the legal

compliance with data processing has a legal basis or consent

of those affected.

Art. 88 DS-GVO provides for the area of employee data protection

opening clause, which enables the member states to

to issue regulations for the area of employee data protection.

With the provision of § 26 BDSG, the legislature has this possibility

made use of. In principle, according to Section 26 (2) BDSG (see Chapter 11.1)

consent to data processing also in the employment relationship

legitimize; However, this is only possible under very narrow conditions:

The data processing as part of the camera surveillance was not completed

a consent corresponding to the requirements of § 26 Para. 2 BDSG

justified. Because when assessing the voluntariness of consent

comes to the circumstance of the agreements existing in the employment relationship

pendency (so-called over-subordination relationship) is of particular importance.

For a voluntary and therefore effective consent, a

lawful alternative behavior (e.g. the refusal of data processing

procedure) be possible, so that the persons concerned have a genuine electoral

have possibility. In the case to be assessed, the cameras were already there

installed in the vehicles before the workers even had an opportunity

had to "consent" to the data processing procedure. The affected

Drivers were thus faced with a fait accompli from the start

asked. However, effective consent was due to the lack of voluntariness

not subject to consent.

After my hearing and the indication that the submitted declaration of consent

clarification did not meet the requirements of Section 26 (2) BDSG, appealed

controllers no longer rely on consent as a legal basis,

but on § 26 paragraph 1 sentence 1 BDSG (see Chapter 11.1).

Need for employment?

However, the monitoring of the employees was also not in accordance with Section 26 (1).

S. 1 BDSG lawful. According to § 26 paragraph 1 sentence 1 BDSG, personal

data collected from employees for the purposes of the employment relationship

processed if this is necessary for the decision on the justification

of an employment relationship or after establishing the employment

tenancy is necessary for its implementation or termination.

152

Employee data protection

The interests of the employer are included in the necessity test

and to weigh up and protect the interests of employees that are worthy of protection

to bring a balance between the two interests as far as possible

is fair (practical concordance).

This requires an examination based on the proportionality

principle, which in turn requires that on the part of the person responsible

a legitimate purpose is being pursued, the processing procedure for the

for the realization of this purpose, and it is the mildest of all

equally effective means available. In addition, must

it may also be reasonable after considering the circumstances of the individual case.

An open video surveillance is thus according to § 26 Abs. 1 S. 1 BDSG as

Measure within the framework of the implementation of the employment relationship

permissible if the purpose of the data processing is based on the

departure, implementation or termination of the employment relationship

is directed and the requirements of the principle of proportionality

is equivalent to.

Insofar as monitoring the driving behavior of the employees themselves

Accidents at fault are to be avoided is a nationwide one

built-in video surveillance not required. Even if accepted

is that the video surveillance has a legitimate purpose in mind

of § 26 Para. 1 S. 1 BDSG, and it is assumed that this is the case

is an appropriate measure, come at least comparable

consider effective, milder measures, such as implementing re-

Gel-like sensitization or training measures for those affected

drivers.

It must also be taken into account that the indiscriminate installation in the

Vehicles of all employees, also taking into account the circumstances of the

individual case is inappropriate. Here would be a distinction regarding the

Accident propensity of the employees in the past necessary, so that

if necessary only the drivers the camera system

for outdoor use is installed in your vehicle, which is already increasing

were involved in accidents that were their fault.

Filming the interior of the driver's cab - i. H. the manufacture of

Recordings of employees - cannot be justified under data protection law

and constitutes a material breach of the provisions of the

data protection law on the part of the person responsible.

The video surveillance of the interior of the driver's cab is

is a performance and behavior control of the employees

which creates a permanent monitoring pressure. Because those affected have to

expect that every behavior can be monitored (cf. BAG:

Open video surveillance - Evidence prohibition and admissibility

of data collection, NZA 2019, 1212). Gestures and facial expressions, conscious or

unconscious gestures, the facial expression at work or when

Communicating with superiors or colleagues is subject to the

Possibility of documented observation, so that there is pressure to

to behave as inconspicuously as possible at all times (cf. BAG: video recordings on

Workplace - general personality rights of employees - principle

of proportionality, NZA 2004, 1278). Such an intense intervention in

the personality right in the form of a full control is data protection law

inadmissible.

memory limit?

Automatic storage of all recordings for a duration of 60

Hours also violates the principle of storage limitation

of Art. 5 Para. 1 Letter e GDPR. Thereafter, a personal reference may only

be allowed for as long as is necessary for the purposes of data processing

is required. If the data is no longer required for this purpose,

the person responsible is therefore obliged to delete them immediately. This

arises, concretizing the principle of memory limitation

Art. 17 DS-GVO (see short paper no. 11 of the DSK on the right to deletion,

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf).

It is true that with regard to the proof of the course of a traffic accident

note that video recording is an effective means of reconnaissance

of a fact (cf. Balzer/Nugel, mini cameras in street

verkehr – data protection law limits and civil procedural exploitation

availability of the video recordings, NJW 2014, 1622). However, just at

accidents caused by third parties, the driving behavior of drivers

recorded without the record being associated with any

specific misconduct. Such an encroachment on personal rights

which arises without suspicion and without cause by the persons concerned

a high level of intensity (cf. Balzer/Nugel, mini cameras in road traffic

– Limits under data protection law and usability in civil proceedings

video recordings, NJW 2014, 1622).

A permanent, unrelated recording of traffic events

contrary to data protection (cf. DSK position paper on the inadmissibility of vi-

deodorant monitoring from vehicles (so-called dashcams) from January 28, 2019,

https://www.datenschutzkonferenz-online.de/media/oh/20190128_oh_posi-

tion paper_dashcam.pdf).

154

Employee data protection

This intervention intensity can be reduced by using ring memory

The video recordings made at fixed periodic intervals

delete and save only those video recordings in which certain

Prerequisites - such as the triggering of a vibration

sensors during heavy braking - are given.

With regard to the intervention-reducing effect, the duration of the regular

Recording in the ring memory and the concrete triggering of the sustainable

Storage in the cloud instance must be observed (cf. Starnecker, in: Gola/

Heckmann, GDPR/BDSG, 3rd edition 2022, BDSG § 4 paras. 47-51).

It must also be taken into account that the interest of the person recording

regarding the gathering of evidence solely on the record of

direct accident events (cf. Giesen, dashcam recording

taking part in civil proceedings, NZV 2020, 70). Thus, usually only
Recordings immediately before, during and shortly after the accident
to be considered necessary (cf. BGH, dashcam recordings as evidence
in the accident liability process, NJW 2018, 2883).
The record made by the responsible person with a
Ring memory with a periodic recording of 60 hours was sufficient
did not meet these requirements and therefore also violated the principle
the storage limitation of Article 5 Paragraph 1 Letter e, Article 17 Paragraph 1 Letter a
GDPR.
This also applies to the storage of the video clips uploaded to the cloud
for a period of up to six months. Will data be used for the purpose of
Data processing is no longer required, the person responsible is obliged
delete them immediately. This is for created video recordings
the case if e.g. B. a preservation of evidence is no longer necessary. If
such an event existed can, in principle, be determined within one to
clarify two working days. Orientation is also recommended here
the maximum storage period of 72 hours (cf. DSK, orientation guide
Video surveillance by non-public bodies, p. 22f., https://www.da-
tenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf).
Longer storage intervals would only be permitted if criminal offenses or
Significant breaches of duty are only discovered during extensive checks
can become. In the case to be assessed, such a situation did not exist
given.
Data Protection Response
The identified violations require action to be taken
Art. 58 Para. 2 DS-GVO Due to the identified violations would be next

a fine procedure measures according to Art. 58 Para. 2 Letter f DS-GVO

in the form of a prohibition order. After my

hearing and based on my legal statements, the responsibility

literal the system meanwhile no longer. Therefore, the judiciary

my authority is now examining the initiation of fine proceedings.

11.3

Active sourcing to attract applicants

Under active recruitment (Active Sourcing) is the targeted search

by employers or personnel service providers for suitable female candidates

or candidates on the Internet and how to address them personally

the. Professionally oriented networks, websites, applicant data or also

Search engine queries – the sources for collecting personal

Data on the Internet is diverse. Active sourcing may be allowed if

the data subject has apparently made their data public.

At the beginning of the reporting period, one complainant contacted me

the request for a data protection check and evaluation in connection

hang with the contact of a personnel service provider to me. The

Recruiting company was sent to the person concerned by e-mail with analogy

received the following message:

"Dear Madam, dear Sir,

We hereby inform you in accordance with Art. 13 or Art. 14 of the data protection

basic regulation (DSGVO) that we use your personal data

included in our database. We have your data out

social media or a public database.

We are a personnel service provider (...). Chat for this purpose

we have a database of potential candidates,

which is constantly being updated and expanded to include employees for our

to find customers. Your data will be processed within our company

processed. A disclosure of personal data

does not take place, unless it is a question of specific projects

which we will inform you in advance. The legal basis for this

processing is our legitimate interest (Art. 6 Para. (1) f) GDPR)

in the mediation to our customers.

The person responsible within the meaning of the GDPR is (...)

Contact our data protection officer (...)

156

Employee data protection

You have the right to object to the processing (Art. 21 DS-

GMO). Your other rights and detailed information about ours

Data processing can be found in the data protection declaration on our

Website: www.(...).de/datenschutz.

Best regards"

The person concerned had thus been informed that their personal

transferred data for the purpose of recruitment in the database of

company have been included. The e-mail also contained

send the personnel service provider the contact details of the person responsible and

of the data protection officer and the person concerned was informed of their objection

correctly pointed out.

Due to the complaint of those affected, I have the responsible

affiliated with recruitment agencies. In my hearing I have
asked where the data of those affected came from and how
company had become aware of them. The person in charge led
at my hearing extensively, explained his field of activity and
the process of collecting and storing potential candidates
Candidates in your own database. Regarding the data processing
events surrounding the complainant explained the personnel service
ter that he was due to a specific customer vacancy according to the required
Qualifications via the Google search engine for suitable
I was looking for didatinnen and candidates. Here is a hit for a
Website operated by the complainant with a professional context
been achieved. From this website are then the personal
Data of the persons concerned collected and in the database of the recruiter
been saved.
Art. 5 para. 1 letters a to f DS-GVO contains the principles for the processing
processing of personal data and clarifies in paragraph 2 that the processing
responsible for compliance (“accountability”).
According to Art. 5 Para. 1 Letter a DS-GVO, personal data must be
lawfully, in good faith and in a manner appropriate to the
be processed in a comprehensible manner ("lawfulness,
Fair processing, transparency”). Overlooking the through
my authority to assess the facts was against this background
on the one hand to check whether the data processing by the HR
medium can be based on a legal basis, and on the other hand,
whether the information requirements of Art. 14 DS-GVO have been observed and that
The responsible person's actions were therefore sufficiently transparent.

Legal basis for the processing of personal data

Data

Regarding the legal basis for the processing of personal

With regard to the data of those affected, it seems obvious that the provision of § 26

Para. 1 sentence 1 BDSG (see Chapter 11.1). According to this, personal

related data will be processed in the application phase if this

for the decision on the establishment of an employment relationship

what is required. With active sourcing, however, it should be noted that

the person addressed does not take part in any application process and

therefore not yet an applicant. It is the Active

Rather, sourcing is something that precedes the application process

Procedure. The scope of § 26 paragraph 1 sentence 1 BDSG is therefore

neither in a personal nor in a factual respect.

With regard to the lawfulness of the processing, it was therefore necessary to check whether a

of the conditions specified in Article 6 Paragraph 1 Subsection 1 Letters a to f GDPR

applies. My examination showed that as the legal basis for the

processing of the complainant's personal data

overriding legitimate interest of the person responsible in the provision

its personnel placement service, thus Art. 6 Para. 1 Subparagraph 1

Letter f DS-GVO, comes into consideration.

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

(...)

f) The processing is to protect the legitimate interests of the person responsible

or a third party, unless the interests or fundamental rights and

Fundamental freedoms of the data subject, the protection of personal data

require, predominate (…).

According to Recital 47 GDPR, the lawfulness of the processing

tion by the legitimate interests of a controller to which

an economic interest also counts, must be justified. the sensible ones

Expectations of the data subject must be taken into account. It is closed

check whether a data subject at the time the personal

personal data and given the circumstances in which it occurs,

can reasonably foresee that there may be processing for

this purpose will be done.

158

Employee data protection

The starting point for any weighing of interests within the framework of Art. 6 Para. 1

Subsection 1 letter f DS-GVO are on the one hand the personal rights of the

affected and the effects of processing the data in question

data for this entails, and on the other hand the interests of the

responsible (cf. BGH judgment of June 23, 2009 - VI ZR 196/08, NJW 2009,

2888). When weighing up the interests, it was particularly important to consider

that the person concerned stores their personal data on one of their

made a professionally oriented website publicly available. She

had thus restricted its claim for protection through its own actions.

Data are made public if they are accessible to an indefinite

number of people without significant admission barriers

(Schulz in Gola/Heckmann, DS-GVO, 3rd edition 2022, Art. 9 para. 33). Public made data can be found, for example, in freely accessible data areas of the Internet, on your own website or in opinion forums. It is crucial that the data is freely accessible without restrictions not only made accessible within a closed group. Even if the stored data includes special categories of personal collected data (e.g. ethnic origin, political opinions, ideological beliefs or union membership) contained, would be the prohibition according to Art. 9 Para. 1 DS-GVO, such data process, according to Art. 9 Para. 2 Letter e DS-GVO, if it is the processing of publicly disclosed personal data.

Art. 9 GDPR

(1) The processing of personal data revealing racial and ethnic Origin, political opinions, religious or philosophical beliefs or the trade union membership and the processing of genetic data (...) of a natural person is prohibited.

(2) Paragraph 1 does not apply in the following cases:

(...)

e) The processing relates to personal data that the data subject obviously made public.

Contains a regulation comparable to Art. 9 Para. 2 Letter e GDPR Article 6 GDPR does not. But if Art. 9 Para. 2 Letter e DS-GVO a Exception to the processing ban for those in need of special protection Data categories of Art. 9 Para. 1 DS-GVO, this must be a fortiori for Personal data apply that are subject to the requirements of Art. 6 GDPR can be processed. The personnel service provider could

Processing of the personal data of the persons concerned is therefore based on Art. 6

Paragraph 1 subparagraph 1 letter f GDPR, possibly in connection with Article 9 Paragraph 2

Letter e DS-GVO, support. Anyone who has their own professionally oriented website

te operates must expect that the data provided by

potentially interested employers or recruiters for purposes

a possible staffing or recruitment service

be used.

Compliance with the information obligations according to Art. 14 DS-GVO

Also a significant violation of the in Art. 5 Para. 1 Letter a DS-GVO

contained principle of transparency, which i.a. through the information obligation

of Art. 14 GDPR is specified, was not given. Art. 14 GDPR

obliges those responsible to inform the data subject if the

personal data were not collected from the data subject.

This is the case with active sourcing, since the personal data -

as in the underlying case - not with the data subject himself,

but collected from another source.

Article 14 of the GDPR includes, among other things the obligation to provide information about the stored

th personal data, the legal basis of the processing, the

Contact details of the data protection officer, the purposes of data processing

tion, the duration of storage, a list of the rights of those affected,

the existence of a right of appeal and the source from which the data

come. In the case to be examined here, the information obligations were

observed. There was no information about the exact origin of the data.

The data source was informed of my request.

Summary and further information for practice

The case shows that Active Sourcing, in accordance with the provisions

data protection can take place. As the legal basis for data processing

Article 6 paragraph 1 subparagraph 1 letter f GDPR applies in particular to the processing

consideration; the regulations on employee data protection, on the other hand, can be found

no use.

If those responsible for data processing are based on Article 6 Paragraph 1 Subparagraph 1

letter f DS-GVO, it is mandatory to carry out a weighing of interests

to lead. It should be particularly relevant here whether potential candidates

and candidates their personal data for professional purposes

have made generally available. The considerations also apply to

job-oriented networks, provided the users concerned

not make use of the possibility of privacy settings,

so that your personal data is generally accessible (Göpfert/

160

Employee data protection

Dußmann, Recruiting and headhunting in the digital world of work - Her-

challenges in labor law practice, NZA supplement 2016, 41, 43).

However, has data access been restricted to contacts with whom the

data subject is "networked", the balancing of interests can only be

In favor of the person responsible if he is already at the

"Contact request" as a recruiter or recruiter and on the

potential data processing. Otherwise the data processing

also inadmissible for work-related social networks, since the data

are not "generally" accessible (excerpt from ArbR Aktuell 2017, 185). The

Processing of personal data collected on a website or in

published on a social network for social communication

and have a private character, on the other hand, constitutes a violation of the

personal rights (cf. Gola, The Internet as a source of applicant data,

NZA 2019, 654).

When recording the personal data of a possible applicant

bers or an applicant in the database of a personnel service provider

meet the information requirements described above in accordance with Art. 14

GDPR. Of particular importance is the reference to the

Right of objection (paragraph 2 letter c) and naming of the source (paragraph 2

Letter f) to. If it is not possible to name the specific source, what

standardized data protection information should be the rule

the specific source of the survey, at least upon request from the person concerned

can be named. Those responsible must therefore

Take precautions (see also the

Guidelines for transparency according to Regulation 2016/679, WP 260 rev. 01

the Article 29 Working Party).

The right of objection, which pursuant to Article 14 (2) (c) GDPR

Art. 21 DS-GVO regulates that information must be provided when it is included in the database.

The right to object to data processing for the purpose

of recruitment can be exercised at any time, whereby the in

Para. 1 justification required not to make any special requirements

are. Rather, the contradiction in an overall view with Art. 6 para. 1

Paragraph 1 letter f DS-GVO to be considered. Expresses an affected person

an opposing interest, the intended purpose of the personal

nal mediation can no longer be reached.

web, advertising

12. Internet, Advertising

web, advertising

The importance of the internet for social coexistence

economic activity and the fulfillment of administrative tasks

is becoming more and more important. This applies not only to the virtual world created by the

Internet came into being, but through the Internet of Things also for the

physical world. In principle, every activity in both worlds can be digital

be recorded and evaluated. This increases the importance of data protection

zes increasing. Very many providers of sites on the WWW record user

data and create user profiles from it (chap. 12.1). In an even stronger way

This is done to a certain extent by providers of digital platforms such as e.g. Facebook

(Chap. 12.2). The profile data is used for advertising on the web, but also for advertising

exercise by e-mail (chap. 12.3 to 12.5). A form of the Internet of

Things are voice assistants that pose particular risks when they

in business premises (Section 12.6). Many traders in

enable or even require the establishment of online accounts,

through which they want to conduct business relationships. This creates

There are also often unnecessary data protection risks (Section 12.7). The operation of each

Web page leads to the processing of personal data. Not everyone

However, the operator is aware that this is associated with information obligations for him

is (Chap. 12.8).

12.1

And the user profile greets you every day – data protection for online services

For many people, the term data protection is closely linked to usage

of internet and telemedia services such as e.g. B. websites, online portals,

Apps or smart devices. Achieve a corresponding number of complaints

me to. The providers of such services process personal data

Data of the users in different constellations, goes particularly frequently

It is about the creation of user profiles and the mostly required

common cookies.

The day-to-day use of Internet services has long since gone beyond the "classic"

Surfing out on websites. All internet-connected devices

such as B. Smartphones, Smart TV or intelligent household appliances

such as B. heating thermostats connected to the WLAN are based on so-called

telemedia services. That data is collected when using such services

and processed, which are necessary for the provision of the respective service

are generally recognizable and understandable for the user. Who

want to find out the cheapest travel connection with an app

In addition, information about start and destination, travel time and, if necessary, for pricing

relevant factors such as one's own age.

In addition, almost all such services also

Background data is collected that is not relevant to the actual purpose of the respective

Service are required and their processing for the users mostly only

is difficult to recognize. Many service providers collect analysis data in order to

find out exactly how users use their services. Based

This data allows them to tailor their services to the needs of users

and adapt to their own business interests and example

Information or functions that users search for particularly frequently or

use, identify and place more prominently within an app.

Especially relevant is the collection of data for the creation of

User profiles to focus on the personal interests of the respective user

to place tailored advertising. Personalized advertising is

ubiquitous on the Internet, since it generates greater profits than with

non-personalized ads and a significant part of the Internet

services financed in whole or in part via this business model.

As a rule, the providers of websites, apps or others collect data

Internet services do not process user data for these purposes themselves, but

are used by specialized service providers whose tools for data

collect them technically integrate. In addition, tools or

Third-party content incorporated into the Services that ostensibly

Offer added value for the user, but often also in the background of the survey

of data (e.g. integration of web fonts or content from social

media or video platforms).

Since already the call of an Internet service and all associated with it

Data processing for technical reasons unique identifiers

such as B. require the IP address of the user, the collected data can

always (at least potentially) traced back to individuals

become. Therefore, these services are always relevant under data protection law.

Complaints submitted to my agency about online services

most commonly concern the processing of user data by means of cookies.

Cookies are files stored on the user's end device

many cases are needed to collect usage data. Even if

meanwhile various other techniques are used for similar purposes

are used and relevant providers such as Google or Apple at the

Replacing cookies work, they still represent an essential element

in the processing of user data on the Internet and are used by many

l users also perceived as such. In the reporting period reached me

hence dozens of complaints against the use of cookies

164

web, advertising

generally or against the design and function of the ubiquitous

Set up cookie banners.

With § 25 of the Telecommunications Telemedia Data Protection Act (TTDSG)

At the end of 2021, a new legal regulation for dealing with

Cookies and similar technologies created, with their implementation

I was involved for the first time in the reporting period. After that requires use

of cookies usually requires the express consent of the user

usually the first time a website is called up with a cookie banner

will fetch. To help and advise the providers of telemedia

In particular, to give the lawful use of cookies

Data Protection Conference published their “Guideline for the supervisory authorities for

Providers of telemedia" (https://www.datenschutzkonferenz-online.

de/media/oh/20221130_OH_Telemedien_2021_Version_1_1.pdf).

revised and adapted to the new legal situation.

Unfortunately, many providers of telemedia set the requirements from § 25

TTDSG and the data protection requirements for processing

of user data so far only insufficiently. Correspondingly themed

many complaints missing, insufficient, incomprehensible or technical

Cookie banners not working correctly. After all, these complaints could

Frequently remedied by the providers addressing their oversights

were made aware of them and then turned them off.

Among the tools and plug-ins that are often integrated into Internet services

Third-party providers were particularly impressed by the "Google Fonts" service in the reporting period

out. These are different fonts that Google under

a free license. These fonts are not uncommon

already preset in construction kits for website designs and thus far

spread. If Google Fonts are integrated online, the browser

ser of the user when accessing the website these fonts and takes over

Contacting Google's servers. In doing so, personal

User data is transmitted to Google, so that there is a legal basis for this

is required. If there is also a transmission of personal data

takes place in the USA are also those for third-country transmissions

comply with applicable requirements, including those set forth in

the judgment of the ECJ in the Schrems II case (judgment of 16 July

2020, C-311/18). It is therefore advisable to store the fonts locally on the

provide your own web server. This also applies to all providers

from web fonts.

During the reporting period, I received numerous requests for advice from

Website operators who received warning letters in which, among other things

Compensation for damages due to the use of Google Fonts was claimed.

Legally, the warnings were based on a judgment of the regional court

Munich. This had the operator of a website to blame, among other things

compensation of 100 euros due to the use of Google Fonts

sentenced (LG Munich I of January 20, 2022 - 3 O 17493/20). Although could

I lack jurisdiction in civil disputes no individual

conduct consultations. However, I have the affected website operators -

also via an article on my homepage – to the one described above

data protection issues and possible solutions.

Public prosecutors are now investigating several lawyers

law firms that have sent such warning letters. It exists

suspicion that the warnings were sent with fraudulent intent,

without actually qualifying for a claim for damages

due to a violation of the right to informational self-determination

would have existed. Even if the background to this wave of warnings is questionable

was worthy or even illegal, the operators of websites must

make sure they embed Google Fonts in a legitimate way. At-

Otherwise, violations can not by dubious warnings, but by

be pursued by the supervisory authorities. Next to it they also sit down

Danger of legitimate claims for damages from those actually affected

people out.

It is not uncommon for me to receive complaints about online reviews.

On various platforms, customers can usually anonymously or

under a pseudonymous username, evaluate companies and

describe their experiences from the business relationship. Mostly offer

the platforms also indicate the possibility that the rated companies

respond to reviews, especially negative ones

be able to state their point of view publicly. Always publish

again companies consciously name or other from the business

proportionately known data of the reviewers when they are based on ratings

of their content can be traced back to specific customers. This mostly serves

solely for the purpose of publicly exposing the reviewer

deliver, and is clearly inadmissible under data protection law if the

Those affected have not previously disclosed their identity publicly

has. At my request, the customer information immediately from their reply

to remove the review and to avoid sensitive sanctions

to refrain from any comparable publications in the future

the companies contacted usually quickly.

With the high number of complaints from the online area, unfortunately

also accompanied by a not inconsiderable proportion of abusive complaints.

In this way, I keep receiving submissions where it is clearly recognizable

166

web, advertising

that the petitioners are not concerned with violations of personal rights,

but solely about the prosecution and punishment of an opponent (in

for example a competitor or former business partner).

the regulator goes. For this purpose, possible

Searched for data protection violations, which websites are particularly suitable for because

they are operated by almost every company and always public

are. In the reporting period, in particular, has a series of abusive

Inputs generated significant workload. In doing so, under false

Dozens of “complaints” against various identities over months

Websites always submitted according to a similar template. With constant questions

and threats should also be enforced to be dealt with promptly.

Not in the case of clearly abusive complaints or submissions by itself

affected persons, it is at my discretion, the (alleged)

investigate violations. This ensures efficient supervision

cannot be exploited or even slowed down. Nevertheless

can I track and stop data protection violations even if I

only receive informal references to it or even through abusive ones

Complaints will be made aware of this.

12.2

No like for Facebook pages

Facebook pages with which many companies, associations, authorities,

present municipalities and other bodies in the social network,

cannot currently be operated in accordance with data protection regulations. In particular

the public authorities bear a special responsibility

the visitors of their social media appearances and are

therefore asked to use data protection in their public relations work

to set alternatives.

What are Facebook Pages?

In addition to the so-called profiles, Facebook offers only natural persons

and can use, also so-called pages (= pages, formerly known as fan pages)

with which institutions such as B. companies, associations or state

Be able to operate their own presence in the Facebook network. you can

In particular, notifications and other content such as photos or

Share videos, communicate or interact with Facebook users directly

or use Facebook advertising services.

In Hesse, too, many authorities, municipalities and other public

che put such pages on Facebook. These are often used to

Disseminate information from one's own business, general

to carry out public relations work or a low-threshold contact possibility

to offer citizens.

Why are Facebook pages problematic under data protection law?

With the operation of Facebook pages, there are some data protection regulations

problems. So e.g. B. when sharing certain content or the

public communication on Facebook against personal data

spread worldwide without the will or even without the knowledge of those affected

become. From a data protection point of view, however, it is far more problematic

the processing of user data in the background.

Meta Platforms Ireland Ltd. (previously: Facebook Ireland Ltd.) as operator

from Facebook collects data using cookies and similar technologies

of users and visitors of Facebook pages - regardless of whether they

own a Facebook account. Some of this data is provided in the context

the function called “Insights” by Facebook for the site operators

provided for web analysis purposes. These get so statistical

Information about the visitors of the respective page. In addition, raises

Meta, above all, but also for your own purposes, creates extensive data

User profiles and uses them profitably, especially for marketing

individualized advertising. The scope and the personality rights

Risks of this data processing are greater than most users and

Facebook page operators are probably aware of. Meta can be multiple

collect, store and evaluate hundreds of types of personal characteristics

and use it for advertising purposes. Just visiting a few Facebook pages

and websites linked to Facebook enables precise conclusions to be drawn

on, for example, age, gender, origin, personal taste and

possibly even sensitive information such as sexual orientation or

political attitude of an individual user. The longer appropriate

Data is collected, the more comprehensive and accurate the

Profiles about the individual.

May this data be collected and processed?

For a long time it was disputed whether the operation of Facebook pages/fan pages against

violates data protection regulations. To judge this is not least

difficult because Meta neither the operators nor users of pages

nor disclosed to the supervisory authorities which data processors

processing operations are precisely connected to Facebook pages.

168

web, advertising

In the meantime, however, the legal situation has been changed by a judgment of the ECJ (judgment of

June 5, 2018, C-210/16) as well as several judgments of German courts (esp.

BVerwG, judgment of September 11, 2019, 6 C 15.18) clarified. In this

drive it was about a decree of the Independent State Center for

Data protection Schleswig-Holstein (ULD SH), which is a company den

had prohibited the operation of his fan page. This decree was approved by the OVG

Schleswig-Holstein with a judgment that has now become legally binding

found lawful (judgment of November 25, 2021, 4 LB 20/13).

In principle, the judgments issued relate to the decision of the

ULD SH from 2011 and thus to the one valid at that time

Legal situation and the "Fanpage" service in the form in which it was published at the time

Facebook was offered. One commissioned by the Data Protection Conference

Task force, consisting of specialized employees from several German
Data protection supervisory authorities, however, has found in an expert opinion that
the findings made in the judgments also apply to the current ones
Facebook service "Pages", which largely derived from the "Fan Pages" of the time.
speaks, as well as transfer the current legal situation. Although since
more than ten years have passed, Meta Platforms Ireland Ltd.
not adapted the service to applicable law.

In particular, the courts found that the data protection
legal responsibility for the operation of a Facebook page not alone
lies with Meta. Rather, the operators of the pages together with
Meta according to Art. 26 DS-GVO legally responsible for the associated
data processing.

From this joint responsibility arise for both parties
Responsible for various data protection obligations, for example
with regard to the transparency and legality of data processing
tion. However, Meta does not meet its obligations in this regard itself
to a sufficient extent, nor does it represent those who are jointly responsible
Page operators the necessary information available to them
need in order to be able to meet their obligations.

So e.g. B. the one provided by Facebook after the judgment of the ECJ
Agreement (“Site Insights Addendum Regarding Controller”)
does not meet the requirements of Art. 26 GDPR (see also the decision of the
data protection conference on April 1, 2019). Also, the site operator
do not fulfill their information obligations according to Art. 13 DS-GVO, because Meta
does not make transparent to them which data processing is involved
closely related to the operation and use of Facebook pages.

The measures previously considered and partially already implemented by Meta

men are not enough to eliminate these problems. Also a conceivable one

Switching off the so-called "Insights" would not result in the data

protection requirements are met. Because by deactivating

the insights function would not eliminate the shared responsibility that

between Meta and the operators of a Facebook page. the deak

activation would be the relevant data processing when operating a fan page

hardly change, the site operators would only from the - after

as before - processed usage data are no longer played out statistics.

Furthermore, the site operators set their own

responsible for the cause of the collection of personal data

Visitors to their page through meta that are there without running the Facebook page

again would not exist. The sites benefit from this data processing

operator as well as meta alike. The site operators increase through the

Network effects of the social network their reach, while meta

specific profiles based on the interactions of site visitors

targeted advertising addressing can create. The purposes of the site

operator and meta complement each other so what for the assumption

a common purpose within the meaning of Art. 26 GDPR is sufficient.

In addition, data are also transferred to the USA

as well as through the possible access to data of European users

US security agencies privacy issues. True, the meta

Platforms Ireland Ltd. based in the EU Contract partner of the European

Facebook customers, but this is a subsidiary of the US company

mens Meta Platforms Inc. (until 2021: Facebook Inc.). Both companies

exchange data permanently and it can be assumed that this

also concerns personal data of European users. Since the

far-reaching powers of American security agencies

Subsidiaries of US companies based abroad Application

can also be accessed at Meta Platforms Ireland Ltd. saved

Data by US authorities at least possible. So far it is not apparent

that Facebook has taken sufficient measures within the meaning of the ECJ (judgment of

July 16, 2020, C 311/18 – “Schrems II”) to protect the rights of

To protect those affected in such a constellation.

The requirements that have been in force since December 1, 2021 will also apply

the setting and reading of cookies from the TTDSG by the jointly

responsible site operators and meta not complied with. According to § 25

Paragraph 1 sentence 1 TTDSG is u. the setting and reading of cookies in the

Rule only allowed if the end user on the basis of clear and

comprehensive information has consented therein. these requirements

However, Meta and the fan page operators do not do justice, since the

Meta obtained consent is not sufficient and the legally

Exceptions apply in the case of Facebook Pages are not relevant.

170

web, advertising

The obligation from § 25 TTDSG does not only affect Meta, but also

the operators of Facebook pages themselves, since they are providers of telemedia

are within the meaning of § 2 Para. 2 No. 1 TTDSG. On the one hand, they provide one themselves

Telemedium, since they provide a page that can be called up separately in the network

as well as fill with content, also act through the operation of their

Facebook page but also on the social network Facebook. Because this

thrives on Facebook users interacting with Facebook pages

and publish content there. Hence the content design

the Facebook page is a major contributor to the social network.

All of these data protection deficits can be solved without the active support

tion by meta by the site operators alone, nor

– for example by obtaining consent – can be circumvented.

What does this mean for the operators of Facebook pages?

As long as Meta does not process data on Facebook pages

– makes sufficiently transparent,

– provides the site operators with an agreement that

Claims of Art. 26 DS-GVO are sufficient,

– demonstrably meets the requirements of § 25 TTDSG,

– demonstrably adheres to the limits of permissible data processing and

– demonstrably necessary protective measures to secure the data

ten transfers to the USA,

the operation of Facebook pages encounters significant data protection

common concerns.

The operators of Facebook pages can therefore hold themselves accountable

according to Art. 5 Para. 2 DS-GVO. After determining the

OVG Schleswig-Holstein is the operation of a Facebook page

"Serious violation of data protection regulations".

On March 23, 2022, the data protection conference made a decision

fen with which the above Points are noted and a common

and uniform procedure of the supervisory authorities of the federal government and the

Countries agreed (https://www.datenschutzkonferenz-online.de/media/dskb/
DSK_Decision_Facebook_Fanpages.pdf). The decision follows several
Resolutions and resolutions (including June 6, 2018, September 5, 2018
and from April 1, 2019), with which the data protection conference has always been for years
again pointed out the existing deficits on Facebook pages.
As a result, I expressly closed the public authorities in Hesse
pointed out the now clarified legal situation and in particular opposite

the state government expressed my expectation that the
public bodies in Hesse do not create new Facebook pages and
from the Facebook Pages they operate to alternative, privacy-
change legally unobjectionable ways for their public relations work.
When changing, they must ensure that the chosen alternative
did not cause comparable data protection problems. Until this change
is completed, public bodies may not exclusively use information
Facebook offer, but must for the publication of this information
information, always use at least a second communication channel
zen, which does not raise any data protection concerns, and on this
expressly point out.
Facebook pages have been used for public relations by authorities and other
whose public bodies are undisputedly of great importance. Nevertheless are
the data protection supervisory authorities and therefore I am also obliged to do so
To ensure that the site operators meet their responsibilities
and the basic rights of the visitors to their pages are not

jeopardize Public bodies in particular are bound by law and order

fulfill a role model function. Therefore, on this point, too, they must

Take into account concerns and clear case law. As long as

international service providers such as Meta fulfill their obligations under the DS-

GMOs do not meet, users of social media services are doing this

called for their communication and publications on alternative

To set providers and communication channels that comply with data protection law

Meet requirements.

The process of moving to privacy-safe ones

Alternatives are actively supported by my authority. this happens

in particular by advising those responsible, but also by

direct support of the responsible authorities in setting up and establishing

provision of alternative services.

12.3

High hurdles for email advertising to existing customers

Consent is generally required for e-mail advertising. Out of-

alternatively, for existing customers, an interest

serve as a legal basis for weighing up The regulatory practice

shows, however, that many advertisers find it difficult to meet the conditions

of the DS-GVO and also to be taken into account when weighing up

Law against unfair competition (UWG) for consent-free

e-mail advertising, as this ultimately involves high practical hurdles

are overcome. I therefore recommend advertisers to always use viable ones

web, advertising

obtain consent for e-mail advertising from customers and

It is better not to make use of the acceptance regulations of the DS-GVO and the UWG

gain weight.

For the processing of a personally identifiable e-mail address for

Sending e-mail advertising is always an explicit, informative

informed and voluntary consent of the address holder in accordance with Art. 6 Para. 1

Subsection 1 letter a and Article 7 GDPR required as the legal basis.

The provisions of the GDPR are in line with the

Regulations in the UWG, where the admissibility of the use of different media

for advertising purposes is regulated from a competition law perspective. Here is

according to § 7 Abs. 2 Nr. 3 UWG e-mail advertising inadmissible if none

prior express consent of the addressee has been obtained.

However, both the GDPR and the UWG allow existing customers

under certain conditions an exception to this consent

Requirement to: In addition to consent, data protection law can also

Weighing of interests according to Article 6 Paragraph 1 Subparagraph 1 Letter f GDPR in connection

tion with Recital 47 GDPR for the use of e-mail ad

use for advertising purposes for their own products or services

Serve legal basis if it is a customer of the controller

advertisers with whom a contract has previously been concluded

has been closed and where it is possible that the e-mail advertising the

reasonable expectations of the customer concerned. So that these

data protection balancing between the legitimate interests

of the advertiser and the legitimate interests of those affected

person in favor of the e-mail sender must also always

all the conditions of Section 7 Paragraph 3 No. 1 to 4 UWG must also be met. The this-

The relevant provisions of the UWG must therefore be integrated into the GDPR

and consequently in the weighing according to Article 6 Paragraph 1 Subparagraph 1 Letter f

GDPR to take into account.

Advertisers who use email marketing to their own existing customers

want to forgo an effective consent have the following

To meet the requirements of § 7 Para. 3 No. 1 to 4 UWG cumulatively, so that

the interests of those affected the legitimate economic interests in the

promotional use of the e-mail addresses do not outweigh:

173

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

§ 7 para. 3 no. 1 UWG

The email address used for promotional purposes must be related

collected from the customer with the sale of a good or service

have been.

Many companies overlook the fact that this requirement affects the advertising

processing of e-mail addresses that a company e.g. B. about

a prospect or price inquiry or because of the inquiry for one

has received a cost estimate or an offer, as there is no "sale"

has taken place. E-mail addresses resulting from pre-contractual relationships

are not commercially usable without consent. And also at

Sales that – for whatever reason – later reversed

were made or were invalid under civil law, the collected

Email addresses are not advertised. The same applies to e-mail addresses

s that do not come directly from the customer, but rather from the advertisers

received from third parties or other sources.

As a consequence, those responsible for data collection must be organized

take organizational and data processing precautions in order to

be able to use email marketing data from customers with a best-

existing contractual relationship from the data of other data subjects who

collected from other communication situations.

Only such differentiation that is present in the supervisory authority

Cases often omitted or in the underlying IT-technical

processes in the company was not mapped correctly, can

afford that only under competition law and thus also under data protection law

permissible e-mail advertising is operated without consent.

§ 7 para. 3 no. 2 UWG

The e-mail address of an existing customer may not be used by the responsible

operators only for direct advertising for their own similar goods or services

services are used.

On the one hand, this provision prohibits it for goods or services

other companies to operate e-mail advertising without consent.

This also applies to the goods or services of affiliated companies

companies, business partners or companies belonging to the group. For the

other particular attention should be paid to the fact that in the competition law

case law, the concept of "similarity" is interpreted very narrowly. It

must ultimately be goods or services about which

previously a contract existed, or these must have a very similar purpose

serve like those advertised. Permitted here is e.g. B. the advertising of goods or

web, advertising

Services that are interchangeable and serve the same purpose. It

but may also be accessories, spare parts or additions to an already

trade the purchased product. However, a clothing company is not allowed to
Advertise men's clothing by e-mail if women's clothing has previously
was purchased, a travel agency may not advertise a cultural event if
previously only a one-way trip was booked, and if, for example, a
printer was bought, must therefore not automatically for all others
EDP products of a company without separate consent by e-mail
to be advertised.
To meet this additional legal requirement for consent-free
To be able to do e-mail advertising justice, companies need it
Evaluate the product and service portfolio accordingly and
referenced according to the criterion of "similarity" (or "replacement", "accessory",
"Supplement") and before an e-mail campaign with the respective
ligary data origin as shown under No. 1. That's the only way
the result is a list of recipients for each individual advertising mailing
be compiled under the two previously described pro-
suspensions may be advertised by e-mail without consent.
§ 7 para. 3 no. 3 UWG
The customer may not object to the use of his email address
have.
This condition under competition law can be found in Art. 21
Para. 2 and 3 DS-GVO and can simply by setting an advertising block
maintained in the data subject's record in the customer database
become.
§ 7 para. 3 no. 4 UWG
The customer must collect his e-mail address and each
use must have been clearly and conspicuously stated that he is the

Use for advertising can object at any time.

This regulation also has data protection equivalents: According to

Art. 13 para. 1 letter c DS-GVO must be used when collecting data about the

Purposes are informed (data protection notice) and after

Art. 21 Para. 4 DS-GVO must be referred to at least in the first advertising

Right of objection according to paragraph 2. This legal

Requirements are fairly easy to meet. Even if in individual cases

Transparency deficits in data protection notices were identified

the intended advertising use of collected data predominates

correctly informed. In promotional e-mails, it is usually used with a at the end

the unsubscribe link attached to the advertising e-mails to the right of objection

against advertising and a simple deregistration for address holders

made possible by the sending of advertising e-mails.

Advertisers who only meet one of the requirements of Section 7 (3) UWG

do not comply with Article 6(1)(1)(f) GDPR

as the legal basis for e-mail advertising under data protection law

take, since an economic interest in illegal advertising never

can be recognized as a legitimate interest.

Recommendation

Especially for larger companies with an extensive product or

range of services constitutes the use of the exemption

6 Paragraph 1 Subparagraph 1 Letter f GDPR and Section 7 Paragraph 3 UWG for

E-mail advertising without consent often poses a major challenge.

If it's already considerable organizational and EDP-technical effort

means, the conditions of § 7 Abs.3 Nr. 1 UWG in the differentiation

to comply with the origin of existing e-mail addresses,

formed the combination with another subsequent exact

Differentiation of products or product groups according to their competitive

"Similarity" under advertising law within the meaning of Section 7 (3) No. 2 UWG for broad

planned and regular advertising campaigns are even more problematic.

The possibility, welcomed by the advertising industry, of e-mail addresses

as an exception to use for advertising without consent, keeps

closer inspection, there are high hurdles in practice, which can only be overcome with considerable

effort can be overcome.

In addition, it must also be taken into account that those affected by the e-mail

are generally opposed to exercise without consent. They bring

especially then no understanding that your e-mail address

resse is used for advertising if you register as a customer in the

WWW offer of a company the non-preassigned radio button for

a newsletter registration under the registration form is not

voted and thus did not agree to receive the newsletter. This

Customers lay after receipt of the first not expressly desired

Advertising e-mail immediately an advertising objection. The trust to

the company that provides the basis for as many new customers as possible

represents long-term customer loyalty in the interests of the company

This is already the case with the first order through consent-free e-mail advertising

sensitively disturbed.

176

web, advertising

Against the background of the legal and practical difficulties

It is recommended that responsible advertisers take better care of the

Claiming the exemption from the consent requirement

for e-mail advertising according to Article 6 Paragraph 1 Subsection 1 Letter f GDPR and Section 7

Abs. 3 UWG, as a variety of legal and practical risks

to deal with it. E-mail advertising should only be used with an explicit,

are operated with the informed and voluntary consent of the address holder.

12.4

An objection to advertising has no expiry date!

According to Art. 21 Para. 2 DS-GVO, those affected can use their data

for advertising purposes (advertising objection to direct

exercise). Art. 21 Para. 3 DS-GVO stipulates that personal data then

may no longer be processed for such purposes. A repeat purchase

of a product after filing the advertising objection does not make this

ineffective. The effectiveness of the objection also does not depend on the for

the sales channel used for the respective purchase or the sales channel behind it

technical system. Technology has to be human-oriented

and not the other way around. Once to a person responsible

An objection to advertising is always valid until it is raised by the person concerned

person is revoked.

As part of my supervisory work, I became aware of a company

sam, which informed customers in its general terms and conditions that an inserted

Objection to advertising lifted by purchasing a product again

becomes. After each purchase, an advertising objection must be filed again

to prevent the use of customer data for advertising purposes in accordance with Art. 6

1 subparagraph 1 letter f GDPR.

The data subject's right to object to the processing of personal

related data for direct marketing purposes and the corresponding

The legal requirement for advertisers can be found in Art. 21 Para. 2 and 3

GDPR:

Art. 21 para. 2, 3 GDPR

(2) If personal data is processed in order to operate direct advertising, the

data subject has the right to object at any time to the processing of data concerning them

submit personal data for the purpose of such advertising; This also applies to

profiling to the extent related to such direct marketing.

(3) If the data subject objects to the processing for direct marketing purposes,

the personal data will no longer be processed for these purposes.

I have informed the company that its terms and conditions information

onen and its data processing based on it for advertising purposes

do not comply with the requirements of Art. 21 Para. 2 and 3 DS-GVO

and advertising contradictions have no validity limit. In particular

a contract for a product purchase raises the validity of the

taken statutory rights of data subjects.

In the further course of the subsequent discussion with the advertising

ing companies also turned out that it was his customers

Offers products on different sales channels and next to one

Retail store also via an online shop on the WWW and via a

mobile app, which is also used for customer registrations

and products can be purchased. The company represented here

legally erroneous view that after making a purchase in the online shop

Advertising contradiction does not apply to the mobile app. A customer whose data

due to an objection after a purchase in the online shop for advertising

have been blocked, so can be reactivated after a purchase via the mobile app

be advertised until he also receives an advertisement via the mobile phone app

appeal. This was justified by the fact that for the two sales

because two different customer databases are maintained, which are not

are compatible and cannot be synchronized.

I then made it clear to those responsible that the data

protective regulations on the interests of those affected that are worthy of protection

customers and their use of legal rights

and not due to organizational deficits in responsible bodies or

as in the case of the incompatibility of technical systems. If it's dem

Company for technical reasons is not possible a uniform

Customer database for online shop customers and mobile app customers too

lead, the company needs other technical or organizational

Find processes to ensure that the rights of data subjects are taken into account

to be able to afford. The problem finally got through the introduction

solved with a uniform blocking file, in which the daily advertising contradictions

are fed in from both systems and with which the mailing lists

be compared before each new mailing.

178

web, advertising

12.5

Polite or promotional - E-mail greetings as advertising

An initially courteous “Happy Birthday”, “Frohe

Christmas", "Happy Hanukkah" or "Happy Easter" can

privacy poses many problems when it is emailed from

Pages of a company is sent.

The sending of e-mail advertising represents a fixed constant within

of online marketing. The benefits of email marketing vs

postal advertising are above all the low costs and that

Potential to reach a large number of people in a short period of time. But

Data protection is often neglected with this form of advertising.

To limit the flood of e-mail that the benefits just listed

wise, and to protect the personal rights of the

Recipients are contacted by means of advertising e-mails by the

Legislators set strict limits.

In terms of data protection law, this means first of all that in favor of the

ders the e-mail congratulations a legal basis for processing

of the personal data must be available. Crucial to the

Lawfulness of the processing of the personal data (e.g

date of birth or first and last name and especially e-mail address)

is therefore not the motive, but exclusively whether a legal basis

consists.

The admissibility of advertising e-mails is essentially determined by

the GDPR and the UWG.

The sending of advertising e-mails is subject to data protection aspects

permissible if the person concerned has given an express, informed and free

Willing consent in accordance with Article 6 Paragraph 1 Subsection 1 Letter a and Article 7 GDPR

has granted. The essential competition law regulation on admissibility

of e-mail advertising can be found in § 7 Para. 2 No. 2 UWG. As a result

E-mail advertising without prior express consent in principle

unacceptable harassment.

If there is a violation of the regulations mentioned, the advertising

anti-competitive. There is then a claim for injunctive relief by the

competitor. The person concerned is a legal

unlawful encroachment on the general right of personality.

At the beginning of the reporting period, an airline based in Hesse

company sending birthday wishes to a customer by e-mail

telt, who follows up in advance in writing any advertising approach

Art. 21 Para. 2 DS-GVO had objected. The person concerned felt his

clearly expressed right of objection disregarded, since his in the company

stored personal data for purposes of direct

advertisements were processed.

However, the airline was not at all aware of a data protection violation

consciously, the transmission of birthday wishes did not take her

true as an advertising act.

What falls under the term "advertising" is determined by the courts together

related to direct marketing measures very widely understood. Advertising

is according to Art. 2 Letter a of the EU Directive 2006/114/EG any direct

or indirect action aimed at promoting the sale of products

and services or the image cultivation of one's own or someone else's

company serves.

The birthday greetings in the present case contained, in addition to congratulations

also give an indication of bonus miles due to the birthday

could be credited if travel via the airlines during this time

society would be booked.

Just the sending of the congratulations by e-mail, but even more so the addition

to bonus miles, aimed at promoting the company and

thus represents advertising within the meaning of the EU directive. Due to the intensive

exchange with the airline could improve the understanding of the

be sharpened. The advertising approach was logical

expressly complained about despite the present advertising objection and measure

58 para. 2 DS-GVO, if again in the future

the personal data stored in the company about the data subject

data would be processed for advertising purposes. Because of that

the company takes appropriate technical and organizational measures

taken in order to meet the legal requirements in the future.

12.6

Use of language assistants in business premises

Voice-controlled assistance systems are able to use an algorithmic

man-based language analysis to understand human language and then

to provide appropriate assistance services. Common systems are about

Siri from Apple or Alexa from Amazon. It is obvious that in the context

speech recognition also involves the processing of personal data

uninvolved persons can take place. Here are the respective specifications

of the GDPR to be observed.

180

web, advertising

The following case was brought to me via a complaint: In a

A smart loudspeaker was installed by the owner of the shop,

to play music. The person concerned expressed their discomfort at

an impairment of the right to informational self-determination, since

It is unclear to what extent the spoken word of the customers to the servers of the

Provider of the assistance system is transferred to its functions

to offer.

In fact, once activated, the voice assistant sends a

specific keyword sends the recorded voice data to the server

his provider. There, software transcribes the audio data and

averages an answer or implements a function, such as playing

of music. This means that personal data is processed.

Depending on the content of the spoken word, it can even be a

processing of special categories of personal data pursuant to Art. 9

Para. 1 DS-GVO act according to the will of the Union legislator

are specially protected.

The specifications for the use of such an assistance system are therefore

to comply with the GDPR. This includes in particular the existence of a

Legal basis according to Art. 6 Para. 1 DS-GVO. Because other legal bases

are not apparent, consent is given in accordance with Article 6 Paragraph 1 Subparagraph 1

letter a DS-GVO, the existence of which according to Art. 7 Para. 1 DS-

GMO must be proven. The persons affected by the data processing

are to be informed extensively in accordance with Art. 12 et seq. GDPR.

The consent must relate to all processing operations,

the same applies to the fulfillment of information obligations. As far as the servers

of the provider of the assistance system are located outside of Europe

and personal data are transmitted there, Chapter V of the

DS-GVO as well as the relevant case law, such as the judgment

of the ECJ of July 16, 2020 in the case "Schrems II" (C-311/18).

In the present case, based on corresponding information from me,

the configuration options shown below in the settings

of the language assistant achieves an adequate level of protection and a

Processing of personal data of those affected is prevented.

Microphone and camera should be turned off. The one recorded by the system

Language may neither be saved nor used to improve the system

become. Any voice history that has already been recorded must be deleted. Besides

the choice of a rare activation word offers itself to reduce the risk

to minimize unwanted activation. As far as the system means

a voice command is activated, this should be outside of the presence

possible affected persons happen.

181

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

After the business owner had implemented these requirements,

Music could continue to be played via the system and the customers could

without impairing their right to informational self-determination

continue shopping.

12.7

Unused online accounts as a security risk

A growing number of complaints concern desire

after deletion of online accounts. Because every additional online account

increases the potential risk of data and identity theft.

In an increasingly digital world, it is no longer necessary just for a quick

shopping experience of an online account, but also for the reservation

of tables in trendy restaurants, the streaming of music and videos, the

Ordering private trips, sharing in social networks or

also for participation in forums.

With each registration, a personal account is created, the one

Username and password required in the next step to per-

to store personal data such as first and last name. sense

such an account is the recognition of the user and his

authentication. Basically, online accounts are ahead of everyone

Things security measures of the website manager

its website users. However, the user leaves behind the facility

an online account and the associated deposit of personal

of data related to digital traces on the World Wide Web (WWW). Furthermore

the risk increases with the creation of more and more accounts

Use usernames and passwords for different services.

If a user decides to delete his online account, this

sem does not always have the "Delete Account" functionality in its account settings

positions available. Neither are the web service providers

obliged to a simple deletion z. B. with its own button

to allow. In accordance with Art. 17 Para. 1 DS-GVO, those affected have

However, individuals have the right to request that the person responsible

relevant personal data will be deleted immediately. The

However, “how” is not regulated. It should also be noted that no right

to the deletion of personal data by the person responsible

exists if one of the reasons mentioned in Art. 17 Para. 3 DS-GVO for

another storage is available. The retention periods for companies

are primarily based on two legal bases, on the one hand

tax law and on the other hand according to commercial law. For merchants

182

web, advertising

the German Commercial Code (HGB) contains corresponding regulations, e.g. B.

§ 257 HGB, and in the area of tax law regulates the tax code

(AO) mainly in § 147 AO the respective storage obligations. Therewith

For example, you need documents about transactions and payments made

are kept insofar as they are of importance for taxation.

Every merchant is also obliged to keep records of the physical

Financial and value inventories of all assets

and carry debt.

However, some officials are mistaken in assuming that

retention requirements also exist for online accounts. This is

not like that.

At the beginning of the reporting year, a forum user contacted me

asking them to help them enforce their data protection claims

to support. After falling out with the forum owner-

te, she wanted her account deleted because the forum didn't post any

Possibility to independently delete the account once created. But

instead of deleting the user's data, the forum owner merely blocked it

the online account and kept the stored personal data

before. From the point of view of the forum operator, this measure should serve to

Enforce domiciliary rights and ensure that the forum user does not

more opportunity to participate in his forum in the future. He saw

prompted to take this measure because the forum user is of his opinion

after violating the netiquette rules.

From the point of view of data protection law, the case was clear and the

leading actions in the form of deletion of personal data

and the account itself. However, in considering one

in any case, in addition to the purely legal assessment, also the external ones

factors and the aspirations and needs of the parties

and weigh.

Measures according to Art. 58 Para. 2 Letter c DS-GVO were therefore not necessary

derlich, instead it was enough to give the respondent a legally compliant

and recommend a mutually acceptable alternative. To be le-

Gitimes need to protect and enforce his forum, it was enough for him

to offer the maintenance of a so-called "block list".

As part of this blocking list, he was allowed to

deposit and keep the given e-mail address in order to be able to

Match new registrations and unauthorized re-registration

to fend off Thus, the Respondent could exclude a

ensure future participation by the petitioner in his forum.

Simultaneously with the introduction of the blocked list, the Respondent

all other personal data of the complainant including

delete account.

All parties were pacified and agreed to the solution. the personal

Personal data and account were deleted, the blocking list was created

and the file could be closed.

12.8

Data protection declaration for a website

If you want to be represented on the WWW and set up an online presence,

must comply with certain information obligations and legal requirements

comply with

The task of a data protection declaration is to inform users of online services

to inform about the type and scope of data from

website visitors are processed and what rights they have towards them

can assert against the website operator. This information should

Above all, ensure transparency and the informational self-

ensure the mood of all data subjects to make their own decisions,

how his data is handled and who receives which information

and potentially evaluated and processed.

Due to several complaints I received, I wrote some

small and medium-sized companies, but also large holdings within

halfway through the reporting period and asked them to comment

how you as a provider of online content and thus as the person responsible in

Within the meaning of Art. 4 No. 7 DS-GVO their information obligation according to Art. 13 Para. 1

and 2 DS-GVO usually comply, as they have not yet done so

had maintained a data protection declaration.

Frequently, out of ignorance, those responsible stated that they had no

would process data as part of their small online presence and

with no privacy statement required. But this assumption is wrong.

The embedding of a contact form, the use of advertising banners, the

decision for social media plugins or the use of cookies

However, the collection and processing of personal data for

Consequence. However, even when doing without these applications takes place in the background
a collection of personal data takes place. Because with every call one
Website is transmitted in the background metadata to a technically
to enable smooth retrieval of the content. This also includes those
IP addresses stored on the server of the hosted website in so-called
Server log files are saved. Does the website operator save this
184
web, advertising
together with the time of access, the subscriber of the domestic
internet access can be determined.
According to a decision of the ECJ (October 19, 2016, C-582/14)
Both static and dynamic IP addresses represent personal data
data. Thus, personal data is actually already ex
collected as soon as a website is called up.
Conclusion
Every operator who collects personal data on his website
transmitted, used or processed in any other way, according to DS-GVO
provide a privacy policy on their site. Also
if the person responsible does not have any user data on his website
queries and collects personal data by the commissioned
of the responsible host provider. It is thus in operation
impossible for websites not to collect any personally identifiable information,
therefore the data protection notice is a must.
Danger
Those responsible who refuse to comply with their information obligation
men, threatens in addition to possible measures and sanctions by the

Data protection supervision also a warning from competitors. So e.g. B.

the Hamburg Higher Regional Court (judgment of June 27, 2013; AZ. 3 U 26/12) decided,

that an inadequate data protection declaration on the website violates the

violates competition law and thus e.g. B. warned by competitors

can be.

The responsible persons I wrote to reacted after the clarification

position on the need to embed a data protection declaration

promptly, showed understanding and took care of it immediately, their

comply with information obligations.

However, a holding company provided the necessary information despite repeated

liger request and showed no willingness to

to do that. As a result, I have instructed them according to Art. 58 DS-GVO,

post a privacy statement, and this statement with the

Fixing a fine supported. These measures unfolded

their effect. The company improved and embedded a data protection

declaration on its website.

185

social affairs, video surveillance

13. Social affairs, video surveillance

social affairs, video surveillance

Video surveillance is for companies and public bodies as well as private

people obviously have an important need, that of overview and security

shall serve. However, it severely interferes with the basic rights of the persons recorded

and therefore leads to many complaints. So I always have them

to determine the limits of permissible video surveillance and must

take corrective action if this is exceeded (section 13.1). Also in social data protection

new constellations of data processing arise again and again

request data protection answers. The following are questions

according to the authority of job centers to demand the submission of documents,

which also contain data from third parties (section 13.2) and data on rental agreements

to pass on to the tax offices (chap. 13.3), answered.

13.1

Video surveillance – a perennial favorite

In 2022 I again received a wealth of complaints and advice

inquiries about video surveillance. I summarize them below

my home directed submissions under review.

overall view

Overall, video surveillance (except in the police area) went to

I received 408 complaints and 80 requests for advice during the reporting period.

In these cases, it had to be checked whether the scope of Art. 6 para. 1

Subsection 1 letter f GDPR for private individuals and companies or the

Article 6 paragraph 1 subparagraph 1 letter e GDPR in connection with § 4 HDSIG

authorities was opened.

Of the 408 complaints, 278 were finally processed and 130

Complaints are still pending (as of December 31, 2022).

Of the 80 requests for advice, 77 were finally processed (status:

12/31/2022).

Of the 80 requests for advice, 77 were finally processed (as of December 31, 2022).

complaints

(total 408 cases)

130; 32%

278; 68%

completed

open

Figure 1: Complaints about video surveillance (status: December 31, 2022)

Figure 1: Complaints about video surveillance (status: December 31, 2022)

Consultation Requests

(total 80 cases)

3; 4%

77; 96%

completed

open

Figure 2: Consultation requests for video surveillance (status: December 31, 2022)

Figure 2: Consultation requests for video surveillance (status: December 31, 2022)

Video surveillance in non-public spaces / civil matters:

For the testing of video surveillance systems, which exclusively

relate to non-public spaces (e.g. video surveillance between

neighboring properties, video surveillance that is not sidewalk,

street or other public space), there is no data protection

Video surveillance in non-public spaces / civil matters:

For the testing of video surveillance devices, exclusively for non-public

relate to space (e.g. video surveillance between neighboring properties,

Video surveillance that does not affect the sidewalk, street or other public space) does not take place

data protection supervisory authority procedure by me as an expression of my

Discretionary resolution according to Art. 58 Para. 2 DS-GVO. Only checking video surveillance

public spaces is part of the (obligatory) area of responsibility of the Hessian

Data protection supervisory authority according to Art. 57 DS-GVO in connection with § 4 BDSG and § 4 HDSIG.

188

In cases that exclusively concern non-public spaces, complainants have the right to

social affairs, video surveillance

regulatory action by me as an expression of my

closing discretion according to Art. 58 Para. 2 DS-GVO. Just checking the

Video surveillance of public spaces is part of the (mandatory) task

area of the Hessian data protection supervisory authority according to Art. 57 DS-GVO

in connection with § 4 BDSG and § 4 HDSIG.

Appellants stands in cases that are exclusively non-public

Affect space, the civil legal action against the camera operator according to §§ 823

and 1004 BGB because of a possible violation of personal rights

open. 52 complaints were referred to civil courts.

handling clues

The investigation following a complaint should, after consideration

reason 141 to Art. 77 Para. 1 DS-GVO go as far as this in individual cases

is appropriate. A complaint requires an individual

impact of the respective complainant.

If a complainant merely submits that at a certain location a

surveillance takes place, this alone does not justify concrete concern.

It is then a matter of a notice for which no subjective legal

there is a right to a referral and examination by me (see also VG

Wiesbaden, Az. 6K 470/22.WI of September 22, 2022). At about ten

cases, no specific concern was identified.

Video surveillance of catering establishments

Video cameras are often used in restaurants to record gastronomic

To film surfaces, i.e. areas where visitors are. As

Reasons are e.g. B. theft and damage to property, but

also the quick look through the lens to compensate for the lack of staff.

The same applies to video surveillance – as it does to other data protection areas

– the principle of data minimization in accordance with Article 5 (1) (c) GDPR:

The data processing and the selection and design of the technology are

align with the goal of collecting only necessary data and so little

process personal data as much as possible.

In restaurants, cafés and catering areas, including outdoor catering

areas, video surveillance is generally not permitted. Especially in

places that you use in your free time and where you stay longer,

Do those affected find the video surveillance disturbing, which is reflected in the

Complaints to my house down.

I can dismantle a video surveillance system - often unfortunately

- do not order, but only the data protection compliant operation. For this

includes, for example, video surveillance during opening hours

ten (which is usually used for the purposes of "preserving evidence at

burglary/theft" is sufficient) or to swivel the video device,

so that it does not appear as if during the

Film opening hours.

Regrettably, simply disabling a camera is usually

not visible, which often leads to subsequent complaints. Normally

However, restaurateurs want complaints from their customers

avoid, so that in the year under review cameras of the

mounted or clearly covered.

In the past, a tourist restaurant, which has been proven

repeatedly affected by after-hours vandalism damage

was under video surveillance outside opening hours. In day-to-day operations

the camera was covered by the host so that the camera was not visible.

The signage according to Art. 12 et seq. GDPR has been changed accordingly

made that the monitoring times were specified transparently.

A total of 14 complaints were directed against catering establishments.

Fees from police authorities

Police authorities give procedures to me, which are found on site

becomes that public space is monitored. They also post ads

me, where private individuals have video surveillance of the

complain to the police about public space. Here is an exam

according to Article 6 Paragraph 1 Subsection 1 Letter f GDPR and, if necessary, the introduction of

other measures, possibly also issuing a fine.

In test procedures, I often come across camera operators who tell me

that police officers took them to video surveillance after an incident

have advised. Also a police advice

However, such an institution does not legitimize the data protection per se

surveillance of public space. For a permissible video surveillance

of public space requires the legitimate interests of the camera operator

drivers, which outweigh the interests of the

persons affected by video surveillance. This is usually not the

In any case, the hurdles for this are high. The right to informational

Self-determination basically grants every individual the right to

to be able to move freely in public without having to fear

become the subject of video surveillance. Regular is the

social affairs, video surveillance

Need for protection in publicly accessible rooms in which people

typically move, stop and communicate with each other,

especially high.

It should also be taken into account that the police used footage from a video surveillance

surveillance of public space as evidence for e.g. Legs

crime can ensure. A delivery will then still be made to me

to examine a data protection violation, which also accordingly

fulfill an offense punishable by a fine and can be punished. In the

In the year under review, I received 19 procedures from the police (+ 53 procedures

by regulatory authorities).

Video surveillance "in the forest and on the heath"

Video surveillance using animal surveillance cameras was already in

past activity reports (e.g. in detail in the 43rd activity report)

Theme. I received a total of eight complaints in the reporting period

on this topic.

In 2012, in coordination with the Hessian Ministry of

Environment, energy, agriculture and consumer protection a leaflet on

Operation of wildlife surveillance cameras created. This leaflet was

revised and specified in the reporting year. With my support

the ministry published the leaflet on April 1, 2022

data protection compliant operation of animal observation cameras in public

accessible space in the open countryside.

The leaflet follows the following general principle:

Entering the open countryside on roads and paths as well as on

used area is for the purpose of recreation according to § 59 of the law

ces on nature conservation and landscape management (Federal Nature Conservation Act)

all allowed. Entering the forest is according to § 15 paragraph 1 Hessian

Forest Act and Section 14 Paragraph 2 of the Federal Forest Act for the purpose of recreation

basically everyone is allowed, so that the forest - even in private ownership -

is considered to be a publicly accessible space, provided that there is no recognizable entry

ban exists.

For monitoring areas in the open countryside (fields and

forest) using an animal observation camera (wildlife camera, photo trap, threat

ne etc.) Article 6 paragraph 1 subparagraph 1 letter f GDPR applies. After that, the processing

processing is only lawful if it is used to protect legitimate interests

sen of the person responsible or a third party is required, unless the

Interests or fundamental rights and freedoms of the data subject,

that require the protection of personal data prevail. That clean

private operation of animal observation cameras in the publicly accessible

Space and thus also in the open landscape, that is, in the forest and in the

Feldflur, is fundamental in terms of data protection law - also e.g. B. to protect

Property - not allowed. In exceptional cases, there is a legitimate interest

of the monitor, who has no overriding interest worthy of protection

se of the person affected by the surveillance precludes, a

Surveillance with an animal surveillance camera may be permitted.

The following special basic rules apply:

1. For the forest area, with regard to forest management

generally assume that no particular

there is a legitimate interest in video surveillance.

With regard to the practice of hunting, there is predominantly no

legitimate interest in video surveillance. this applies

equally for circuses, since generally milder means can be used

are cash.

2.

3. As possible exceptions that justify a legitimate interest,

research projects and, alternatively, the use of animal observation

attention cameras to prevent excessive game damage acc.

Section 27 of the Federal Hunting Act (order to reduce the number of game

by the competent authority). Also for disease control in

danger zones proclaimed by authorities, the use of the

Animal observation cameras for a necessary reduction or for

supporting detections can be helpful. In these cases, too

take the following measures into account.

4. When using animal observation cameras in the context of

officially commissioned or approved investigations such as monitor

ring projects e.g. a legitimate interest can be assumed.

5. Before using an animal observation camera, always check whether

whose means come into question (e.g. game clocks). Unless milder means

are possible, these are to be applied.

The following implementation instructions apply to the use of animal observation

tion cameras if there is a legitimate interest:

1. A recording of people should be unlikely and with

be prevented by all available means, e.g. B. through

– the use of animal observation cameras, which

192

social affairs, video surveillance

know whether the object is a human being,

and erase that area completely from the image,

– mounting the camera at a maximum height of 1 meter,

– the alignment directly to the ground,

– the orientation against the sky (bird detection cameras for

Avoiding bird strikes e.g. B. on wind turbines).

2. When setting up the animal observation camera, data economy

must be observed (e.g. no video sequences, single images with a few

distance from customers, low resolution of the camera).

3. Areas that are in the immediate vicinity of a barbecue area and in particular

are located outside of a playground must not be monitored.

4. In close proximity to trails (e.g. scientific bird,

wolf or lynx observation) special measures must be taken

be taken to prevent people from being photographed (e.g.

Alignment to the ground or to the sky, monitoring if necessary

finally at night).

5. If you plan to monitor animals at night, the camera is

about turn off.

6. The information signs with the information requirements according to Article 13 DS-GVO (including name and contact details of the person responsible, purposes and legal basis for data processing) must be clearly visible be brought.

storage of recordings

According to Art. 17 Para. 1 Letter a DS-GVO, stored data are non- to be deleted immediately if they are no longer required to achieve the purpose are required or interests of those affected that are worthy of protection prevent storage. The EDPB assumes a storage period of maximum 72 hours (Guidelines 3/2019 on processing of personal data through video devices, Adopted on 29 January 2020, paragraph 121).

A violation of the lawfulness of the processing as well as a man- transparency (lack of information signs) meet the fine monetary offense according to Art. 83 Para. 5 DS-GVO.

Distribution of topics in the supervision of video surveillance

Overall, the thematic breakdown in the year under review is as follows:

Distribution of topics in the supervision of video surveillance

Overall, the thematic breakdown in the year under review is as follows:

distribution of topics

52; 13%

14; 3%

10; 2%

19; 5%

civil matter

gastronomy

Hints

254; 62%

53; 13%

8th; 2%

Submission by police authorities

Delivery by regulatory authorities

Wildlife observation / wildlife cameras

Personally affected (e.g.

neighborhood or employees)

Figure 3: Origin/causes of complaints in video surveillance

Figure 3: Origin/causes of complaints in video surveillance

13.2 (Social) data protection compared to independent SGB II “top-ups”

Request as part of the local examination of the eligibility requirements for SGB II benefits

Hessian option municipalities from self-employed claimants

often also evidence in the form of their business documents, sometimes also of invoices

have made these available to third parties. This may be necessary for performance testing and provides

then no violation of (social) data protection regulations, such as an unauthorized

Disclosure of data of third parties, if for the job center the examination and assignment of the

Income and expenses of the self-employed in other, less intrusive ways

is possible.

13.2

(Social) data protection compared to independent SGB II-

"top up"

As part of the local examination of the eligibility requirements for SGB

II services require Hessian optional municipalities from self-employed

Claimants often also provide evidence in

form of their business documents, sometimes also of invoices

have made these available to third parties. This can be used for performance testing

be required and then does not constitute a violation of (social) data protection

legal requirements, such as B. an unauthorized disclosure of data of third parties,

if the job center is responsible for checking and allocating income and

Spending by the self-employed in other, less intrusive ways

not possible.

facts

I regularly receive submissions from those affected who are topping up as self-employed (so-called).

have to apply for benefits according to SGB II and then from the job center responsible for them in the

Within the scope of their duty to cooperate, they are confronted with the demand, among other things, that the job center

Submit invoices that you have submitted to third parties for your self-employed activities

have. Those affected are concerned whether they will not be subject to a

commit a data protection violation or even be asked to do so. Finally reveal

194

social affairs, video surveillance

facts

I regularly receive submissions from those affected who are self-employed

(So-called) have to apply for top-up benefits under SGB II and

then by the job center responsible for them as part of their obligation to cooperate

ten among others be confronted with the demand to pay the job center bills

to submit to third parties for their self-employed activities

have asked. Those affected are worried whether they will not get a - possibly

subject to fines - committing a data protection violation or even leading to such a violation

would be prompted. Finally, they disclose data from third parties, viz

the recipients of invoices (e.g. name,

postal address, customer number) if they issue their own invoices

provide evidence of their activities.

Legal Assessment

Top-up, self-employed applicants or

Recipients are basically then

not obliged to submit third-party data if the examination and approval

arrangement of their income and expenditure from their self-employment

the responsible job center is (also) possible in another way.

In addition, to ensure social data protection, it must be noted that

Job centers may only collect the data necessary for the fulfillment of their tasks

required are. Whether it is for calculating the benefit entitlement in each

case within the meaning of § 67a Para. 1 Sentence 1 SGB X is required, in addition to the

bank statements submitted by the applicant and so on

assigned receipts and expenditures, individual invoices are not redacted

to submit is questionable.

§ 67a paragraph 1 SGB X

(1) The collection of social data by the bodies mentioned in Section 35 of the first book

is permissible if their knowledge is required to fulfill a task of the collecting body

this code is required. This also applies to the collection of special categories

Categories of personal data within the meaning of Article 9 Paragraph 1 of the Regulation (EU)

2016/679. § 22 paragraph 2 of the Federal Data Protection Act applies accordingly.

The job center may therefore only request the submission of the invoices

gen, if in the specific individual case other documents of the applicant

person without personal data of third parties are insufficient to the

proof of eligibility requirements.

195

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

With regard to the applicant, it must be checked whether they

documents with data from third parties may be submitted to the job center in order to

To contribute to clarifying the entitlement to benefits and to benefit from the

access social benefits. Article 6 paragraph 1 subparagraph 1 letter f

DS-GVO be a legal basis.

Article 6 paragraph 1 subparagraph 1 letter f GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met:

(...)

f) the processing is to protect the legitimate interests of the person responsible

or a third party, unless the interests or fundamental rights and

Fundamental freedoms of the data subject, the protection of personal data

require, especially when it comes to the data subject

is about a child.

The legitimate interests of the person responsible, here the applicant

or the applicant for (the granting of) social benefits

in the exercise of the constitutionally protected right to vote

ment of a decent subsistence level. This should by the

Granting of benefits according to SGB II are secured, so that the

the applicant has a legitimate interest in

that the approving authority (the job center) is put in a position to

to check and establish the claim based on the documents submitted.

The disclosure of the data must be necessary for the pursuit of the legitimate interest

esses be required. If the job center accepts the submission of the documents

demands and the applicant with a rejection of their

or his application must be reckoned with if she or he does not meet this demand

Fulfills. For her or him, the revelation of the personal arises

Third-party data as required. Applicants are not required to provide a

to accept rejection of their application and then more incidentally within the framework

an obligation action the necessity of the refused submission of the

to have data checked by a court.

Within the scope of the necessary balancing of interests, it is also necessary to consider

ensure that the data contained in the documents are available to the job center in

become known as part of the application, are subject to social secrecy

gen. The further processing by the social service provider is subject to the

particularly strict data protection regulations of the SGB. Task

and purpose of processing by the social service provider is exclusive

the examination of entitlement to social benefits.

196

social affairs, video surveillance

The data processing by the person responsible - in this case: the transmission

Delivery of invoices from the applicant to the

Social service provider - can protect the interests of the applicant

or the applicant and after weighing up the interests in the result

are therefore classified as permissible under data protection law.

The possible existence of an obligation to increase

the service recipient or the top-up service recipient,

the persons concerned the forwarding of their data to the job center

according to Art. 13 Para. 1 Letter e GDPR.

Art. 13 (1) lit. e GDPR

(1) If personal data is collected from the data subject, the responsible

verbatim to the data subject at the time such data was collected:

(...)

e) where applicable, the recipients or categories of recipients of the personal

gene data (…).

In principle, there could be an obligation to provide information. To

it should be noted, however, that according to Art. 23 Para. 1 Letter i DS-GVO these

Duty to protect the rights and freedoms of others to whom

who is responsible also counts, can be restricted.

Article 23(1)(i) 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:

(...)

i) the protection of the data subject or the rights and freedoms of others;

(...)

This restriction can be found in national law in Section 32 (1) No. 4 BDSG.

51. Activity report on data protection

§ 32 paragraph 1 BDSG

(1) The obligation to inform the data subject pursuant to Article 13(3) of the

regulation (EU) 679/2016 exists in addition to that in Article 13 paragraph 4 of the regulation

(EU) 2016/679 does not apply if the information about

the intended further processing

(...)

4. interfere with the assertion, exercise or defense of legal claims

would and the interests of the controller in not providing the information

the interests of the data subject prevail (...).

According to § 32 Para. 1 No. 4 BDSG there is no obligation to inform the affected

person. Applicants could be prevented from exercising their fundamental rights

protected right to maintain a decent standard of living

to claim nimums if this means that they receive their social benefits

towards their customers, business partners, suppliers and employees

reveal and consequently negative effects on their self-

constant activity would have to fear. Again, the required

Weighing of interests in principle in favor of the increasing self-

constant failure. In this respect, an information obligation of the top-up

to deny self-employment.

13.3

Forwarding of landlord data to tax authorities by the

job center or social welfare office

A transfer of landlord data to tax authorities in cases where

Doubts about actually existing leases, especially between

family members, is usually not in accordance with data protection law

reasonable. Such means of intended determination, in particular

Whether rent payments are actually made is available to the job center or

generally not available to the social welfare office.

facts

A Hessian district administration turned to a request for advice

to me: There it comes in the social administration in the scope

of the SGB XII (3rd and 4th chapter) occasionally states that the clerical work

considerable doubts as to the effectiveness of concluded rental agreements,

especially between family members.

At the same time, there is not always support on the part of the social welfare agency

the possibility of refusing the demanded rent. In order to

198

social affairs, video surveillance

tendential) to prevent performance abuse, there are considerations that

provided landlord data in suspicious cases to the responsible financial

to pass on to authority.

The basis for this could be Section 71 Paragraph 1 No. 3 SGB X in conjunction with Section 116 AO

(Notification of tax crimes). § 116 AO provides that courts and

the federal, state and local authorities of the public

Administration Facts that they learn on the job and that raise the suspicion of a

Justify a tax crime, have to notify the tax authorities. Problematic

could be from the point of view of the district that data would be passed on

those that were collected from the recipient of social assistance (e.g. rental agreement,

Rental certificate), but also the data of the landlord (third party)

would be passed on if e.g. B. a collusive interaction at

Rental contract is obvious or the suspicion that the landlord is the income

from the tenancy agreement at the tax office.

On this issue, the district has my data protection law

Opinion requested.

Legal Assessment

A transfer of landlord data to the tax authorities for the described

same case constellation on the basis of § 71 Para. 1 No. 3 SGB X in connection

with § 116 AO is usually not responsible.

This results from the consideration of these two in terms of data protection law

regulations.

Section 71 Paragraph 1 No. 3 SGB X

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

the statutory notification obligations (...),

3. to secure the tax revenue according to § 22a of the Income Tax Act and

Sections 93, 97, 105, 111 paragraphs 1 and 5, Section 116 of the Fiscal Code and Section 32b paragraph

3 of the Income Tax Act, insofar as these provisions are directly applicable

are, and to notify data of foreign companies based on

bilateral government agreements on the employment of workers

Execution of work contracts, according to § 93a of the tax code, (...).

§ 116 paragraph 1 AO

(1) Courts and the authorities of the federal, state and local authorities of the public

Administrations that are not financial authorities have facts that they learn in the course of their work

and which indicate a tax offence, the Federal Central Tax Office or,

to the extent known, to notify the tax authorities responsible for the criminal tax proceedings.

If the tax authorities responsible for the criminal tax proceedings have not already

The Federal Central Tax Office will inform you that you have been informed immediately

these facts with. The tax authorities responsible for criminal tax proceedings,

with the exception of the authorities of the Federal Customs Administration, transmit the notification to

the Federal Central Tax Office, insofar as this is not already recognizable directly in

notice has been given. (...)

My negative attitude is mainly based on the wording of

§ 116 para. 1 AO, which is based on facts that are officially experienced

and justify a suspicion of a tax crime. The express

According to the wording of the law, there are (considerable) doubts about the processing

just not out. "Only" in the case of facts is a notification to the tax office

(ex officio) displayed. This notification requirement is based on established

Fact-based presence of specific suspicions;

mere assumptions do not justify a notification obligation.

The district as the responsible body must (also in this case constellation)

lation) In addition, also be aware that he has an accountability

according to Art. 5 Para. 2 DS-GVO - at least towards me as the person responsible for him

Hessian data protection supervisory authority - which he accordingly (and

objectively comprehensible) would have to be able to prove.

Art 5. Para. 2 DS-GVO

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

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

A third party commits tax evasion or another tax crime

assume is a serious accusation, the hurdles for this must be

be set accordingly high.

Incidentally, it would be – assuming that in an individual case one could

Transmission on the basis of established facts

existing suspicion to be admissible according to the provisions mentioned – the

District administration also only possible, "only" a data transmission

to the tax office. Because the other way around, there would be nothing about it

said whether the tax authorities in turn have a power of transmission

would be available, which would allow her to the social administration then - in

for example - to inform: "Yes, Ms./Mr. XY gives in his/her annual tax

declaration of rental income for apartment ABC from Ms./Mr. DEF"

(or not). The social administration would therefore remain in the dark

and thus did not achieve its "goal" of proper case testing.

200

social affairs, video surveillance

I finally offered the district administration if it should be up to date

give special and concrete individual cases in the social administration,

this together with her to their admissibility under data protection law

check over. The social administration has not yet received any of this offer

made use of.

201

Economy, banks, credit bureaus, self-employed

14. Business, banks, credit bureaus, self-employed

Economy, banks, credit bureaus, self-employed

The large area of the economy, the banks, the credit bureaus and the

self-employed causes a variety of data protection issues. Also for

the reporting period are assessments of very different data

to report protection issues. This chapter is about accountants

(Chap. 14.1), banks (Chap. 14.2), credit bureaus (Chap. 14.3) and two companies

business models and their data processing operations that are relatively innovative

are (chap. 14.4 and 14.5)

14.1

Software provided by tax consultants

IT systems that tax consultants provide their clients with for secure

transmission of personal data without the intention of making a profit

makes available are not subject to the requirements of Art. 28 GDPR.

I keep getting inquiries about the applicability of Art. 28 DS-

GMO on specific facts. The background here is always the question of whether

for a specific situation, the conclusion of a contract within the meaning of

Art. 28 Para. 3 DS-GVO is required or not.

This time I got a request from a tax consultant. The tax advisor

provides its clients with a system with which the clients

Upload documents to cloud storage. The tax advisor

then takes the files uploaded from the tenant to the cloud storage

in its IT systems. The system is primarily used for secure transmission

of confidential documents in a protected and encrypted environment

giving. Admittedly, the tax consultant for the use of the system is due

the client demands remuneration. But this is based on the

cost price. There is no intention of making a profit.

The tax consultant now asked whether the transfer of the system

conclusion of a contract within the meaning of Art. 28 DS-GVO is required. The

I denied the necessity of concluding such a contract.

The defines when there is order processing within the meaning of the GDPR

GDPR itself does not. Although the GDPR prescribes which data protection

legal requirements it places on order processing. When this

is present, but results neither from Art. 28 GDPR nor from the definition

of the processor in Art. 4 No. 8 DS-GVO. Art. 4 No. 8 defines this

DS-GVO the order processor, but not the order processing. One

such is only present, however, if the personal data

by the contractor on behalf of and on the instructions of the client

are processed. Such a situation does not exist here.

Client and tax advisor can equally and for their own purposes

access the data loaded into memory. The purpose of the system is

not the processing of the data according to the instructions of the client, but

rather the secure transmission of the data to the tax consultant. she is

therefore an ancillary service of the tax consultancy contract. The tax advice

itself is not an order processing according to § 11 StBerG. According to § 11 paragraph 2

S. 1 StBerG, the processing of personal data takes place insofar as

this is necessary for the provision of the services of the tax consultant,

independent. Therefore, for the processing of data within the framework of

Steuerberatung does not have a contractual relationship within the meaning of data protection law.

The transmission of the data in a secure way is necessary for the provision of the

Services of the tax consultant are required and are therefore subject to § 11 paragraph 2

p. 1 StBergG. Even if this were not the case, an order processing would

processing in terms of data protection law, since the system is already

exclusively for the transmission of data and not for the processing of the

Data according to instructions is provided.

14.2

Collection of customer data by credit institutions

Banks are authorized to collect data on the activity (occupational group,

che) of their customers or the origin of assets

to collect in order to meet the requirements of the Money Laundering Act (GWG)

to be able to fulfill.

A frequent topic of complaints in the area of the credit industry is the

Banks' request to their customers, certain

to transmit data. In addition to the usual data, such as surname, first name,

date of birth and address, is also searched for data on the activity, in particular

to the professional group (or the profession itself), as well as to the industry in which the

activity is performed, asked. In other cases, call the credit institutions

Evidence of the origin of assets. In such cases, in the

Complaints submitted to me often on the legality as well as

asked about the permissible scope of data collection.

Basically, the collection of personal data u. then

is permissible if a legal norm requires the responsible body to do so

(Article 6 (1) subparagraph 1 (c) GDPR).

204

Economy, banks, credit bureaus, self-employed

Art. 6 GDPR

(1) The processing is only lawful if at least one of the following conditions

conditions are met: (…)

c) the processing is necessary for compliance with a legal obligation imposed by the

Controller is subject to; (...)

The GWG contains such a legal obligation. It obliges

ditinstitute to collect certain data based on risk. This follows from

the regulations on the general duties of care according to § 10 ff. GWG.

§ 10 GWG

(1) The general duties of care are:

1. the identification of the contractual partner and, if applicable, those acting for him

Person in accordance with Section 11 Paragraph 4 and Section 12 Paragraphs 1 and 2 as well as the examination,

whether the person acting for the contractual partner is authorized to do so,

2. the clarification of whether the contractual partner is acting for a beneficial owner,

and, if this is the case, the identification of the beneficial owner

Subject to Section 11 Paragraph 5 and Section 12 Paragraphs 3 and 4; this includes in cases in

where the contractual partner is not a natural person, the obligation to

to find out the control structure of the contractual partner by appropriate means,

3. the collection and evaluation of information about the purpose and about the

type of business relationship sought, insofar as this information does not differ in individual cases

already unequivocally derived from the business relationship,

4. Using appropriate, risk-based procedures to determine whether the

contractual partner or the beneficial owner of a politically exposed

person, a family member or a person known to be close

acts, and

5. the continuous monitoring of the business relationship including the

actions taken during its course to ensure that these

transactions match

a) with the documents and information about the obligated party

Contractual partners and, if applicable, about the beneficial owner, about their

business activity and customer profile and,

b) if necessary, with the information available to the obligated party about the

source of assets;

As part of the continuous monitoring, the obligated parties must ensure

that the respective documents, data or information, taking into account the

respective risks are updated at appropriate intervals.

Regarding the scope of the due diligence requirements, Section 14 (2) sentence 2 GWG requires:

205

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

In any case, the obliged entities must verify transactions and

Ensuring oversight of business relationships to an extent that allows them

allows to detect and report unusual or suspicious transactions.

What information and under what conditions do credit institutions collect

the supervisory authority responsible for the GWG, the Federal

desanstalt für Finanzdienstleistungsaufsicht (BaFin), on the basis of

§ 51 para. 8 GWG with its interpretation and application notes from

June 8, 2021 (https://www.bafin.de/SharedDocs/Downloads/DE/

Interpretation decision/dl_ae_auas_gw.pdf;jsessionid=288F6442B71F-

BAA666EA309F8F0A6863.2_cid503?__blob=publicationFile&v=17).

After that, there is an obligation for questions about employment

§ 10 Para. 1 No. 5 Letter a GWG the following authorization to examine: To

ordinary or suspicious transaction, e.g. B. Receipts of money to identify

can, the bank must u. a comparison between the height of

Incoming money and information on the activity (occupational group) and industry

carry out. if e.g. B. a customer indicates that he or she is a helper in the trade,

monthly but receipts of money are recorded, which are clearly in the amount

deviate from the usual inputs appropriate to the activity, the one

Be indicative of a money laundering related transaction that may be

would then also have to be reported by the bank.

For questions about the origin of assets, it should be noted that

Section 10 (1) no. 5 letter b GWG stipulates that the obligated credit institution

as part of the continuous monitoring of the business relationship

Transactions of customers with information about the origin of assets

must be balanced. According to the design and application

From June 8, 2021, the depositors must point out for cash transactions

provide proof of origin of the cash to be deposited. As

Proofs of origin are used here e.g. B. Account statements from other banks

kens from which the cash was withdrawn, cash withdrawal receipts,

Sales and invoice receipts and similar documents. The ones in this

The guarantees of origin submitted in connection with this are from the credit institution

then to record and store it in accordance with § 8 GWG.

In summary, it can be said that the collection of customer data

according to Article 6 Paragraph 1 Subsection 1 Letter c GDPR in conjunction with Section 10 Paragraph 1

No. 5 and 14 para. 2 sentence 2 GWG is permissible under data protection law, provided

with this data, the testing obligations imposed by the legislature

respective credit institution can be ensured.

206

Economy, banks, credit bureaus, self-employed

14.3

Information about data recipients by credit agencies

The third-party collection of personal data e.g. B. by credit agencies

In accordance with Art. 14 DS-GVO, active information is provided to the person responsible

towards the person concerned. According to letter e)

where applicable, the recipients or categories of recipients of the personal

name related data. On the naming of the specific recipient

may only be waived if the recipient at the time of

census not yet determined.

I received a complaint in which it was criticized that an

does not provide sufficient information about the recipients of the respective person

transmitted data would inform.

Credit bureaus are private commercial companies.

They collect information e.g. about the identity, the credit, the

Willingness and ability to pay of companies and private individuals.

This information is stored and transmitted to third parties when

they have a legitimate interest within the meaning of Article 6 Paragraph 1 Subparagraph 1 Letter f

DS-GVO have such information. Credit bureaus can also be used as

so-called third-party users for their customers in the context of address research,

e.g. B. in the case of undeliverable letters. Here the

Credit reporting from a creditor (who credibly has a legitimate interest

can do) commissioned, the current address of the invoice addressee

to detect. The credit agency then determines the address from third parties

(e.g. at residents' registration offices) and is due to the processing

they are then obliged to inform the person concerned in accordance with Art. 14 DS-GVO

to inform the processing of his personal data.

The background here are the transparency regulations in Art. 12 et seq. DS-

GMO. The principles of fair and transparent processing require

es, the data subject about the existence of the processing operation and

to teach its purpose. If the data is transmitted to third parties, it is

according to Art. 14 Para. 1 Letter e DS-GVO required, the data subject

the recipients or categories of recipients of the personal data

share data.

In the present case, the credit agency acted as a so-called third-party collector.

After checking the information provided, the complainant confirmed

just. In the information letter according to Art. 14 DS-GVO only the

"Requested address" and the "Collected address" provided information. Possible

Recipients of information were in an attached supplementary sheet in abstract

way described. The credit agency only informed the person concerned in the context

a further request with the actual recipient of the data.

According to Art. 14 Para. 1 Letter e DS-GVO, in the case of third-party collection

the data subject the recipients or categories of recipients of the personal

personal data are communicated. Whether the specific recipient or

only the categories of recipients to be communicated depends on the respective

circumstances, in particular the stage of data processing. Stands

the recipient at the time of notification according to Art. 14 DS-GVO not yet

fixed, it cannot be named either. In this case, only the

communicate categories of recipients. If at the time of collection

the recipient of the data is already known, but this is specific

to name. Since the credit agency is commissioned by a specific creditor,

locating the address of the person concerned is therefore the recipient

of the data as the client is known in advance. Consequently, this recipient

of the data according to Art. 14 Para. 1 Letter e GDPR. In

As a result, the credit agency was instructed to change the content of the information in accordance with Art. 14

adapt DS-GVO and thus in the future in all relevant cases

name recipients of information.

14.4

GO Kart & Guest Accounts

The decision of the Conference of Independent Data Protection Authorities

that of the federal and state governments (DSK) of March 24, 2022 with regard to the

There may be an obligation to set up guest accounts in online trading

also apply to situations in the analogue world. To safeguard the

principle of data minimization according to Art. 5 Para. 1 Letter c DS-GVO

therefore mandatory for the one-time use of a leisure facility guest

account models are offered. A retention of data,

for any future use of the leisure facility is not permitted.

I received a complaint against a go-kart track in Hesse

directed. There is a digital system for customers at the entrance to the go-kart track

for user data collection, which the user himself before using the kart track

operated via touchscreen. Extensive personal

related data is queried, without entering it a use of the kart track

was not possible. In particular, visitors had to name, address, telephone

and exact date of birth and a face photo (explicit

allow demand without face mask). By entering the data

you acquired a so-called "racing license", which was valid for one year. At that one

"Racing license" was a user account.

208

Economy, banks, credit bureaus, self-employed

On the home page, the operator also asked for confirmation of the liability

conditions. Except for the rudimentary information that the data from

Operators are processed were those required in accordance with Art. 13 DS-GVO

information not included. A comprehensive data protection regulation was
the linked nor were further information for further use, e.g. B.
by an insurance company, the external data protection officer
or similar, available. Information on the duration of storage and a possibility
to refuse consent to be granted were also missing.
After hearing this, I immediately asked the operator of the kart track to
change procedure. The main focus here was on reducing
adornment of the mandatory information, the obligatory taking of facial photos
and the missing information. He said the timely implementation of the
necessary changes.
An on-site appointment then took place to check the changes
employees of my authority in the karting hall. This showed
that the operator after the process adjustment although the possibility
had created the data protection consent for processing
to provide personal data by checkbox, without providing
However, the registration process could not be completed with the consent
become. Consent was therefore still mandatory.
The collection and processing of personal data within the framework
the "racing license" was issued by the operator, e.g. with the occurrence of any
case of liability justified. So he kept that data for a year. The
Customers no longer had to worry about repeated use of the kart track
register. The model was thus similar to the ongoing customer accounts model
in long-term business relationships in online trading.
The collection of the aforementioned personal data constitutes a
Violation of the principle of data minimization according to Article 5 Paragraph 1
Letter c DS-GVO. In addition, there is a violation of Art. 7 Para. 4 DS-

GMO before. According to this, the voluntariness of the consent to the processing
processing of personal data is not available if the provision of the
service is made dependent on the consent, but this for
the fulfillment of the contract is not required. The scope
of Art. 7 Para. 4 GDPR is primarily in connection with Art. 6 Para. 1
Subsection 1 letter b DS-GVO, according to which the fulfillment of the contract
necessary data processing is permitted without consent. The width
the scope of application for entities not covered by Art. 7 Para. 4 DS-GVO
declarations of consent is therefore low, because precisely for the fulfillment of the contract
required data processing does not require consent, which is why it
there is also a lack of necessity for these (Ingold, in: Sydow/Marsch,
209
The Hessian Commissioner for Data Protection and Freedom of Information
51. Activity report on data protection
DS-GVO/BDSG, DS-GVO Art. 7 para. 30-33). Those recorded by the operator
However, data were not required to fulfill the contract within the meaning of Art. 6 Para. 1
Subsection 1 letter b DS-GVO required and an assessment within the meaning of
Art. 7 para. 4 DS-GVO led to a lack of voluntariness of the grant
a consent.
Driving on the kart track was only possible if the affected
person had consented to the processing of personal data. Consequently
there was a coupling situation. Based on the guidelines of the EDPB
05/2020 from May 4th, 2020, there is currently no over and
subordination situation or even monopoly position of the person responsible.
Accordingly, consent can be considered non-voluntary, too
if a controller argues that between its service

tion, to which the consent to the use of personal data for

additional purposes, and a comparable service that

is offered by another controller, a choice

exists (on the controversy as to whether a monopoly position must exist, see

Stemmer, in: BeckOK DatenschutzR, DS-GVO Art. 7 No. 46; Schulz, in:

Gola/Heckmann, DSGVO/BDSG, 3rd edition 2022, DS-GVO Art. 7 paras. 19-34).

In the present case, the decision of the conference of the independent

pending federal and state data protection supervisory authorities

March 24, 2022 (DSK, data protection compliant online trade

via guest access, https://www.datenschutzkonferenz-online.de/media/

dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf). Thereafter

must be responsible for the goods or services in online trade

offer to their customers regardless of whether they give them

in addition, a registered user access (continuous customer account)

provide, basically a guest access for the order

provide. The Kartbahn is not an online mail order

dealer. Nevertheless, the principles of the DSK decision are to be applied.

In the case of a one-time use of the kart track, the person responsible cannot

per se claim that he collects data from customers for possible

may reserve further but uncertain future journeys.

The use must therefore also without providing personal data

to be possible. Consequently, I have instructed the operator to take the opportunity

set up a guest account. He has also implemented this. In addition

he revised the data protection declaration and a DS-GVO-compliant

possibility of consent created.

Economy, banks, credit bureaus, self-employed

14.5

360° panoramic shots when driving on roads

As the legal basis for the collection of personal data for

Provision of 360° panorama shots in which personal data

such as house facades, license plates and the appearance of people

may be included, Art. 6 Para. 1 Subparagraph 1 Letter f DS-GVO comes into play

consideration. If the images are not published and not necessary

such personal data are made unrecognizable

No unconditional objection on the part of the data subjects

right. The possibility for data subjects to object in accordance with Article 21

Para. 1 DS-GVO e.g. B. to appeal against the image of the house facades,

however, remains unaffected. However, this right must be explained and can

can also be refused by the person responsible if none are sufficient

comprehensible reasons were presented by the applicant for

the removal or de-identification of the data.

I am receiving more and more inquiries from citizens who

in their communities notice road traffic by vehicles that

are equipped with cameras. The company active in these cases

is based in Hesse, which is why I am associated with it

dealt with data processing in the reporting period.

Recording of 360° panoramic images

The company collects 360° panoramic views with specially equipped vehicles

norama images of public space and laser point clouds using a

nes LiDAR scanner by road traffic. So becomes a citywide

Geographical information system, extended by 360° panorama images, created

and as a "digital twin" via license agreements to the municipalities and other

other actors and target groups (mainly in services of general interest, e.g.

Network operators, telecommunications providers) are made available. This

acquire appropriate access and use this to carry out their tasks

to be able to fulfill more effectively and efficiently directly from the office, so that

On-site visits can be reduced or even omitted entirely. application

are found, for example, in the context of urban design, e.g. B. around the

To evaluate the building fabric of real estate or the greening and the

Document the condition of trees and green spaces. Also in the area

operational planning, e.g. B. at events or fire brigade operations,

the data are used. It is also possible in the "digital twin"

To visualize scenarios such as heavy rain events in order to

to include the described effects in the disaster control planning

hen. The data are not public, but only by the named and

limited user group available.

In addition to the geographic information, such as addresses or corresponding geographic coordinates

data, further personal data become when driving on the road

Data such as images of house facades as well as people and vehicles

recorded in public space, for which there must be a legal basis.

There is always lawful processing of personal data

occurs if one of the requirements of Article 6 paragraph 1 subparagraph 1 letter a bis

f GDPR is fulfilled. In this respect, the "permission principle" applies in data protection law,

because data processing is always permissible if permission is granted

inventory is given (Roßnagel, NJW 2019, volume 1-2, p. 5).

With a decision of May 20, 2020, the conference of independent

Data protection supervisory authorities of the federal and state governments also after validity

of the DS-GVO their legal opinion, according to which in the context of StreetView

and similar services Art. 6 Para. 1 Subparagraph 1 Letter f GDPR as a legal

basis for processing street views, including partial

These images of house facades and private property areas,

which border on the public street space, come into consideration

can (DSK, decision on preliminary objections at StreetView and comparable

available services, 2020, https://www.datenschutzkonferenz-online.de/media/

dskb/20200526_beschluss_vorabwidersprueche_bei_streetview_und_ver-

equal_services.pdf). Features like faces and license plates are

however, to make it unrecognizable. As part of the balancing of interests

is also a request of those affected when the data is published

Individuals to de-identify their data to be considered to which

also illustrations of house facades and private property areas

are to be counted.

balancing of interests

Provided thereafter private companies panoramic shots of the public

room, the legal basis can be Article 6 Paragraph 1 Subparagraph 1 Letter f

DS-GVO are used. After that, processing is personal

The data collected is permitted if it is used to protect legitimate interests

of the person responsible or a third party and the interests

or fundamental rights and freedoms of the data subject requiring protection

require personal data, do not prevail.

The existence of the requirements of Art. 6 Para. 1 Subparagraph 1 Letter f DS-

GMO is tested using a three-stage test procedure. First will

determines the legitimate interest of the controller or a third party. In the

212

Economy, banks, credit bureaus, self-employed

A check is then carried out to determine whether the intended data processing is

Protecting the legitimate interest is also required. Finally will

the actual balancing of identified legitimate interests

of the controller and the third party with the interests, fundamental rights and

fundamental freedoms of the person concerned in the specific individual case

men (DSK, guidance from the supervisory authorities for providers

Telemedia providers from December 1, 2021, pp. 30-31, https://www.

datenschutzkonferenz-online.de/orientation aids.html).

The legitimate interest of the companies according to Art. 4 No. 7 DS-GVO

are to be regarded as responsible is an economic interest. Then

the personal data are used for the purpose of creating and

commercial marketing of so-called "digital twins". In this

context is to be considered that the legitimate interest far

is laid out (Simitis/ Hornung/ Spiecker gen. Döhmann-Schantz, data

property right, DS-GVO Art. 6 Para. 1 Rn. 98) and the existence of economic

interests has already been recognized by the ECJ (ECJ, judgment of 13.

May 2014 - C-131/12, paragraph 81).

The second test step, which determines the necessity of data processing,

is explained in recital 39 DS-GVO to the effect that the personal

personal data for the purposes for which they are processed,

be reasonable and relevant and limited to what is necessary

must. Thus, the data are only to be processed if the purposes associated with them

be prosecuted, not in a reasonable manner by other, milder means

can be reached. In contrast to the legitimate interest, the

Necessity to be interpreted narrowly (Kuhling/Buchner-Buchner/Petri, 3rd ed.

2020, GDPR Art. 6 para. 147a).

The inclusion of house facades is explicitly intended in order to

mune as a customer added value for their administrative work via the

to offer a digital twin. As an example, it is advertised that

Administrative procedures such as the granting and enforcement of various

permits or urban design measures more efficiently and effectively

to allow. Without the recording of the house facades such would be

Use not possible. So there is no other way to do it.

On the other hand, both the license plates and the recorded ones

people are not necessary. However, it is when driving on roads

unavoidable to collect this personal data. A milder one

Funding does not seem to be available here either. However, the

Limiting data processing in these cases to what is "absolutely necessary"

zen (ECJ, judgment of May 4, 2017 - C-13/16, para. 30). data accordingly

are not required are to be made unrecognizable accordingly. The DSK

213

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

has therefore correctly determined that this is at least for the faces and

License plates should be made when creating panoramic images

(DSK decision of 2020, see above). In practice, these data are therefore

usually automatically while driving through AI technology

pixelated.

This rendering unrecognizable is finally also in the third level of
to take into account the balancing of interests and is a recognized method
in order to "reconcile the often conflicting interests (...) into an appropriate
to bring balance" (OVG Lüneburg, decision of January 19, 2021 -
11 LA 16/20, paragraph 25). Data processing according to Art. 6 Para. 1
Subsection 1 letter f DS-GVO is already permissible if the interests of the
those responsible are equivalent to those of the data subject. only one
overriding interest of the person concerned leads to a corresponding
Exclusion.
However, there are many factors to consider when making the assessment, e.g. B. the
purpose, the risk of data processing and the intensity of the intervention,
the data category and its "public accessibility", the technical
and organizational measures and the reasonable expectations in the
With regard to data processing (Recital 47 DS-GVO) and the
Possibility to reasonably refrain from such processing
(Taeger/Gabel-Taeger, 4th edition 2022, GDPR, Art. 6 para. 148f.).
The legitimate interest of the data subject is to protect theirs
informational self-determination and their privacy. the
Companies, in turn, can invoke their basic economic rights
(Art. 12, Art. 14, Art. 19 (3) GG).
In this specific case, people, license plates and house facades
recorded in connection with geo-coordinates, which are in the public
ness or in areas that are in public space, e.g. B. by a
stay in the corresponding spatial environment, perceived
can become. In this respect it concerns z. B. the house facades that face the street
aligned, and vehicles parked in front of the building, or

people who are on sidewalks or in front gardens. data like that

License plates or the house facade are therefore publicly accessible

or viewable.

Nevertheless, the house facades and those belonging to the residents of the

Vehicles to be assigned to the building are generally suitable for providing information

about personal living conditions. For example, the

External appearance of the house and garden in connection with the

Number and condition of the vehicles assigned to the residents

Provide information about their financial and family circumstances. Insight

214

Economy, banks, credit bureaus, self-employed

in the front yard, for example, is often sufficient to provide information about it

to find out if there are children living in the house and what their age range is

to find oneself. Because typically there are indications such as toys,

Identify swings, slides or pedal and slide vehicles. As well

is it possible, due to the location and the fabric of the building

to draw conclusions about its economic value.

However, it turns out that the data that is in the public domain

have a lower protection requirement. The Federal Constitution has

1983, the Supreme Court found that such data “represents social

reality" and the right to informational self-determination of the

Individuals can be restricted in this context (judgment of

December 15, 1983 – 1 BvR 209/83, para. 156).

But there is undoubtedly a difference between the possibility of

via panorama shots or a digital twin developed from them

to get an overview of the environment in peace and quiet,

and on-site inspection.

Consideration of the addressee group

Within the balancing of interests is therefore a more detailed consideration

the group of addressees to whom the data is available and their

purposes necessary.

In contrast to Google Street View or Apple Look Around, the

Images are not disclosed to everyone, but are licensed to a specific

th group of people, in particular authorities, made available to the

In turn, they may only use data for their own legitimate purposes. Over

corresponding mandatory data protection information is therefore possible

and required to make the data subject transparently aware of who

processes the data and for what. This is less for one release

clearly recognizable.

In addition, it should also be noted that the personal data recorded

drawn data do not have a high level of protection, since they

are publicly visible. Furthermore, the recipient of the data - i.e. in

In the case of providing a digital twin, the municipality itself - one

Have a legal basis that allows the data to be transmitted to you and a

appropriate further processing permitted.

As a rule, this can result from the fulfillment of tasks in accordance with Article 6 Paragraph 1 Subparagraph 1

Letter e DS-GVO in connection with § 3 HDSIG and/or the respective

relevant regulations of the area-specific laws exist.

No publication and the data will only be available for a limited time

and identifiable group of people, e.g. B. within the commune for legitimate

purposes is therefore excluded within the balancing of interests

ensure that the legitimate interests of those affected do not prevail

and corresponding data processing in accordance with Article 6 Paragraph 1 Subparagraph 1

Letter f DS-GVO is legally permissible. Of course, that is a prerequisite

at least the faces of the people recorded and the license plates

be made unrecognizable.

Furthermore, there is still the possibility on the part of those affected

Persons, objection in accordance with Article 21 (1) GDPR e.g. B. against the

to insert the building facades. The reasons for exercising this

However, the law must be explained and the implementation can be carried out by the person responsible

chen also be refused if no sufficiently comprehensible

Aspects put forward by the applicant that are relevant to the removal or

talking about data redacting.

Improving transparency

In a specific case, it turned out that the cause for some with me

received complaints is often a lack of transparency. That's how it is

tour calendar and the associated data protection information

on the website of the Hessian company and on the website of the

Geodatenkodex published, however, this information reaches the

Affected people often do not, so that irritation and uncertainty

arise when the vehicle is sighted on the road.

The Hessen-based company therefore assured that in the future

in addition to publishing the inspection dates on its own website

and, if necessary, stimulating reporting in local newspapers in addition

clearly visible QR codes are attached to the vehicles

those affected who see the vehicle directly via the link of the QR

Codes to get to the corresponding stored data protection information.

The implementation should take place in the following year.

15. Health sector

health sector

The processing of health data is doubly explosive: on the one hand

it's about processing data for people's health

to provide for, preserve or restore them. On the other hand it works

in the case of health data, a special category of personal data

Data for which informational self-determination is carried out with particular care

is to be preserved. The corona pandemic, which occurred in the last two reporting years

has demanded special attention from the data protection supervisory authority

no longer so prominent in this reporting period, albeit

corrective action was still required (see Chap. 15.2, 15.3

and 15.5). Rather, there was a reason and an opportunity to express yourself through accompaniment

of legislative procedures also to the conditions of health

to take care of data protection (see Chapter 15.1). After all, the task was

Data protection supervision, compliance with the obligations of those responsible

check (see Chapter 15.4) and to protect the rights of the data subject,

asked - using the example of information (see Chapter 15.6) and correction (see

Cape. 15.7).

15.1

Accompanying legislative projects in the health sector

In the reporting period, advice on legislative projects was a major

point of my activity. In order to provide an insight here, I would like to

The following of the main results of my consulting practice in

Context of the amendment of the Hessian Cancer Registry Act (HKRG),

of the Hessian Hospital Act (HKHG) and the Hessian Law

zes report on help with mental illnesses (PsychKHG). in all

I was able to design these areas in a data protection-friendly manner

work towards the planned regulations.

Amendment of the HKRG

In the context of the amendment of the Hessian Cancer Register Act

by the Hessian Ministry for Social Affairs and Integration (HMSI)

and the research bodies clearly communicated the wish that the

expanded the possibility of data transmission to external researchers and

Research results and data sets for research purposes better

are to be made usable. I supported this wish and

paying special attention to the clarity and specificity of the

planned standards (see §§ 9a and 9b HKRG-E).

The new legal basis for the transmission of anonymous and pseudo-

anonymized data contains mechanisms and guarantees to protect the

interests of the persons concerned. The projects covered by the standard

health services research must focus as far as possible on the use

Limit anonymized data. It is imperative for the researchers to

provide a meaningful data protection concept. In addition to the strict

Purpose limitation is the transfer of data to third parties and identification

of data subjects are prohibited by law. Also a stake

of the scientific advisory board is planned.

In addition, there was a special desire to participate in existing cancer

to orientate themselves to other countries' registers and to a certain extent to it

enable, despite an objection by the data subjects

after deletion of the identity data with the clinical and epidemiological

to continue working on the data (see § 7a HKRG-E). Since in Hesse there are anyway

possibility, the right of objection of the persons concerned is in the interest

to limit the research purposes (see § 24 para. 2 sentence 1 HDSIG).

I worked towards a justifiable balance of interests. accordingly

Accordingly, the remaining data set was kept as small as possible

further corrective measures in terms of data protection achieved. So will the of

data collected after an objection is completely deleted after seven years.

Transmission to external researchers is excluded. Besides that

should be evaluated after seven years whether this restriction of the Wi-

the right of appeal is still necessary for the cancer registry.

Finally, I also supported the initiative, the omitted report

to be sanctioned by the notifying doctor. Corresponding facts

de for administrative offenses already exist in other federal states (e.g.

Rhineland-Palatinate, Baden-Württemberg, North Rhine-Westphalia, Schleswig-Hol-

stein), so that Hesse has also followed suit here with the new regulation.

From an extension of the already very long retention period

Identity data (ten years after death or no later than 130 years after

the birth of the person concerned, cf. § 14 HKRG) was due to my

concerns dismissed.

Amendment of the PsychKHG

I was also involved by the HMSI in the amendment of the PsychKHG

tied. In this respect, Section 14 (1) sentence 2 PsychKHG-E should provide a comprehensive

Catalog of data included by psychiatric hospitals

the technical supervisor (HSMI). After the justification of the law

it was not personal data:

218

health sector

"Since no personal data is transmitted, the

Anonymization is guaranteed and conclusions can be drawn about individual

brought people [are] not possible."

I did not share this perspective. Already the date of the accommodation

ginns and the date of discharge should be recorded to the day and were

so in the combination already taken by itself usually only one

assign person. Consequently, they were clearly personal. This

was corrected and subsequently regulated, the data only in coarser

ter form (quarter of admission and quarter of discharge).

The data to be transferred to the HMSI in accordance with Section 14 (1) sentence 2 nos. 1 to 14 PsychKHG-E

averaging data should also contain a large amount of sensitive data

according to Art. 9 DS-GVO (diagnoses, treatment measures,

security measures). It was therefore also important to me that in § 14

PsychKHG clearly regulates the purposes for which this data is collected from the HMSI

are processed and that a strict earmarking of the collected data

mentioned in the law.

Amendment of the HKHG

Also with regard to the amendment of the Hessian Hospital Act

a new regulation in § 12 Para. 5 HKHG could be obtained. After that are

now the Hessian hospitals, which are subject to the HKHG

obliged to develop concepts for the secure storage of files in the event of their insolvency

to create and maintain. More information can be found on mine

Homepage (see https://datenschutz.hessen.de/datenschutz/gesundheitswesen/

protection-of-patient-data-when-hospitals-close).

Outlook on upcoming legislative projects at federal level

Finally, it should also be mentioned that I spoke about the newly founded task force

Research data (see Chapter 16.1) also in the planned new regulations

am involved at the federal level. The Chair of the Task Force Research

ten, consisting of BfDI and myself, has the development process of the

Research Data Act and the Register Act are and will be followed

support further implementation.

15.2

Decree on facility-related compulsory vaccination

For the introduction of the institution-related vaccination obligation according to § 20a IfSG

In March 2022, the HMSI issued a decree to implement Section 20a IfSG in

Hesse published. I advised the HMSI on this in advance and

I successfully advocated more data-efficient regulations in the decree. So

could be ensured that only to fulfill the legal

Obligations from § 20a IfSG required personal data

collected from employers and, if necessary, to the responsible health authorities

be transmitted.

background

On December 12, 2021, the law to strengthen vaccination
prevention against COVID-19 and to change other regulations in the
in connection with the COVID-19 pandemic (Federal Law Gazette I p. 5162). With
this law was u. a. the institution- and company-related
Obligation to prove vaccination, recovery or contraindication in
§ 20a IfSG introduced.

Like the new facility-related vaccination requirement by the health authorities
to be implemented in Hesse required more detailed provisions. Also from there
From the point of view of data protection law, a number of questions arose that were not clear
stipulated by the federal legislature. The lead HMSI
therefore asked me for advice on this matter at an early stage.

Data protection assessment

According to § 20a Para. 2 S. 1 and Para. 3 S. 1 IfSG, employees of the
institutions and companies covered by the law of the management of these companies
and facilities must provide appropriate proof (proof of vaccination,
proof of recovery, medical certificate). Didn't do this until
as of March 15, 2022 or there were doubts about the authenticity or content
The correctness of the proof presented was the responsible health authority
to notify and it was personal information to this
transmit (§ 20a Abs. 2 S. 2 and Abs. 3 S. 2 IfSG). The evidence itself
However, according to the principle of data minimization (Art. 5 Para. 1
Letter c DS-GVO) not copied or stored by the employers
become. After checking the evidence, the employers were only allowed to store
that valid proof has been submitted and, if applicable, the expiry date of the
Evidence, since this information is required to fulfill legal obligations
from § 20a IfSG were sufficient.

health sector

In an official model for a medical certificate about a con-

traindication as proof to the employer was allowed for reasons of

Data minimization and, if it is not necessary, the specific diagnosis is not

to be named. Rather, it was sufficient if in such a medical

Certificate established that a medical contraindication

against a COVID-19 vaccination.

The transmission of evidence to the health department was not

intended and therefore impermissible. It was allowed according to the principle of

Data minimization only the reason for reporting and the personal data

according to § 2 No. 16 IfSG (name, address, contact details) to the responsible person

be sent to the health department.

Section 20a IfSG expired on January 1, 2023. The corresponding

de Obligation of the institutions and companies and thus the data

legal basis for the processing of personal data

Data. Employee data collected on the basis of Section 20a IfSG

were to be deleted or destroyed by December 31, 2022 at the latest.

In the decision of April 13, 2022, the DSK issued "For the processing of personal

related data in connection with the institution-related vaccination

obligatory" confirms these data protection assessments on § 20a IfSG.

Result

As part of the advice given by the HMSI, I was able to achieve the above

mentioned data protection requirements in the implementation of the

facility-related compulsory vaccination in Hesse fully taken into account

became. Even when setting up the digital reporting portal for

I was involved in an advisory capacity with regard to compulsory vaccination and was able to

work towards data protection-compliant processes.

15.3

Data protection in test centers

In the health sector, the consultation and review of COVID test

centers is a focus. The data protection laws I have identified

The failures of the test centers were compensated by sensitization of the

employees, adjustments to technical processes and revisions

of the documents. In some cases I have fine proceedings

initiated.

background

During the reporting period, COVID testing centers were frequently the subject of

Complaints. Numerous test centers also asked for advice on

data protection-compliant design of their processes. As the COVID-

Test results according to Art. 4 No. 15 and Art. 9 Para. 1 DS-GVO in particular

health data to be protected is subject to the operators of

test centers high data protection requirements (see also Chapter 5.2).

Unfortunately, these legal requirements were not always met, so that

my intervention became necessary. Here I found that

the data breaches encountered are similar and regularly under one

of the following topics can be summarized.

Collection of unnecessary data

When registering online or on site, in principle

lich only such personal data from the persons to be tested

are queried and collected, to carry out the COVID test and

are required to fulfill the associated legal obligations.

Some test centers submitted during the supervisory procedure that personal

National IDs would be copied to verify information or to meet obligations

from the Coronavirus Test Ordinance (“TestV”).

However, the coronavirus test regulation does not require the preparation of one

Copy of the identity card nor the documentation of the identity card

white number. According to Section 6 Paragraph 3 No. 4 TestV, the person to be tested has to

their identity by submitting a citizen test to the provider

official photo identification. A visual inspection with data

adjustment is sufficient here.

Therefore, copies of ID cards are not allowed by the operators

of the test centers are generated. In individual cases, however, the collection of

ID card number may be allowed if required, e.g. B. at

the use of the identity card number for international test certificates

and if the data subject has consented to it.

Inadequate privacy statements

The test center has the persons to be tested when collecting their data

to provide the information specified in Art. 13 GDPR. You need to

in particular about the name and contact details of the person responsible,

the purposes and legal bases of the data processing, the recipients

of data and the rights of data subjects. At this point should

they also state that within the framework of the tests according to Art. 9 Para. 1

DS-GVO process specially protected health data.

The information according to Art. 13 DS-GVO ("Privacy Policy") must

the test centers to the citizens to be tested in the test center

make available on site, especially for the people who are not

register online and therefore not already in the online registration

can take note of the data protection declaration. copies of the data

must be in stock so that a copy can be requested

can be given to the person concerned.

The reference made by some test centers to the general

Website privacy statements may reflect legal requirements

Art. 13 DS-GVO do not meet. Because there is a lack of concrete information

to the data processing in connection with the test execution.

Here I was able to improve the information texts and for

ensure more transparency towards the persons concerned.

In one case, the operator of the test center remained due to a lack of proper

Data protection declaration unknown and only possible with the support of the

be determined by the health authorities. By this blatant violation of

Art. 13 Para. 1 Letter a DS-GVO the persons concerned could not

know who is responsible for the processing of their data and towards

whom they can exercise their rights. Also in this case I click the

fulfillment of the information obligations. In addition, I check

further supervisory measures against the person responsible.

Inadequate discretion and lack of access protection

According to Art. 5 Para. 1 Letter f and Art. 32

DS-GVO obliged to protect the personal data of the persons concerned

to protect people from unauthorized access and knowledge of third parties

Zen. Therefore, the premises of the test centers must be designed in such a way that
the customers cannot see the screens of the test center
have. The test results are only to be disclosed to the tested person,
so that the calling out of the test result is in front of the people waiting
of course forbidden. Also the documentation of the test results
and the test certificates must be kept safe. Appropriate
Paper documents are in particular also outside the opening hours
of the test center in a safe and locked place.
These basic rules on discretion and access protection in the
Test center were unfortunately ignored by some test centers. in one
case, the test certificates were in an unlocked box in public

accessible rooms of a town house. In another
case, parts of the written test documentation with personal
nal data is used as a “slip” and disclosed to third parties
(see Chapter 5.2). Here regulatory measures were taken against both test
center operator required.
The internal guidelines for the user
interface for test management open. The username and password
for access to this web interface were therefore visible to third parties.
This allowed unauthorized third parties to log in and personal
retrieve genetic data of the tested persons. Because of the generic
Username ("Testzentrum1") and the weak, easily guessed one
Passwords (street name + 2022) were also easy to enter the access data

for other test centers of the same provider. against the provider

of the test centers I initiated a fine procedure.

Security in the electronic transmission of the test result

Even if the test certificate is sent to the tested persons electronically

is provided, the test centers must provide the personal

Data according to Art. 5 Para. 1 Letter f, Art. 24 Para. 1 and Art. 32 Para. 1 DS-GVO

through effective authentication mechanisms sufficient before access

protect unauthorized third parties. The transmission of the test results by

E-mail regularly requires effective content encryption.

I already have the requirement for such an encryption in my

last activity report (see 50th activity report, chap. 17.2., p. 184

et seq.). In its orientation guide “Measures for

Protection of personal data when transmitted by e-mail" (https://

www.datenschutzkonferenz-online.de/media/oh/20210616_orientation-

hilfe_e_mail_verschluesselung.pdf) comprehensively with the requirements

engages in such transmission by email.

In practice, the necessary encryption of test center

drivers e.g. B. by using an encrypted attachment. As

For example, the Advanced encryption method is recommended

Encryption Standard (AES) with a sufficient key length (256

bit or longer). Responsible persons can choose others in

Procedures in question, for example, on the technical guideline

"Cryptographic methods: recommendations and key lengths" (BSI TR-

02102-1) of the BSI (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/

Publications/Technical Guidelines/TR02102/BSI-TR-02102.pdf).

Such encryption can be made using generally available

health sector

Software that is sometimes also a standard part of current operating systems

is, can be applied to common file formats such as ZIP files.

The password must be sufficiently complex and, in particular,

Third don't be easy to guess. Therefore, it should not be obvious

gene characteristics of the person can be derived. The date of birth is appropriate

therefore not as a password. A brute force attack would be this

also very easy to guess, since the number of possible combinations

nations is very low. The BSI keeps low-threshold information on

selection of suitable passwords on its website (https://www.

bsi.bund.de/DE/Themen/Consumers-and-Consumers/Information-

na-and-recommendations/cyber security recommendations/account protection/

create-safe-passwords/create-safe-passwords_node.html).

Further requirements for passwords with a view to the broader one

context of IT security can be found e.g. in the ORP.4 block (identity and

Authorization management) of the IT baseline protection compendium of the BSI

(https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/

Compendium_Individual_PDFs_2021/02_ORP_Organization_and_Personal/

ORP_4_Identitaets_und_Authorization_Management_Editon_2021.pdf?__

blob=publicationFile&v=2).

Such a password may only be sent to the

data subject are transmitted. If the transmission of the

content-encrypted test result via email, so email comes as a means

therefore no longer suitable for password transmission. Since Art. 32 Para. 1 DS-

GMO requires controllers to assess the risks of processing personal

related data, they would have to consider the possible risk here

unauthorized access to the receiving e-mail inbox

and therefore assume that a single unauthorized access at the same time the

disclose the data to be protected as well as the password granting protection

would. For the password transmission must therefore be on an alternative medium,

such as telephone or SMS, are avoided.

In supervisory practice, a number of complaints showed that these

Requirements for submitting test results are not consistent

were taken into account by the test providers. Therefore I had to

procedures in many cases for a better protection of the test certificates, e.g. B.

by using a second authentication factor. Such

Above all, multi-factor authentication may also be required

den, if the responsible body for retrieving the test results

online service uses. When evaluating the appropriateness of such

Service lays my authority u. a. the requirements of the guidance

"Requirements for providers of online services to secure access"

the DSK (https://www.datenschutzkonferenz-online.de/media/oh/20190405_

oh_Provider_onlineservices.pdf).

Frequently, the necessary changes could only be made by the

technical service providers employed by the test centers. while has

shown that a regulatory action against the provider

the technical solutions for the electronic provision of test certificates

kate is significantly more effective than taking action against individuals responsible

test site operator.

In one case I also had to prevent the test result

was already mentioned in the subject of the respective e-mail.

Incorrect delivery of test results

With COVID test results being sent out thousands of times a day, it is

not uncommon that due to an oversight or a typo

a test result is sent to the wrong person. As far as the technical

cal protective measures such as the encryption of the test result (see

above) have been complied with, the person incorrectly addressed has

a misdelivery by e-mail, however, regularly no access to the

test result. This shows how important it is to choose appropriate

its technical protective measures. It is also important that the

Operators of test centers comply with their obligations to report a data breach

Art. 33 DS-GVO and have implemented corresponding processes,

in order to be able to react in accordance with the law in the event of such incidents.

Conclusion

The business model of the COVID test centers has now existed for more than two

years, so that data protection-compliant processes have now been established here

should have. When it comes to data protection, however, the operators have

still some catching up to do. Test center operators

in Hesse should be aware that the determination of a serious

major data protection violation to a not inconsiderable fine

can lead. For some operations I already have the opening of a

fine proceedings initiated. In this activity report, in Chap. 5.2

several fine proceedings against test center operators are presented in more detail.

I have more information about the data on the website of my authority

tenschutz published in test centers (https://datenschutz.hessen.de/daten-

protection/healthcare/data-protection-in-sars-cov-2-rapid-tests). This

Publication is intended to help the operators of the test centers in fulfilling their

data protection obligations and was able to clear up some ambiguities

226

health sector

remove. Beyond the COVID pandemic, it can also be used by the operators of

Test centers offer assistance for other test-relevant diseases,

to recognize and fulfill their data protection obligations.

15.4

Upload medical images to the cloud for retrieval by the

patients

Uploading medical images to a processor's cloud

a radiological practice does not require the consent of the patient

or the patient. The creation of the images and the processing of these for

an uncomplicated transmission to the doctor treating you is required for fulfilment

the contractual obligation of the radiological practice within the meaning of Art. 9 Para. 2

Letter h DS-GVO required.

Complaint against uploading images

As part of a complaint I had to assess whether it was

when medical images are uploaded by a radiological practice

in the cloud of a processor for retrieval by the patient

or the doctor treating you for an additional service without a suitable one

Legal basis for the patients and therefore a

consent would be required.

The complainant was due to a referral to

Provision of medical images in treatment in a radiological practice.

Before the treatment, she expressly stated that her health data

may not be passed on to third parties. She wanted before a possibly

necessary disclosure and asked for consent.

After her treatment, she was given a CD containing her

examination images were stored, an information sheet with information

information on accessibility. With that she could

Access examination images online as well. For this purpose, their sub-

search images are sent to an order-processing service provider.

If this is not desired, the practice asked for feedback. The access

will then be deactivated and the pictures will be deleted.

The complainant then asked for the immediate deletion of the

Online access and your examination images from the server of the external

service provider. The practice complied with this request immediately. There

the complainant felt insufficient about

been informed about the transfer of the data to the external service provider

and that a transmission would not have taken place without your consent

allowed, she turned to me with a complaint.

The practice argued that making the images available via the

online functionality of the external provider to their contractual obligation

belong and same as handing out the pictures on a CD. The first

renting and making the images available in this way is hers

Order as patients use the images for their treatment

needed at another doctor. In addition, practice has shown that

fewer and fewer patients and medical practices CDs at all

could read because they hardly had CD-ROM drives anymore.

Legal Assessment

I followed the reasoning of practice and have some processing

accepted on the basis of Art. 9 Para. 2 Letter h DS-GVO.

The collection, storage and use of health data by

a treating doctor is part of the treatment contract and

the scope required for the treatment according to Art. 9 Para. 2 Letter h

last alternative DS-GVO without the patient's declaration of consent or

of the patient permitted by law. After that, in particular

Name, contact details and insurance number of the patient, medical history

nese and treatment documentation, doctor's letters and laboratory reports too

be processed without consent.

If a medical practice offers additional services such as B. a newsletter or

wants to offer a recall service, the related processing of patient

duck data due to the not covered by the treatment contract

For the purpose only with the consent of the patient within the meaning of

Art. 9 para. 2 letter a DS-GVO permissible.

In this case, it had to be considered that a radiological practice in

is essentially a reporting body that is largely based on referral

ment by other medical specialists. It is therefore mainly

to a co-treating facility. The medical images become

Created for the purpose of passing it on to the treating physicians. The creation of

Images and the processing of these for an uncomplicated transmission

the attending physician is therefore responsible for fulfilling the contractual obligation

radiological practice within the meaning of Art. 9 Para. 2 Letter h DS-GVO required

lich. It's not just an additional service.

In this respect, the transmission to a processor was not allowed

complain. The processor is not a "third party" within the meaning of the DS-

GVO (see Art. 4 No. 10 DS-GVO: "except […] the processor"). It

228

health sector

exists rather between the responsible person issuing the order

and its processor an "internal relationship". Processing by

the processor is therefore in principle the person responsible

attributed. For the transfer of personal data to the

contract processor and the processing by the processor

there is usually no further legal basis within the meaning of Articles 6 to 10

DS-GVO as the one to which the person responsible carries out the processing himself

(Data Protection Conference, Briefing Paper No. 13, https://datenschutz.hessen.

de/sites/datenschutz.hessen.de/files/2022-08/kurzpapier_nr.13_auftrag.pdf).

The possibility of using IT service providers by professional

Bearer of secrets was made aware of by the legislature in § 203 paragraph 3 sentence 2

StGB expanded. In the explanatory memorandum, the storage of data

expressly mentioned in the cloud (BT-Drs. 18/11936, p. 18):

"For all persons named in Section 203 Paragraph 1 of the Criminal Code,

the storage of data on external information technology

systems (e.g. in a “cloud”) make economic sense. This

economic interests of persons subject to professional secrecy are fundamental

additionally entitled, provided, however, that they are in accordance

may be brought with the legitimate interests of the holders

of secrets to their legal protection.”

Such use of external service providers is therefore not per se

objectionable, provided that other data protection reasons do not arise.

against, which is also not the case in the case I am working on

was. It should be taken into account that for such processing activities

already due to the special categories of personal data

Art. 9 GDPR requires a high level of protection. For the deployed

Online service should meet the requirements of the “Requirements

to providers of online services for access security" of the DSK (https://

www.datenschutzkonferenz-online.de/media/oh/20190405_oh_lieferant_on-

linedienst.pdf) must be taken into account.

If this is taken into account, the reference to radiological practice will apply

the state of the art, which in many places is already saying goodbye to physical

Storage media such as the CD-ROM and the appropriate readout technology

meant. Also from a technical point of view, data protection makes a

ments on outdated technologies are not necessary if using contemporary ones

Transmission paths and communication media are already comparable

protection for the personal data of the persons concerned

can be.

15.5

Postal delivery of COVID vaccination certificates

I've received a few complaints about the digital ones sent by post

vaccination certificates. These vaccination certificates were issued together with a

sian Ministry of the Interior and Sport (HMdIS) and the Hessian

Cover letter signed by the Ministry for Social Affairs and Inclusion (HMSI).

shipped. For clarification and to promote transparency, I have

log reached an adjustment of the process with the ministries involved.

After a vaccination in Hessian vaccination centers, the citizens received

and citizens put together their personal digital vaccination certificate (QR code).

with a cover letter signed by HMdIS and HMSI. Through this

some people got the impression that the vaccination dates of the

would be stored in the ministries.

According to the opinion of the HMdIS, the vaccination data of the citizens

and citizens not processed by the ministries, but for the creation

and to send the digital vaccination certificates from the vaccination centers to the

municipal service provider ekom21. The cover letter from HM

dIS and HMSI was added to the respective vaccination certificate before dispatch by the

ekom21 only attached, since the creation and dispatch of the digital

Vaccination certificates were organized centrally for all Hessian vaccination centers.

In the joint cover letter from HMdIS and HMSI on the vaccination certificates

fictitious, these are recognizable as the sender. Unfortunately, the cover letter contained

no appropriate clarification that the creation and dispatch of the

Vaccination certificates on behalf of the responsible health authorities as carriers of the

vaccination centers was carried out by ekom21 as a service provider and the

ben of the ministries was only settled. Hence the concerns of

Citizens in principle with regard to their sensitive vaccination data

understandable.

Especially when dealing with those affected who are extremely vulnerable

Health data requires special sensitivity. Also in interest

of citizens' confidence in the vaccination campaign

such misunderstandings through a transparent presentation of data processing

be prevented in advance.

If the integration of an external service provider for the creation and the

Sending the vaccination certificates is not required, this should be considered critically

become. With the transmission of sensitive health data to others

Jobs may potentially involve new risks.

230

health sector

At my suggestion, the processes were revised to allow for more

to ensure transparency towards the citizens and

to prevent understanding. After adapting the procedure, the

digital vaccination certificates directly from the responsible health authorities

Carriers of vaccination centers sent and signed on their behalf. On the

Integration of ekom21 was omitted.

15.6

Electronic provision of information in the health sector

Electronic information must also be provided in the healthcare sector in accordance with Art. 15

Para. 1 and 3 DS-GVO may be possible if the person concerned so wishes.

There are a number of ways doctors can do this.

Right to electronic information?

I'm getting more and more input and inquiries about that

Medical practices only provide information in accordance with Art. 15 DS-GVO in writing, whether

probably the persons concerned submitted the request by e-mail and order the

I have asked for the provision of information "in a common electronic format"

ben. The provision of information is then often made with reference to data protection

rejected. The patients are offered the documents

either pick it up or receive it by mail.

According to Art. 15 Para. 3 S. 3 DS-GVO, the information is in a common format

to make available in electronic format if the data subject

submits the application electronically and unless otherwise indicated. Also the

information about a possible delay in the provision of information

according to Art. 12 Para. 3 S. 4 DS-GVO if possible if this is available

Conditions to be done electronically. These requirements and

the possibilities of secure electronic transmission to the patient

Doctors' practices are often unaware of the fact that women and patients are aware of it.

Requirements for electronic information

When providing information electronically, it should first be noted that the

The identity of the data subject must be established without any doubt. Is not this

the case, the person responsible according to Art. 12 Para. 6 GDPR additional

Request information needed to confirm the identity of those concerned

person are required. In the cases known to me, the identity of

applicants, because in addition to the electronic

electronic application, among other things, in person at the doctor's office

to request electronic information, or by post

have communicated to the medical practices.

Particularly problematic in the provision of information in medical

The area is that according to Art. 9 Para. 1 DS-GVO particularly worthy of protection

Health data and data subject to secrecy under Section 203 of the Criminal Code

subject, must be transmitted. According to Art. 5

Para. 1 letter f DS-GVO in connection with Art. 32 DS-GVO with regard to

required levels of protection adequate and appropriate technical and

to take organizational measures to ensure the security of the transmission

to ensure. This is also the reason why the electronic

The provision of information from medical practices is often categorically rejected.

This is understandable insofar as when sending e-mails with

Health data a transport encryption alone, d. H. the frequent of

Encryption automatically performed by the e-mail providers for the

Transmission path between the servers of the sender and the recipient

gers, is fundamentally not sufficient. Rather, what is needed here – is a

to ensure an appropriate level of protection - taking into account the

State of the art in addition to transport encryption also one

Content encryption (“end-to-end encryption”).

How content encryption of e-mails can be achieved

I presented in detail in my last activity report (see 50.

performance report, chap. 17.2., p. 184 ff.). Also the Conference of Independents

Data protection supervisory authorities of the federal and state governments have in their

Guidance on “Measures to protect personal data at

of transmission by e-mail" (https://www.datenschutzkonferenz-online.

de/media/oh/20210616_orientation_help_e_mail_encryption.pdf)

comprehensively with the requirements for such transmission by e-mail

occupied.

For inquiries about the electronic provision of information by medical practices

I refer primarily to the possibility of transmission as a password

protected ZIP or PDF file attached to an email. This is from mine

View the simplest way to secure electronic transmission

of health data. It should be noted that the

Password protection must be combined with effective encryption.

The effectiveness of an encryption is always subject to one

limited in time by technological advances and accordingly

improving attacks on encrypted files. is currently

gigantic encryption method such as the Advanced Encryption Standard

(AES) with a sufficient key length (256 bits or longer) as an effective

to look at sam. Those responsible can choose appropriate

health sector

procedure e.g. B. the technical guideline "Cryptographic methods:

Recommendations and key lengths” (BSI TR-02102-1) of the Federal Office for

Security in information technology (https://www.bsi.bund.de/SharedDocs/

Downloads/DE/BSI/Publications/Technical Guidelines/TR02102/BSI-

TR-02102.pdf).

In any case, the medical practice must ensure that the patient

patient is able to open the message. For this purpose, before the transmission

always consulted with the recipient

become. Exchanging a password for decryption can also

in the context of a telephone consultation. Under no circumstances should for

the transmission of a password uses the same communication medium as

can be selected for the transmission of the encrypted data. By a

Prompt consultation can also prevent any misunderstandings

be bent. So have z. B. some affected persons in the me

present cases with the designation "electronic information" on the

Transmission of digitized documents on a data medium (e.g. CD

or USB stick). Of course, a doctor's office can also

comply with their obligation to provide information in this way, including in this case

think about encrypting the transmitted data.

Furthermore, the unencrypted transmission of health

health data based on the patient's consent (https://

www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Be-

schluss_waive_on_TOMs.pdf). This legal opinion often comes across

Lack of understanding among the people concerned, who usually at a fast

and uncomplicated provision of information. The responsible

However, medical practices risk violating the requirements of Art. 5

Paragraph 1 letter f and 32 GDPR.

15.7

Correction in the patient record

The patient only has a right to correction according to Art. 16

GDPR if the patient records contain objectively incorrect or

there are incomplete data. The right to correction is directed

only on statements of fact that are amenable to empirical evidence.

I regularly receive requests for corrections

Art. 16 GDPR in patient files. In this case, the inputter has priority

all about the fact that the doctor, in their opinion, is wrong

made a diagnosis.

In principle, patients have the right to be asked by the doctor

or the doctor the correction of the incorrect personal

related data according to Art. 16 DS-GVO. This right is i.a.

the expression of the principle of correctness from Art. 5 Para. 1 Letter d

GDPR.

However, here must be between statements of fact, which are empirical

Evidence are accessible, and expressions of opinion and value judgments about

people are distinguished. The latter are personal data

within the meaning of Art. 4 No. 1 DS-GVO, which can usually be corrected

are not required (cf. Dix in: Simitis/Hornung/Spiecker gen. Döhmann,

Data protection law, GDPR Art. 16 para. 14.) The doctors are

also in the field of diagnosis a wide scope for assessment and evaluation

to. Medical diagnoses or other assessments are

therefore about valuations (see BGH NJW 1989, 774f.). These are one rating

not accessible as correct or incorrect. Medical diagnoses or otherwise

Assessments are therefore not covered by the right of correction.

The submitters are therefore regularly informed by me that

that the data subject only has a right to rectification

Art. 16 DS-GVO if the patient documents are objectively in-

correct or incomplete data. The Right to Rectification

is only based on statements of fact such as e.g. B. height or date of birth

as well as other information such as the address or contact details (see

Schröder in: Dochow/Dörfer/halbe/Hübner/Ippach/Schröder/Schütz/Strueve,

Data protection in medical practice, 2019, p. 158 f.). The incorrectness of

data must be ascertainable without any doubt.

The correction must be made immediately and free of charge if

is entitled. For reasons of medical liability and medical documentation

On duty, the correction of data must always be logged accordingly

become. So it must be traceable who made the correction

and what exactly was changed and what the original date was

(See Munich Lawyer's Handbook for Medical Law, MedR, § 23 Data Protection in the

Healthcare, para. 119, beck-online).

A diagnostic error, on the other hand, is civil law in the context of a medical

processing to assert.

An alternative solution to this is the recording of a counter-notification

(e.g. in the form of an expert opinion) in the patient file. This can be from one

be accompanied by a blocking notice. With this approach I have so far

had good experiences. However, this requires the consent of

both parties.

234

Science and Research

16. Science and research

Science and Research

Research is securing the future. It is not only a fundamental right of research

but also an activity in the public interest. research work

but must also respect other people's fundamental rights and other interests

of the common good into account. As far as they with personal

Data takes place, it must observe the requirements of data protection. The

Conversely, data protection must not hinder research in such a way that

it is no longer possible or only possible with considerable difficulty. Like this balance

can be achieved was the thematic focus of the conference

independent data protection supervisory authorities (DSK) in 2022. At the

I was intensively involved in the search for a solution (Section 16.1). At the same time I

year scientific institutions and associations in data protection issues

intensively discussed (chapter 16.2) and existing cooperation with associations in the

Health sector deepened and new ones established (see Chapter 16.3). A big

nationwide initiative for C0VID research was the subject of one of mine

co-supervised evaluation procedure (chapter 16.4).

16.1

Supporting research through data protection

Research and data protection are often seen as conflicting interests

seen. Both, however, the freedom of research and the freedom of information

Self-determination are fundamental rights. You need an assignment that

restricts the other fundamental right as little as possible. If this succeeds

Assignment, they can complement and promote each other. Research

is dependent on trust when data subjects ask researchers

to entrust their data. An essential basis for trust is

a convincing data protection.

Balancing fundamental rights and the common good

According to Art. 13 GRCh, "art and research are ... free". Likewise, according to Art. 5

Paragraph 3 sentence 1 GG "Art and science, research and teaching ... free". As

Research is any “intellectual activity with the goal, in a methodical, systematic

to gain new insights in a more systematic and verifiable way” (BVerfGE

35, 79, 112f.). Scientific research requires independence and

Independence. However, freedom of research is not unlimited. She

finds its limits in the rights of others and in matters of public interest,

as far as the legislature has specified them.

Such a right of others is the fundamental right to data protection according to Art. 7 and

8 GRCh, which gives the individual the power to make decisions about his personal

related data guaranteed. The same power protects fundamental rights

to informational self-determination in accordance with Article 2 Paragraph 1 in connection with

Art. 1 para. 1 GG. This fundamental right is also subject to restrictions that

established by law in the overriding public interest

are. Therefore, data protection must be the “key function that a free

Science both for the self-realization of the individual as well

for the development of society as a whole” (BVerfGE 35, 79,

113), take into account.

If both fundamental rights come into conflict, according to the principle of

practical concordance to be interpreted as being different from the other fundamental right

as much as possible can be realized (see Roßnagel, data protection

in research, ZD 2019, 157 ff.). On the one hand, this compensation must

grant protection to the persons concerned and, on the other hand,

and development opportunities through scientific research

unduly hinder. The DS-GVO attempt such a compensation concept

and the new German data protection law. You grant research in order to

to allow them multiple "privileges" over other purposes of

Data processing and at the same time put it on, in the implementation of the

Data processing gives the data subjects special "guarantees" for their

guarantee fundamental rights and freedoms.

For research, the GDPR contains many exceptions and preferential

gene – e.g. B. in Art. 5 Para. 1 Letter b an exception to the earmarking

for further processing for research purposes, in Art. 5 Para. 1 Letter e

an exception to the storage limit, in recital 33 a

Exception to the principle of certainty for consent, in Art. 9 Para. 2

Letter j an exception to the prohibition on the processing of special categories

personal data, in Art. 14 para. 5 letter b a restriction

of the information obligation and in Art. 17 Para. 3 Letter d a restriction

the obligation to delete. According to Art. 89 Para. 2, Member States may

provide for restrictions on the rights of the data subject.

To compensate for these "privileges", Art. 89 Para. 1 DS-GVO requires "suitable

te guarantees of the rights and freedoms of the data subject". This

Guarantees should be backed up by technical and organizational measures such as

Anonymization or pseudonymization ensure that in particular

respect for the principle of data minimization is guaranteed.

However, if research with anonymous data is not possible, e.g. B. at

patient-related research, according to the applicable rules, too

possible with personal data.

236

Science and Research

Research data as a key topic of the DSK

Against this background, the DSK sees it as an important challenge

Finding ways and solutions to reduce the processing of research data

scientific research purposes that are in the public interest,

enable and make its advantages usable. At the same time is the

associated risks to be consistently counteracted in order to those concerned

to ensure adequate protection of fundamental rights.

The DSK has therefore addressed the topic of "data protection for research data"

chosen as the focus of their work in 2022. To work on

to promote this topic and to act as a single point of contact for

to function in nationwide research initiatives, it has set up a “Taskforce

Research data" set up and the management of the BfDI and I

gen. This task force met six times during the reporting period and

Met multiple working group meetings, several research related

Conducted evaluation projects (see also Chapter 16.3), was contact person

for many research initiatives and associations (see also Chapter 16.2) and has

prepared two DSK resolutions (see below).

In their unanimous resolution of March 23, 2022 “Scientific

che research – of course with data protection” (https://datenschutz.

hessen.de/sites/datenschutz.hessen.de/files/2022-08/dsk103_entschlies-

sung_zur_scientific_research_0.pdf), the DSK underlined that

scientific research and data protection are compatible. She

welcomed the federal government's considerations for a research data law

and a Health Data Utilization Act and called for a high legal

clarity for everyone involved. It supports research into methods

To process research data in such a way that personal rights are protected as best as possible

to be protected. Finally, she demanded the legal protection of a

research secret.

Organized under the title "Strengthening research through data protection".

the President of the Hessian State Parliament Astrid Wallmann and I on 6.

October 2022 the “25. Wiesbaden Data Protection Forum” in Hessian

State Parliament (see Chapter 18 for more details). It pursued the question as research

and data protection the common goal of a humane

steps we can achieve through responsible data use. prof

Ulrich Kelber, BfDI, went into his lecture “Scientific Research

- of course with data protection" after the question of which legal policy framework is necessary to achieve the goal of responsible data to achieve ten use. Prof. Dr. Franziska Boehm from the Karlsruhe Institute for Technology (KIT) examined in her lecture “The special protection of research in the General Data Protection Regulation”, which special

Consideration of research interests provided by the GDPR and how these special rules can be applied in practice. prof dr dr Eric Hilgendorf from the University of Würzburg expanded Lecture “Data protection in the future regulation of European Research data spaces” the discussion about the European perspective and prof dr Hannes Federrath, University of Hamburg, from 2018 to 2021 President of the Society for Computer Science, considered in his lecture "Data protection-preserving methods of research data processing".

Questions of the conference from a technical point of view.

On November 3, 2022, the BfDI in the Kaiserin-Friedrich-Foundation in Berlin the symposium "Research with health data - challenges ments in the context of the General Data Protection Regulation”. Lectures out the Federal Ministry of Health, from the group of data protection officers, medical (joint) research, medical informatics and Jurisprudence pinpointed the problem areas, those in a practical Balance between medical research and data protection observed Need to become. There was agreement insofar as the task is to the normative framework, the structures of decision-making and

develop cooperation practices.

The DSK held on November 21, 2022 in the old plenary hall of the Federal Council
a symposium "Health research meets data protection" in Bonn,
the highlight of which was one by Frederik Richter from the Data Protection Foundation
moderated debate between Prof. Dr. Sylvia Thun, Digital and
Interoperability at the Berlin Institute of Health in the Charité Berlin, and me
was. This was mainly about the need for processing
personal data for medical research and the possibility
measures to protect the data sovereignty of the patients concerned
Design of the data processing processes. There was consensus that
the legislature for more uniformity and legal certainty with regard to
of the relevant legal regulations. Differences remained regarding
the necessary information technology protective measures in the medical
zinical research and the importance of the principle of earmarking and
the principle of minimizing personal references.

Petersberg declaration

At its 104th conference on the Petersberg near Bonn, the DSK decided
on November 23, 2022 their "Petersberg declaration on data protection
compliant processing of health data in the scientific
Research" (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/
files/2022-11/06_entschluss_-_petersberger_erklaerung.pdf). She gives

with her recommendations to the legislators in Germany and the Union for
the regulation of research with health data. Essential Aspects
are the following:

In the Union and in Germany there is a need to regulate the

to specify the use of research data in more detail and to coherently

design. The aim should be a transnational, uniform regulation

for the processing of health data for scientific research

purposes, the research alliances with partners in different

federal states to comply with data protection requirements

relieved.

The legislature should include research in the public interest

Enabling health data, but also setting its limits and the

protect the interests of the data subjects. He may ask these complex questions

are not entirely related to the persons concerned and the researchers

relocate With such a scheme, he can use data from

other sources, such as treatment data from hospitals,

from medical registers or from other research projects

(so-called secondary use) enable data protection-compliant research

or facilitate if obtaining express consent is not

would be feasible or would seriously impair the research project

would. In doing so, however, he should also determine which research is to be carried out in terms of content

is in the public interest and what other requirements are placed on it

Procedure and implementation must conform to the research.

With regard to the protection of data subjects, the principle applies: the higher

the protection provided by suitable guarantees and measures, the more extensive

the data can be used richer and more specifically. As far as that

Research purpose can be achieved with anonymized data

only anonymous data is processed. There are high requirements

changes to the anonymization of personal data. As far as that

Research purpose prevents complete anonymization are effective
to provide pseudonymization measures. This should be by law
independent and responsible trustees are transferred.
In addition, technical and organizational protective measures
according to the increased requirements for health data
meet the state of the art such. B. the encryption of the data.
Anonymization, pseudonymization and encryption should be dated
legislators to be specified.
If the legislature does not want processing for research purposes
a consent, but on a legal basis, he should
the involvement of the persons concerned through regulations for an

sufficient transparency and to an unconditional
foresee possibility.
Unless a legal basis should be created to record
from various sources, e.g. B. from medical registers, to link
special safety and protective measures must be taken. This
can e.g. B. include special record linkage method that only one
event-related and temporary mergers should be permitted. The
data subjects should have a consent management system
Have an opportunity to be active in knowledge of the risks of merging
agree. Alternatively, technical methods or measures
ensure that the re-identification of the data subject despite the
concatenation is excluded. In addition, the data should - as far as this

is possible due to the research purpose - evaluated at the place of storage

be so that the location of safe storage only anonymous results

leave the data analysis. Multiple storage is allowed

avoid.

By regulating a research secret, the unauthorized disclosure

of personal medical research data is a punishable offence

provided, their confiscation prohibited and a right to refuse to give evidence

be created for scientific researchers and their professional assistants.

16.2

Data protection advice in science and research

In addition to processing submissions, advising on research

research projects make up a large part of my work. from research-

from the students to the university or larger companies

In the health sector, all areas and positions are represented.

need for advice

Especially in the planning and initial phase of research projects

often important to set the right impulses with regard to data protection,

to steer the project in the right direction. As I could observe-

te, there is a lack of contact points for young and experienced researchers in

Hesse. In the past I have therefore been very happy to fill this gap.

With a large number of projects, it is noticeable that some aspects often differ.

are neglected, which are important from the point of view of data protection. these are

the following points in bullet points:

– Detailed considerations and justifications regarding the

structuring of responsibilities, especially when there are several positions

Science and Research

are involved (separate or joint responsibility or responsibility

contract processing).

– Clear determination of the legal bases for the processing of personal

related data.

– Sufficient transparency towards the persons concerned, in particular

special information about data processing according to Art. 13 or

14 GDPR.

– Timely involvement of the internal data protection officer

and, if applicable, the supervisory authority.

– Meaningful data protection concept, as is also the case with many funding

require donors.

– Consideration of the special data protection requirements,

linked to the processing of health data (as special categories

according to Art. 9 DS-GVO) or to automated decision-making

– Keyword algorithm-based decision support systems

(KI) - to be asked. For example, the need for a

data protection impact assessment.

– A risk-based and sensitive to the protection of personal data

oriented technology design, which is already

starts and the principles of data processing - such as B. Confidentiality,

Data minimization, earmarking - implemented and appropriate

and provides for appropriate technical and organizational measures.

If the points mentioned are considered, this is based on experience

at the same time a motor for the implementation speed.

Practical examples

Among the successful projects under the mentioned consulting practice
have emerged, the TeleCOVID Hessen project belongs. Through this
were in a very short time cross-hospital consultations and
professional exchange on COVID diseases during the peak phase
made possible by the corona pandemic. This was also possible due to the
exemplary and timely involvement of my authority by the Hes-
Ministry for Social Affairs and Integration (HMSI): A cooperation
beit how I want them to continue. The project has now been expanded
and is no longer just about COVID diseases (see
see 50th activity report, chap. 17.5; https://soziales.hessen.de/presse/
telecovid-app-hessen-networked-hospitals-0).
In addition, there are currently a number of interesting projects
the emergency services area in which I am involved. Here would be something like this

SAN project to name, with which the emergency rooms of the hospitals
should be relieved by local, nearby medical practices. Currently at
In times of the pandemic, this is again a project of particular importance.
I am also involved in the so-called ETA/ETN project, in which
service-specific messenger services are to be used.
Even if some of these projects have not yet been completed,
the integration of the data protection supervisory authority was thought of here in good time,
so that the course for the projects could be set early on.
Perhaps the wish is still appropriate here that the E-Health Advisory Board
of the HMSI resumes its activities and at a higher frequency

and regularity meets. Currently there are enough projects that are also there
could be discussed and in relation to which it is helpful to
Decision-makers from the healthcare sector in Hesse in one place
brings together. Eventually, this gap can also through this year
newly founded IGH AG Gesundheitsdaten will be closed. This brings
Companies from the health sector and representatives of the ministries
together to Hessen as data protection friendly and digitization
facing location to strengthen the back.
Finally, the reference to a transnational project, des-
whose project coordinators are based in Hesse. In the project goes
It is about researching the effects of the COVID disease on the
Lung. Here I have research data from the DSK as part of the task force
a coordinating function and will go through to a unified vote
all supervisory authorities are working towards this (see Chapter 16.4 for more details).

16.3

Cooperation on data protection in the health sector

In the past, it was an important concern for me to
rich health, science and research in an exchange with
the agencies and associations active in these areas. The
current planned legislative projects at national and European level
levels make this dialogue more important than ever. In my role as
seated of the AK Science and Research of the DSK as well as within the framework
I am conducting this dialogue as the co-chair of the Research Data Task Force
both at the national and international level.

Dialogue with professional associations within the framework of the AK Wissenschaft und Research

Clinical research plays an important role in the research context.

I am particularly pleased that in 2018 I had a permanent

Exchange of the AK Science and Research of the DSK with the association

of the research-based drug manufacturer (v.f.a. e. V.) could bring into being. The

Clinical Research Privacy Consultation Group met

this year for the ninth time. Topics in the past

Nine sessions were on the agenda, ranging from questions about the

Anonymization up to constellations that indicate the responsibility of the

bodies involved in clinical trials. Also the draft one

Regulation of the European Commission on a European Health Data

Space (EHDS) was of strong interest to the researching companies

and was therefore a focus of this year.

As far as this concerns clinical research, the Federal

Association of the Pharmaceutical Industry (bpi e. V.) to mention, which

also repeatedly in an exchange with the AK Wissenschaft und

research is located.

Dialogue with professional associations as part of the task force

research data

One of the main tasks of the Research Data Task Force is to

ninformatik-Initiative (MII) and the associated exchange with the Tech-

nology and method platform for networked medical research

e. V. (TMF) to accompany intensively.

It was a focus in the past reporting period and will be in the future

forthcoming reporting period, the dialogue on the sample texts of the MII

to consent to medical research and the module

coordinate transfers to third countries. A workshop is already being planned for this

which is intended to serve the interests of data protection and researchers

to bring about an interest-based balance.

In addition, the Research Data Task Force is also available on request

ge other committees and professional associations for an exchange on the topic

research data available. For example, in 2022 a

Meeting with the AG Bio-IT, Big Data and E-Health of BIO AG Germany

e. V. instead. It turned out that the topic of secondary use of

data is of particular interest and further consideration of the task

force with this topic from the representatives of BIO AG Germany

e. V is endorsed.

Dialogue with professional associations at state level

In the past there have always been critical voices about the role

of data protection in the context of health care and research

in the medical field. Here it was of particular importance to me that

In 2022 there will be an exchange with the German Society for the Interior for the first time

Medicine (DGIM e. V.) took place, the largest medical-scientific

Specialist society in Europe (see also https://datenschutz.hessen.de/presse/

to-a-better-understanding-between-medicine-and-data-protection).

At the two meetings that took place, it was an important concern

To arouse understanding for the concerns of data protection and at the same time

the requirements and needs in the fields of medicine and research

to discuss. Demands from the DGIM and the DSK

jointly compared in their Petersberg Declaration (see Chapter 16.1). It

there is the expectation that this fruitful dialogue will continue in the next reporting

year is continued.

Participation is equally important at the state level

at the IGH AG health data. This consists of research

health company from Hesse, representatives of the Hessian ministry

for Social Affairs and Integration and the Hessian Ministry for Digital

strategy and development together. Here it is the aspiration, Hessen

as a location for healthcare companies in compliance with data protection

of legal principles and to make them even more attractive.

The roadmap for the use of health data serves as a model here

from Baden-Württemberg (see https://www.forum-gesundheitsstandort-bw.de/

download_file/force/21093/84221). A paper based on this model is in the works

and is expected to be finalized in the coming year.

outlook

It will be important for the future to also increase the dialogue at European level

intensify and exert influence on the committees already in place there

to take the coming developments. For the areas of health

as well as science and research is particularly the "Compliance, eGovernment

ment and Health Expert Subgroup" of the EDSA. Here I am

already examining rules of conduct according to Art. 40 DS-GVO (Code

of Conduct – CoC) and will also draw up the guidelines for

support scientific research.

16.4

Research initiative RACOON

As co-chair of the DSK research data task force, I have the

Advice for the RACOON research initiative coordinated. At

such a transnational research project of different universities

sity clinics, those responsible must provide their respective country-specific

observe data protection regulations. With this challenging

legal starting point I have a constructive advice

the Research Data Task Force.

background

Through the cross-state research initiative RACOON

in which all radiological university clinics in Germany are involved

a novel research infrastructure for structured recording and

evaluation of radiological data from COVID-19 cases.

The radiological data should initially be stored locally in the respective university

versitätsklinikum can be structured and analyzed. In a second step

should the data after removal of personally identifiable information

also to the other participating university clinics via a central authority

made available for specific research projects.

Due to the federal structure of the data protection regulations,

regulations and the responsibility of the respective data protection supervisory authorities

close involvement and coordination between supervisors

necessary. The research data task force founded in autumn 2021

DSK enabled effective and fast cooperation.

Data protection challenges

The responsible university hospitals are part of a joint

responsibility of the participating university hospitals and have assumed

a corresponding contract is drawn up for this purpose. The Charité in Berlin and

the University Clinic in Frankfurt have the project coordination of the research

research initiative taken.

The data protection legal basis for the processing of personal

related data had to be clearly identified. § 287a sentence 1 of the fifth

Social Code Book (SGB V) contains a regulation on the legal basis

in cross-state projects of supply and health research

research, where bodies from two or more countries as responsible

involved. Accordingly, § 27 BDSG is applicable to such projects. Through

the naming of the university clinic in Frankfurt as the main person responsible

the formal requirements of this regulation could be fulfilled.

Due to concerns about federal jurisdiction and systemic

However, there were doubts as to its applicability due to the matic position in SGB V

of § 287a SGB V on the RACOON project. Therefore, the long

of legal regulations, in particular the state hospital laws,

used as a legal basis. The significantly different ones

Regulations in the state laws also had different evaluation

ments by the state supervisory authorities.

Also the data protection requirements for anonymization

of radiological image data provided for those responsible for the project

challenge.

The project managers have given the research data task force extensive

provided rich data protection legal documents and that

Project presented at a special session of the Research Data Taskforce.

Advice from the task force members was taken into account and

Improvements have been made.

At the end of the reporting period, the supervisory authorities involved

mostly agree on a positive assessment of the project

Conclusion

The approach of the Research Data Task Force can serve as a model for

serve to support future transnational research projects.

It has been shown that in Hesse for research in hospital

area through the reference in Section 12 (3) HKHG to Section 24 HDSIG

legal situation exists. In other countries, on the other hand, it was possible

the consultation on the RACOON project, a need for change with regard to the

country-specific regulations are determined.

The observance of different national legal bases

the researchers face challenges. In the interests of research,

the data protection regulations for transnational research

further harmonized in compliance with constitutional requirements

become.

17. Technology and organization

technology and organization

The implementation of data protection law is often hampered by inadequate

Technology and insufficient organization caused. Therefore it is for the truth

It is important to me that I run an IT laboratory that

can carry out the necessary technical investigations (chapter 17.1).

Data protection violations must be reported to me as the supervisory authority (section 17.2).

This is of particular importance when processors are attacked

because many responsible persons are affected (Section 17.3). The

Errors in technology and organization can also be the subject of a

systematic testing (Section 17.4). Relevant for data protection

Vulnerabilities occur in particular with self-developed software

(Chap. 17.5). After data protection violations, the persons concerned can

be notified of a case of misuse of e-mail accounts

ten (Section 17.6). The adverse consequences of attacks on

IT systems can be greatly diminished if those in charge

or processors have a working backup and

recover lost data (chap. 17.7)

17.1

Technical data protection tests in the IT laboratory

Not least because of the ongoing digitization in all areas of life

my authority deals with a wide variety of technical areas

facts. If a purely document-based review is not sufficient

accordingly, the employees of my technical department carry out technical

Data protection checks in the IT laboratory set up specifically for this purpose

through my authority. These technical data protection checks must

sen meet various requirements in order to be carried out in accordance with the law

to be able to.

Submissions on technical issues

In the reporting period, I received regular submissions relating to technical

directed niche issues or had such as a background. examples

were for this

– Complaints in accordance with Art. 77 GDPR about websites in which the

External resources were impermissibly involved, e.g. B.

Fonts downloaded from servers of a company based in the

USA were reloaded,

– Submissions on suspected violations of protection of personal

ner data according to Art. 4 No. 12 DS-GVO, for example in connection with

247

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

potential vulnerabilities in web applications or mobile applications

plications and related unintentional disclosure

personal data, as well

– Personal data breach notifications

according to Art. 33 DS-GVO due to hacker attacks and the publication

disclosure of personal data by the attackers.

These exemplary facts alone provide a first impression of the

wide range of technical issues that employees deal with

the one dealt with and deal with from the technical department of my agency.

The level of detail and technical soundness of the in the reporting period to me

directed inputs varied greatly. They ranged from succinct and general

held descriptions up to a detailed description of the

Facts including the step-by-step procedure for understanding.

Technical privacy review

In the case of submissions on technical issues, there was often a need for

a review of the submitted information and an evaluation and

assessment of the results of this review. These formed the basis

for any further action on my part, such as the seizure of

Measures according to Art. 58 Para. 2 DS-GVO.

According to Art. 58 Para. 1 Letter b DS-GVO, my authority is authorized to

conduct searches in the form of privacy reviews. This

The legislature deliberately formulated the power in general terms and includes it

in particular the implementation of technical data protection checks

with a. This is the review of technical expertise

hold using suitable technical testing tools. Such technical

Data protection reviews do not necessarily have to be on the premises

by persons responsible according to Art. 4 No. 7 DS-GVO or processors

be carried out in accordance with Art. 4 No. 8 DS-GVO. The Power of Investigation

my authority according to Art. 58 Para. 1 Letter b DS-GVO offers me rather

the possibility, in my office or out of this technical

carry out data protection checks (see Bruhn/Roßnagel/Wach-

house/room, data protection checks in the IT laboratory of supervisory authorities,

DuD 2022, 685 ff.). I particularly benefited from this in the reporting period

made use of when technical facts to be checked in connection

connection with IT systems accessible via the public Internet or

-Services stood. Technical data protection checks had to be carried out here

always in accordance with the general principles of official action in

rule of law. During implementation, the corresponding

the requirements are met. Due to the given in the DS-GVO

248

technology and organization

Legal basis, my employees act within the framework of their official duties

Always act in an authorized manner, which is why possible criminal offenses,

such as spying out data in accordance with Section 202a of the Criminal Code (StGB),

are not relevant for this.

As a prerequisite for the implementation of technical data protection

The employees of the technical department have to carry out tests

Authority equipped with adequate and appropriate testing tools

be. They must also have the appropriate infrastructure in order to

to be able to use the respective testing tools effectively and efficiently. Around

to meet these requirements, was in my authority before the

An IT laboratory set up during the reporting period and in the reporting period

further expanded.

Weighing of interests within the framework of technical

Privacy Reviews

As part of the implementation of a technical data protection review

is used in the vast majority of cases with IT systems and services

interacted by controllers and processors. thereby become

generally affects their legally protected interests. type, scope and

The extent of this intervention depends on the underlying facts,

from the test tools used and from the specific process of the technical

technical data protection check. All these factors are therefore in the frame

exercising my professional judgment in designing and

carrying out a technical data protection review appropriately

take into account. In doing so, I have to take conflicting interests into

agree to weigh these interests against my test and protection mandate and

ensure the justifiability and proportionality of the use of funds.

In principle, those test steps of a technical data protection

review be reasonable and proportionate, the form and intensity of which

sity of interactions with IT systems and services of controllers

or processors are expected for them. Such test steps

were and are in the IT laboratory of my agency for reasons of

Proportionality usually without involving those responsible

or processors, for example as part of preliminary investigations.

However, situations can arise in which the justifiability of individual

test steps of a technical data protection review appears questionable.

This can be, for example, in a rudimentary or unclear information

on the situation with regard to the IT systems and services to be checked

be. Also, the nature of a planned test step could in certain cases

lead to damage to tested IT systems and services. In such

cases, the respective responsible persons and processors will be informed

informed of the planned steps. Here are usually further, for

information required for the test is requested, and responsibility is

chen and processors the opportunity to comment and to

Submissions of reservations granted. The replies will be

connection in such a way that, if necessary, an adjustment of individual

ner test steps. Also, it may be necessary to test steps

carried out jointly with responsible persons and processors or

be discarded.

Technical data protection review in the administrative procedure

Technical data protection reviews are often carried out in advance of a

administrative procedure or as part thereof. In the first

In this case, they serve to clarify facts in the context of preliminary investigations

ments to determine whether and with what aim an administrative procedure

is to be opened. In the second case, technical data protection

tests are often used to clarify technical issues and

secure evidence.

In both cases, there is a general obligation to provide prior information

those responsible or processors about the implementation of technical

shear data protection checks are just as little given as an obligation

for information later. Such a stakeholder public is in

the legal provisions on the taking of evidence in administrative proceedings, such as

such as Section 26 of the Administrative Procedures Act (VwVfG), not provided for. One

However, as described above, prior information is still at least

required if the implementation of a technical data protection

examination otherwise appears to be unreasonable.

Responsible persons must be informed about the opening of administrative proceedings

Libraries and processors also do not necessarily have to be informed. She

applies regardless of whether a technical data protection check is carried out

as part of the respective administrative procedure.

A technical data protection review is to be carried out by the

Use of their results in the context of an administrative procedure and

dependent. For example, test results can B. as a basis for the enactment

serve the purpose of an administrative act, such as an order pursuant to Art. 58 (2).

GDPR. In this case, the controller or processor

due to § 28 VwVfG to give the opportunity before the enactment of the

Administrative act to comment on the underlying facts.

For this purpose, he is also provided with the results of a technical data protection

250

technology and organization

to share. Hence the evidential suitability of the test results

and the associated documentation are of particular importance.

Selected test steps

A few selected, representative test steps are listed below

technical privacy reviews outlined in the reporting period to

a first, more concrete impression of the objects more technical

arranging privacy reviews.

As part of technical data protection reviews, re-

research on websites on the Internet, in social media channels or in

called "Darknet". This will be publicly accessible

information is determined and evaluated. These can, for example, relate to

Vulnerabilities in IT systems and services or on the disclosure

obtain personal data. Internet archives and similar services

can be used, if necessary, to determine in which

period of time a publication was expected. The spectrum of

Information procurement can thus relate to different questions

lungs. Sources of information must, however, in any case

analysed, evaluated and assessed in terms of their trustworthiness. At

Research is usually the least invasive type

of test steps. The implementation should therefore generally be justifiable.

Submissions to specific websites can be made for various reasons

me. Examples include complaints about

– the design of cookie banners,

– the unlawful publication of personal data,

– the unlawful use of personal data for shipping

from advertising,

– non-functioning unsubscribe procedures from newsletters or

– specific vulnerabilities in web applications.

To clarify the underlying technical facts,

the IT laboratory with the affected websites and web ads

Use within the framework of the user behavior to be expected from the operator

interacts. These include, depending on the specific subject of a complaint,

for example

– calling up the website to analyze a cookie banner in more detail or

to inspect a publication that is the subject of the complaint,

– the creation of a user account to prevent any unlawful

to confirm the sending of promotional e-mails,

– the registration and subsequent de-registration for a newsletter,

to check the functioning of the corresponding functionalities, or

– the manual replication of what is described in a complaint

Procedure to verify the existence of a vulnerability.

These test steps are usually justifiable since they are all based on the

functions intended and provided by the operator are carried out

become. However, particular care must be taken with the last test step

required. Here it is important to avoid any unexpected side effects and

to avoid the damaging effects.

Another group of test steps in the context of technical data

Protection reviews relate to mobile applications (apps). here

can roughly differentiate between static and dynamic analysis

become. In a static analysis, the building blocks of the to-be-tested

App analyzed, for example with regard to the integration of so-called trackers or the

Presence of security-critical information in the source code. For this is

it is not necessary to run the tested app. Therefore take this

test steps also play a special role, because interaction with IT systems

Men and services of controllers and processors does not find

instead of. Dynamic analysis is used when the behavior of a

App within the scope of use is the subject of one or more test steps

is. These test steps can be based on different questions

lie, for example with regard to the actual transmission of personal data

data to different actors. Such test steps should be justifiable

be. However, special care is required if apps are used in the IT laboratory

had to be manipulated to produce testability. It applies here

also to avoid undesirable side effects with harmful effects.

In the technical data protection review of websites and in the

dynamic analysis of apps is usually network traffic

recorded. On the one hand, this enables an in-depth analysis of the

exchanged data. On the other hand, the complete recording

drawing of the network traffic usually the probative value of the results

a technical data protection review. Often comes as part of the

Network communication uses encryption. This must

additionally broken in order to access the unencrypted data

to obtain. Both the recording of network traffic and that

Breaking the encryption are usually reasonable test steps.

This applies in particular if both test steps are carried out passively and neither

Manipulation of the exchanged data is carried out.

The analysis of IT systems accessible via the Internet with regard to

open network ports or supported encryption methods

252

technology and organization

be reasonable and proportionate. Finally, those responsible and

Processors can expect that such analyzes will be carried out on the Internet

be carried out regularly by different actors. you belong

thus also to the expected interaction patterns.

Conclusion

A basic task of my authority is according to Art. 57 Para. 1

Letter a DS-GVO the monitoring and enforcement of the provisions of

data protection law. For this purpose, my authority orders in accordance with Art. 58

Para. 1 letter b DS-GVO on the power of investigation, data protection

to carry out checks. This also includes technical ones in particular

Privacy Reviews. As a prerequisite for their implementation

adds my agency has a suitably equipped IT laboratory.

Technical data protection reviews must always be carried out in accordance with the general

n principles of official action in the rule of law

become. As part of the implementation, legally protected

te interests of controllers and processors. Therefore

must when designing and planning a technical data protection

review within the scope of due discretion different

Influencing factors are adequately taken into account, interests weighed up as well

the justifiability and proportionality of the use of funds is guaranteed

become.

Technical data protection reviews are often carried out as part of preliminary

communications or as part of administrative procedures. At latest

if test results as a basis for issuing administrative acts

are to be used, the responsible persons concerned and contract

processors are given the opportunity to comment. For this

they must also be granted access to the test results. Here are theirs

Suitability of evidence and its documentation are of particular importance.

17.2

Data Breach Notifications

The number of data breach notifications remained in the reporting

year at a high level. Due to the increase in cyber attacks

the role and duties of those responsible shifted to service providers

Positions active processors in the focus.

Overview and Developments

After a record high in 2021 with a total of 2,016 reports in

Regarding personal data breaches pursuant to

Art. 33 DS-GVO, § 65 BDSG in connection with § 500 StPO and § 60 HDSIG

was recorded, the number of reports submitted in 2022 went down

slightly (about 13%) back. With 1,754 reports, the number of reported remained

However, data protection incidents were also at a high level in the year under review.

The processing of data breach reports thus continued to pose a problem

a large part of the day-to-day work of my authority.

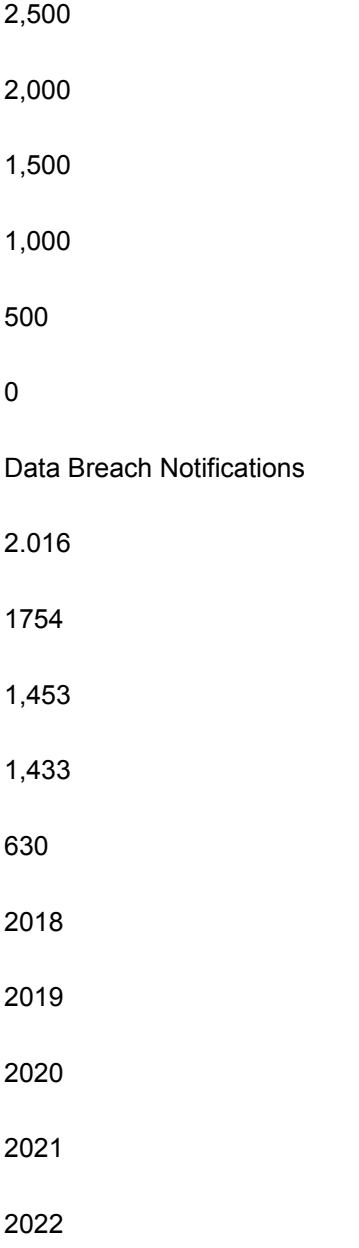

Figure: Development of the number of data breach notifications

at the HBDI since the GDPR came into effect

Overall, the range of reported data protection incidents was very diverse. The

ranking of the most reported injuries, as well as in the

recent years, repeated the incidents related to faulty

shipping and incorrect attribution of data as well as cybercrime. The

Most of the reports reached my authority from the business sector

including banking, debt collection, service providers, trade and commerce.

In addition, the areas of employee data protection and

health and care severely affected.

254

technology and organization

Reports related to the Corona Pandemic

Various injuries were reported in the year under review, particularly in the healthcare sector.

ments of the protection of personal data in connection with

of the corona pandemic. Most of these were

Incorrect transmission of positive test results by the test centers

as well as wrong dispatch of corresponding information with a determined

Corona infection by the health authorities. The causes lay in these

Cases mainly in individual errors of employees and goods

among other things, to the acutely increased incidence of infection and the associated

related workload.

In one case, a doctor's office in Wiesbaden informed me that

an employee allegedly numerous counterfeit Covid 19 vaccination certificates

had exhibited. The report was based on a tip from the police

back, which determined extensively in the case. For further abuse

to prevent, the responsible body reacted immediately with the

Release of employees and other measures, such as changes

of passwords and renewed awareness of all employees.

In another case, a hospital reported that as part of

Access control of patients and visitors instead of a scan and the

Check the presented corona vaccination certificates and identity documents

had been photographed using official smartphones. After knowledge

of the data protection breach, the collected data was deleted and that

Procedures for carrying out access controls changed immediately.

Reports related to the 2022 census

In addition, I received individual reports from

Data breaches that occurred in the context of the 2022 census.

For example, a Hessian city reported the loss of extensive

Census documents by a survey officer. Affected were the

resident of an apartment building. The responsible body reacted

with appropriate measures such as additional awareness raising

employees and the survey officer and the information

the persons concerned according to Art. 34 DS-GVO. On the part of my authority

recommended to the city as part of the comprehensive consultation that

carry out increased controls if necessary.

In another city, the figures raised as part of the census

misused personal data for private purposes.

After the survey had taken place, the survey officer contacted

During a conversation, a citizen who was obliged to provide information by phone and sent her

at the same time suggestive news. Separated on the occasion of the incident described

the city with immediate effect from this survey officer.

Overall, a positive balance can be drawn in this area. In the

in relation to the amounts of data collected in connection with the census

ment are collected and processed, only very few individual cases were reported

reported as data breaches. I therefore assume that

In this regard, the vast majority of those responsible and the

survey officer behaved in compliance with data protection (see also Chapter 9).

hacker attacks

In 2022, cybercrime was also a perennial favorite among data

protection violations. Of particular note is a new one with a

development that is associated with great danger, which was observed in the reporting period

could be tested. Service providers from different

Areas attacked by hackers. In the year under review, several

Hessian service providers are victims of intensive cyber attacks. Furthermore-

numerous responsible bodies based in Hesse were through

Hacker attacks on service providers from other federal states.

Overall, both companies and public institutions,

among other things, critical infrastructures and companies of the existential

precaution, affected by such attacks. Attacks on IT service providers

with a focus on human resources and/or pension

administration, significant amounts of employee data were affected.

With this dynamic development, the problem of cybercrime

new dimensions overall. successful cyber attacks

Service providers, which are usually significant on behalf of several responsible persons

Process amounts of data inevitably reach a large extent and

cause serious cross-divisional and cross-industry damage.

In particular, disruptions in the operation of critical services could

noticeably jeopardize the security of supply for the citizens.

In addition, attacks on service providers due to their complexity

all those involved face special challenges in coping with and

processing of the incidents. Among other things, it must be laboriously identified

which data is affected by which person responsible and to what extent

are. The development described is also reflected in the context of

cooperation of the German data protection supervisory authorities. So

had to answer questions of jurisdiction in several cases in the year under review

and the flow of information are clarified together. Over and beyond

the events required a constant exchange of information

and evaluating the cases. This was evident in all of them in the year under review

cases flawlessly, purposefully and constructively.

The role and responsibilities of processors

On the occasion of the described increase in cyber attacks on service providers

from various areas in the past year, it is a big one for me

Concern, again on the importance of data protection compliant design

the order processing and the successful cooperation between

inform the responsible bodies and the processors.

Processors are important actors involved in data

security incidents can play a crucial role. A successful

Implementation of obligations and effective protection against hacker attacks

only succeed if responsible bodies, processors, competent

Data protection supervisory and other affected authorities cooperatively

work together (see also Chapter 17.3).

If there is order processing in accordance with Art. 28 DS-GVO, you must also

additional regulations in the context of possible data protection violations

are taken into account. Among other things, the processor supports

according to Art. 28 Para. 3 Letter f DS-GVO the person responsible for the fulfilment

its reporting and notification obligations.

Art. 28 GDPR

(3) The processing by a processor takes place on the basis of a

contract or any other legal instrument under Union law or the law of the

Member States that control the processor in relation to the controller

binds and in the object and duration of the processing, type and purpose of the processing

tion, the type of personal data, the categories of data subjects and the

Obligations and rights of the person responsible are defined. This contract or this

other legal instrument provides in particular that the processor (...)

f) taking into account the type of processing and those available to him

Information to those responsible for compliance with the provisions of Articles 32 to 36

supports the above obligations; (...)

This provision is specified in Art. 33 Para. 2 GDPR. After that is

the processor is obliged to notify the person responsible immediately

notify you if you become aware of a data breach.

257

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

Art. 33 GDPR

(2) If the processor has a personal data breach

becomes known, he reports this to the person responsible immediately. (...)

This means in particular that the processor

About any personal data breach in mind

of Art. 4 No. 12 DS-GVO immediately - i.e. without culpable hesitation in

Within the meaning of § 121 BGB - must inform. Conducts its own risk analysis

he didn't go through with it. That means even if a data breach

does not pose a risk to the rights and freedoms of individuals

to bring these to the attention of the person responsible in any case. It ob-
then lies with the person responsible, with the support of the service provider
carry out a risk assessment and then decide whether
Reporting to the supervisory authority and notification of those affected
people are required. I recommend the processors, provided
it is unclear which data is affected by the breach, as a precaution all
To inform customers on whose behalf they are working. The respective
then make a verbal decision, taking into account all the circumstances
of the respective case about the further procedure.
In this context, I suggest that as part of the design
an agreement on order processing clear regulations for the
be taken in the event of a possible data protection incident. These should include
the entire reporting process together with the responsible contact persons and
Absentee representatives and the scope of the service provider
information to be communicated (e.g. detailed description of the
change, timing, number and categories of affected personal
related data and persons taken by the processor
Measures to mitigate the data breach and any others
Circumstances that could be of importance in individual cases) (see also Chapter 17.3).
The processor does not have his own reporting obligation under Art. 33 DS-
GMO to the supervisory authority. Regardless of this, however
the person responsible authorizes the processor, one for him
report to the data protection supervisory authority. In this case
the notification must include all required information according to the specifications
of Art. 33 GDPR. Irrespective of this, occasionally a
additional notification by the processor to the person responsible for him

Supervisory authority - for example for reasons of transparency or

Need for advice – make sense. Such a message is in any case then

displayed, albeit the service provider's own data, such as

technology and organization

Employee data, are affected, for which he considered data protection law

responsible and not as a processor.

Because the person responsible generally ensures the security of the data entrusted to him

must guarantee, he is obliged according to Art. 28 Para. 1 DS-GVO, in the event

an order processing with the necessary care a reliable service

easier to choose. This obligation does not end when the order is placed,

but extends to the entire duration of the contractual relationship. Also

in connection with data protection incidents at the processor

it for the person responsible to continuously check whether the service provider

meets the required requirements. It is in the aftermath of an incident

among other things, by the person responsible to check whether the technical

and organizational measures of the processor

standards and have been adjusted to the extent required. There-

In addition, the person responsible examines whether on the part of the service provider

sufficient action has been taken to prevent the recurrence of a

prevent or minimize incident.

For his part, the processor must at all times provide adequate guarantees in

with regard to suitable technical and organizational measures.

This applies all the more against the background that in the case of data protection violations

processors can be held liable in addition to those responsible

can. In addition, data protection supervisory

Measures according to Art. 58 DS-GVO to order processors. In the event of
of violations are far-reaching sanctions both against contract
process as well as to those responsible. In the reporting year
no measures were taken by my authority within the meaning of Art. 58 Para. 2
GDPR taken against processors.

Conclusion and recommendation

Despite the high number of reported data breaches
only in a few case constellations of mine in the reporting period
Make use of remedial powers within the meaning of Art. 58 Para. 2 DS-GVO.
In most cases, responsible bodies and order processing
workers in dealing with and managing data protection incidents
according to the data protection requirements. In the reporting year
I have individual companies because of a non or not on time
reported data protection violation according to Art. 58 Para. 2 Letter b DS-GVO
warned. A company was established pursuant to Art. 58 Para. 2 Letter e GDPR
to notify affected persons after a hacker attack
reliant. Against another company was pursuant to Art. 58 para. 2
Letter i DS-GVO a fine for failure to document the

Data protection violation according to Art. 33 Para. 5 DS-GVO imposed. About it
In addition, it was necessary to look towards a Hessian town after a
Data protection event with extensive sensitive data requires a formal
tive instruction with the aim of informing data subjects
to enact.

With a large number of reported data breaches, the

events are ultimately attributed to human error.

This applies to the classic incorrect dispatch and the open e-mail distribution list,

but also for the illegal phishing attacks as well as other forms of

cybercrime. Even if such data breaches are not

completely avoided, I appeal to all data processors

Introduce yourself to take even more preventive action in this area

above all through appropriate training to sensitize their employees

ren. In addition to the other technical and organizational measures

an experienced and safe handling of the technology as well as a

heightened awareness when dealing with IT security issues

contribute that various suspicions and irregularities better

perceived and identified accordingly and any attack behavior

seek to be prevented at an early stage, giving hackers no chance

their criminal activity is given.

17.3

Data breaches at processors

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

with processors pose a challenge for controllers

Deficits in the coordination and provision of relevant information

ments between processors and controllers often lead to

avoidable delays in the course of joint treatment

of data protection violations and thus ultimately also to a delayed

ten notification of the persons concerned. This post outlines

on the basis of the requirements of Art. 33 and 34 DS-GVO the expiry of the

Treatment of personal data breaches

based on an ideal-typical scenario of a ransomware attack

a processor. Then typical problem areas

from regulatory practice outlined during the reporting period

led to delays and deficits in incident handling. out of it

are expectations of controllers and processors regarding

the implementation of overarching processes for the appropriate handling of

data breaches derived.

260

technology and organization

Necessary cooperation between those responsible and

contractors

If personal data breaches occur in accordance with

Art. 4 No. 12 DS-GVO for processors according to Art. 4 No. 8 DS-GVO,

then there are often also those responsible according to Art. 4 No. 7 DS-GVO

affected, who process personal data by the processor

let work. Accordingly, there is also for those responsible

the duty to post personal data breaches

Art. 33 Para. 1 DS-GVO to the competent data protection supervisory authority

report. This applies if the incident is likely to result in at least one

risk for the rights and freedoms of the persons concerned has arisen.

In order for those responsible to be able to meet this obligation, the

Processor, for his part, fulfills his obligation pursuant to Art. 33 Para. 2

GDPR and report the incident to those responsible immediately

report (see also Chapter 17.2). With increasing number of involved bodies increases

also the probability that in the coordination between contract

process and those responsible for problems and avoidable delays

comes. During the reporting period, I received a significant number of

Personal data breaches reported in which

In this constellation, there are actually also not inconsiderable delays

ments in the treatment of the incidents came. Also I had to in several

identify deficits in the provision of information. This applied to both

for processors towards the responsible persons as well as from them

towards the persons concerned and towards my authority. Always

again there were also cases where those responsible incidents insufficient

have treated and thus their data protection obligations

sufficiently complied with at the insistence of my authority

are. Especially in data breaches where there is a high

risk to the rights and freedoms of data subjects

quick responses and adequate provision of relevant

information of particular importance. This is particularly necessary

to mitigate the negative impact of the incident and affected

To offer people their turn the opportunity to respond appropriately to the incident

to react.

In the following, the legal requirements of Art. 33

and 34 DS-GVO to processors and responsible persons in connection

related to personal data breaches

summarized. After that, an ideal-typical course of the joint

Treatment of personal data breaches

outlined by a processor and several responsible persons.

For this purpose, an exemplary scenario of a successful ransomware

51. Activity report on data protection

Attack on a processor used by all parties involved

respond appropriately and comply with their data protection obligations

deal with the incident. After that, based on this

Process explains where problems or

delays have occurred.

Data protection requirements of the GDPR

The controllers and processors in the context of breaches

the obligations incumbent on the protection of personal data as well as the

The deadlines to be observed here are regulated in Art. 33 and 34 DS-GVO. In

Art. 5 Para. 2 DS-GVO stipulates that those responsible for compliance

of the principles responsible for the processing of personal data

are and must be able to demonstrate compliance with them. According to Art. 12 GDPR

those responsible are also the interface for the data subjects

and responsible for enabling them to exercise their rights.

The basic requirements for the processing of personal data

Data by a processor are specified in Art. 28 GDPR.

The processing by a processor is in a contract processing

agreement (AVV) that meets the requirements of Art. 28 Para. 3

GDPR is sufficient. According to Art. 28 Para. 3 Letter f DS-GVO

to provide that the processor

Art. 28 Para. 3 Letter f GDPR

(3) (…)

f) taking into account the type of processing and those available to him

Information to those responsible for compliance with the provisions of Articles 32 to 36

supports the above obligations; (...).

This also includes those regulated in Articles 33 and 34 GDPR

duties. Art. 33 GDPR defines these as follows:

Art. 33 GDPR

(1) In the event of a breach of the protection of personal data, the responsible

verbatim immediately and if possible within 72 hours after the breach

became known to the competent supervisory authority pursuant to Article 55, unless

that the personal data breach is not likely to result in a

risk to the rights and freedoms of individuals. If the notification is sent to the

If the supervisory authority does not respond within 72 hours, it shall be given a reason for the delay

to add.

262

technology and organization

(2) If the processor has a personal data breach

becomes known, he reports this to the person responsible immediately.

(3) The notification pursuant to paragraph 1 shall contain at least the following information:

a) a description of the nature of the personal data breach,

as far as possible, specifying the categories and the approximate number of those affected

persons, the affected categories and the approximate number of affected personal

son-related datasets;

b) the name and contact details of the data protection officer or another

point of contact for further information;

c) a description of the likely consequences of the violation of the protection of personal

personal data;

d) a description of those taken or proposed by the controller

Measures taken to remedy the breach of personal data protection and

where appropriate, measures to mitigate their possible adverse effects.

(4) If and to the extent that the information cannot be provided at the same time,

the Controller may receive this information without further undue delay

make available gradually.

(5) The person responsible documents violations of the protection of personal data

including all personal data related to the breach of protection

facts, their impact and the remedial actions taken.

This documentation must be used by the supervisory authority to verify compliance with the

enable provisions of this article.

In order for a responsible person to be able to fulfill his obligations,

according to Art. 33 Para. 2 DS-GVO in any case obliged,

the person responsible for violations of the protection of personal data

report data immediately. In connection with Art. 28 Para. 3 Letter f

DS-GVO, the processor must inform a person responsible

provide the information it needs to perform its duties

to be able to comply.

All personal data breaches are protected under Art. 33

Para. 5 DS-GVO regardless of the risk by the person responsible

document. According to Art. 33 Para. 1 DS-GVO, a person responsible

based in Hesse violations of the protection of personal data

immediately and if possible within 72 hours to my authority,

if the data protection breach is likely to result in at least one risk

ko for the rights and freedoms of the data subjects. After

Notification of a personal data breach

However, not all relevant information is always immediately available. In

In this case, a first, possibly incomplete advance notice

to take place within 72 hours, provided that the conditions of Art. 33 Para. 1

GDPR are met. According to Art. 33 Para. 4 DS-GVO, late registrations are possible

my authority possible. These must, however, without unreasonable further

further delays (see also 50th Activity Report, Chapter 18.1).

If personal data protection breaches

likely to pose a high risk to the rights and freedoms of those affected

Persons arise, a person responsible has these according to Art. 34 Para. 1

GDPR immediately. The persons concerned

at least information to be provided is in Art. 34 Para. 2 DS-GVO

fixed. Also when fulfilling this obligation the person responsible has

the processor assigns them in accordance with Art. 28 Para. 3 Letter f DS-GVO

support.

Data Breach Scenario by a Ransomware Virus

attack

The process of handling a personal data breach

Data that meets the data protection requirements discussed here

fills, is illustrated below using a ransomware attack scenario

shown as an example. The usual flow of ransomware attacks

I have already written in my 50th activity report for the year 2020 in Chap.

18.2 outlined.

For the scenario considered here, a medium-sized

contract processor assumed, the person responsible a number of service

offers services. For the provision and contractual processing of these

services, the processor processes personal data

Data on behalf of those responsible. In addition, he also processes

personal data under your own responsibility, e.g. B. Employee data

of their own employees. The processing of personal data

takes place on various IT systems of the processor.

A ransomware attack in this scenario could proceed as follows: On

On a Friday afternoon, employees of the processor determine

that IT systems and services are increasingly subject to misconduct

and these fail successively. At the same time, customers who

serious that IT services are no longer available. The switched on

IT administration discovers that a ransomware attack is taking place. The

responsible employees inform other colleagues

and carry out the first measures that have been tried and tested for such a case

emergency plan are established. This also includes the early involvement of

company data protection officer.

Concrete technical and organizational measures are described below

not discussed in more detail as they are not relevant in the context of this presentation

technology and organization

are. Clues and further information in connection

with information security, for example, in the working paper

of the BSI "First Aid for a Serious IT Security Incident" (https://

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/

Ransomware_Erste-Aid-IT-Sicherheitsvorfall.pdf).

In the scenario considered here, the processor provides a first

Balance sheet states that a large amount of data was encrypted - including

also databases and content of network drives with data from customers.

The online backup was also encrypted and thus made unusable

(see also Chapter 17.7). The processor informs in accordance with Art. 33 Para. 2

DS-GVO immediately about its customers in their role as responsible

the incident and summarizes the current state of affairs. The transmitted

The information provided enables those responsible to assess the

of the magnitude and potential impact of the incident, as well as its own

risk assessment. Furthermore, the processor reports the violation

the protection of personal data in accordance with Art. 33 Para. 1 DS-GVO

within 72 hours in his role as responsible for him

competent data protection supervisory authority, since own employees from

incident and at risk to their rights and freedoms

must be assumed.

Even if it is not yet possible at this early stage to

to record the behavior conclusively, the first immediate notification

approval of those responsible is required. This is the only way for them to

to react on their part and, if necessary, to take the necessary technical and organizational measures

To take action. Those responsible then carry out

an initial risk assessment based on the reported status (DSK,

Briefing Paper No. 18: Risk to the rights and freedoms of natural persons,

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-08/

kp_18_risk.pdf). On the measures taken by those responsible

includes, for example, the separation of any connections to IT systems

and services of the processor. Since the IT services used by the

processor and the data processed there no longer

are available, appropriate contingency plans are implemented. If the

responsible persons come to the conclusion on the basis of the risk assessment that

the breaches of the protection of personal data are expected

at least a risk to the rights and freedoms of those affected

persons lead, they in turn report the data breaches accordingly

Art. 33 Para. 1 DS-GVO immediately and within 72 hours

competent data protection supervisory authorities. In it they describe the

Incident traceable and also indicate the processor, so that

the reports of different responsible persons assigned to the same incident

can be classified. In this scenario, it is a

first, provisional report, in the event of new knowledge or changes

risk assessments without undue further delay

Late registrations will be added. They inform the respective supervisory

listen to their first message with a corresponding note.

In cases where the initial risk assessment by those responsible for the

Result comes that the violation of the protection of personal

Data poses a high risk to the rights and freedoms of data subjects

result, they inform them immediately in accordance with Art. 34 DS-GVO

plus. For more information on reporting violations of the

Protection of personal data is based on EDPB Guideline 2016/679

(WP250rev.01 – Guidelines for reporting breaches of protection

personal data in accordance with Regulation (EU) 2016/679, as of:

February 6, 2018, https://datenschutz.hessen.de/sites/datenschutz.hessen.

de/files/2022-11/wp250rev01_de.pdf) and the examples for the message

of personal data breaches in the guideline

01/2021 (EDPB, guidelines 01/2021 on examples for the reporting of
Personal data protection regulations, version: 2.0, as of: 14.
December 2021, https://edpb.europa.eu/system/files/2022-09/edpb_guide-
lines_012021_pdbnotification_adopted_de.pdf).
As part of the scenario, the processor is further involved in the management
processing the ransomware attack. For the investigation of
incident, a specialized IT forensic service provider is commissioned. This
is also explicitly commissioned to determine which personal
Data the attackers had access to and whether and if so which data through
the attackers were exfiltrated.
After some time, the attackers contact the processor
up and inform him that they collect a large amount of personal data
have copied. They threaten to publish this data if not
ransom is paid. The processor follows the recommendations of the
BSI and the Federal Criminal Police Office (BKA) and does not meet the demand
according to (Federal Association of Municipal Associations, BKA and BSI,
Handling ransom demands for encryption Trojan attacks
on local government, as of March 3, 2020 https://www.bka.de/
SharedDocs/Downloads/DE/Our Tasks/Criminal Crimes/Internet Crime
nality/RecommendationsRansomware.pdf). The threat of attackers as well
dealing with this are relevant information that the person responsible
be notified immediately so that they can in turn carry out their risk assessment
can update. Even if in the course of further analysis of the
incident, it becomes clear which systems were affected by the incident and which
Data can be restored from an existing offline backup

technology and organization

possible, those responsible will be informed accordingly. Depending on

Those responsible report any changes in the risk assessment

the new situation again without further undue delay

summarized to your responsible data protection supervisory authority and

update their documentation in accordance with Art. 33 (5) GDPR. Furthermore

the responsible persons notify data subjects for the first time in accordance with

Art. 34 GDPR, if the updated risk assessment now

a high risk to their rights and freedoms can be assumed.

People who have already been notified will also be informed again, provided that

an updated information situation makes this necessary, for example due to

newly identified risks.

The attackers publish individual documents after a month

the exfiltrated data in the “dark web”. This serves as proof that the

Attackers have actually exfiltrated data and are said to be putting pressure on the

Increase processors to pay the demanded ransom. Few

later, the attackers start using successively larger amounts of data

provide download. These each consist of a conglomerate

documents, e-mail archives and database excerpts. throughout

ten publication process is observed by the processor for

IT service providers commissioned the publication platform for these purposes

Attackers and continuously analyzes the published data, in particular

also with regard to personal data. He prepares the analysis results

for the processor, so that he, in turn, assumes responsibility

appropriately and adjust their own risk assessment

can. The processor informs the responsible persons about

the new state of affairs, which in turn their risk assessment

update and take action if necessary.

Upon completion of the incident, the Processor and the

Those responsible identify the causes of the incident and critically review the

Processes and cooperation in the context of incident management. In the

The so-called “Lessons Learned” are based on those that have been met so far

adapted to technical and organizational measures and processes.

This scenario describes a process in which everyone involved has their

Obligations to address the data breach promptly

progeny. This means that there are no unnecessary delays. Through this

all those involved are informed promptly about the relevant state of affairs and

can react accordingly. This supports the timely capture of

Measures by the processor, the responsible persons and also

the persons concerned to remedy or mitigate the possible

adverse effects of data breaches.

Exemplary problem areas from supervisory practice

Based on the comparable injuries reported to me in the reporting

With regard to the protection of personal data, I have found that

the cooperation between processors and controllers

while dealing with this type of incidents in different areas

has potential for improvement. The following are some of these

Possibilities for improving processes are described.

The first avoidable delays and deficits often arise in

the initial supply of information to those responsible by the
contract processor. The termination of an IT security incident had in the
Usually a high priority for processors. The data protection law
Obligations were therefore always given priority. At the beginning
the treatment of an incident, it was often not yet known what exactly
had happened and the extent of the incident. It therefore happened
that processors should initially inform those responsible
put back, for example in order not to worry their own customers unnecessarily.
However, this meant that those responsible under data protection law
were informed too late and were only able to react too late.
Inadequate preparations and contingency plans also made themselves felt
negatively noticeable in successful ransomware attacks. So there was
for example processors who had difficulties, controllers
to contact since they have access to the contact information of the customers
and had lost their communication infrastructure and for this case none
had provided alternatives. There were also isolated cases in which
contract processors first provided information to the controllers,
which did not reflect the actual extent of the incident. Through this
those responsible were weighed with a false sense of security.
As shown in the scenario, the information situation can change
complex data breaches such as ransomware attacks successively
change. These changes were another source of delays,
if the processor does not promptly and
communicated appropriately prepared to those responsible, for example in the event
the announcement of the release of exfiltrated data. If at ransom-
ware attacks did not actively monitor the attackers' websites on the dark web

were, this usually led to the actual publication

of data was not known or only became known with a delay.

When data is published, it usually has to be analyzed

to personal data contained therein and those concerned

to identify people. Since published data but by the attackers

may be compromised, for example by being infected with malware

programs should not use this data without proper precautions

opened or otherwise processed. Furthermore, the effort

and the associated costs for such an analysis are very high.

If the processor and the controllers do not rely on a

responsibility for the analysis, this can cause major delays.

genes or even lead to the analysis not being carried out at all.

Further delays may arise if a processor

awaits the final result of the analysis of the published data,

before informing those responsible that a data disclosure

has taken place at all.

Avoidable delays also occurred on the part of those responsible

on. If from the first information of the processor e.g. B. not

it was clear whether or to what extent a person was specifically responsible

was affected, those responsible decided in part, first others

Waiting for information and not taking action yourself. However, it was

the task of those responsible, the information provided by the

processor about the breach of the protection of personal data

Evaluate data and present your own risk assessments based on this

take. In the event of an insufficient supply of information, they must

actively request further, necessary information. Even if at the beginning

If there is still little information available after the incident has been dealt with, a

carry out an initial risk assessment, since at least

it is known which personal data the processor processes for him

processed. A responsible person must carry out his risk assessment when it is available

review new information and adjust if necessary. If relevant

Changes must be checked to determine whether further measures need to be taken.

A recurring problem when processing the

breach of personal data protection was that

Those responsible report this to me directly in accordance with Art. 33 Para. 1 DS-GVO

any new information that is missing or relevant to me only upon explicit notification

made available for queries. Art. 33 Para. 4 DS-GVO provides,

that information can be submitted later, but this should be done without

unreasonable further delay occurred.

The processing of the processes in my authority was partly also

made more difficult by the fact that those responsible have to

beiters forwarded it to me without any processing or evaluation.

Particularly in the case of incidents involving many responsible persons, it therefore happened

that I have received the same e-mail from a processor several times without comment

got forwarded. Those responsible should submit the new

Put information in context to your report and in particular

Changes related to their risk assessment, on technical made

and organizational measures as well as any notifications

affected persons. For a deeper understanding of this

in addition, the information newly provided by the processor

be attached.

Conclusion and evaluation

The scenario considered was used to show how the communi-

cation between the processor, the controller and the

Data protection supervisory authority in case of breaches of protection

personal data triggered by a ransomware attack

have been should expire. Through quick and coordinated action

between the processor and the controller on the one hand

and avoiding the problem areas presented on the other side

avoidable delays in the process can be prevented or at least

be minimized. This eliminates possible adverse effects of

Personal data breaches on data subjects

Persons avoided or at least reduced. It is also ensured

that the notification of the persons concerned does not only take place in larger

some time after the actual incident.

In the event of an assumed high risk to rights and freedoms,

averting possible damage should be a primary concern for people affected

be in the interest of everyone involved. This also applies regardless of the legal

technical requirements of the GDPR. Therefore, special attention should be paid

to prompt and appropriate notification of those affected

people and their required support.

Elaborated and regularly practiced processes as well as emergency manuals

support the effective and efficient handling of IT security

incidents. When designing this, the implementations of the

data protection requirements as part of the planned processes

be ensured. In particular in the case of order processing

interlocking processes between processors and those responsible

required for data breach reporting chains that are shared

should be regularly rehearsed, evaluated and adjusted if necessary.

For a timely response, it is essential that the processor

Those responsible are informed quickly and appropriately. It can make sense in doing so

be that he reminds those responsible of their data protection obligations

remembered, especially when those responsible are smaller ones

companies or organizations.

270

technology and organization

Art. 28 Para. 3 Letter f DS-GVO already stipulates that the company

assisting a controller in complying with its obligations

the processor is to be contractually regulated. This includes in particular

dere also the duties related to the treatment of breaches of protection

concerning personal data. Depending on the processing activity

it therefore makes sense to provide appropriate,

to contractually record the services to be provided by the processor,

especially with time guarantees.

17.4

Testing the use of communication media at a large

Association

If certain forms of data protection violations occur in individual

responsible persons occur frequently, this can affect the data protection supervisory authorities

constitute a reason to carry out an unprovoked examination. One

Such testing can be especially true in the case of more complex organizational structures

require the cooperation of different specialist departments and several

have focal points. An example of a possible approach

in such an examination, the report shows a currently still in progress

examination at an association.

Occasionally I find that certain breaches of protection

of personal data accumulated at individual responsible

ten. Sometimes this can be a reason for me, a deeper one

to initiate testing. A large association based in Hesse reported in

several personal data breaches in the past

Data according to Art. 33 GDPR in connection with phishing. minimum

At least one of these reports revealed deficiencies at the technical level

and organizational measures. About this incident I have already in

reported in my 48th activity report on data protection. The editing

These reports were initially received without regulatory action

closed as it was deemed responsible

appropriate technical and organizational measures to

to better avoid similar incidents in the future. However, initially stayed

It is still unclear whether the planned measures are actually to the extent expected

would be implemented and thus now adequate protection at the

Processing of personal data at the relevant processing

activities exist. Therefore, I have decided, pursuant to Art. 58

Para. 1 letter b DS-GVO an unreasonable supervisory authority examination of the

initiate those responsible.

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

In 2020 and 2021, the independent data protection authorities
federal and state supervisory authorities face a variety of challenges
posed, not least as a result of the COVID-19 pandemic. The use of
Communication media was one of the focal points here, in particular
the use of video conferencing systems (VKS). Among other things, the DSK
Guidance on submitting personal information via email
(2020, https://www.datenschutzkonferenz-online.de/media/oh/20210616_ori-
entierungshilfe_e_mail_verschluesselung.pdf) and VKS (2021, https://
www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonfe-
renzsysteme.pdf) provided. I myself have added to my website
relevant information on VKS (https://datenschutz.hessen.de/datenschutz/
it-und-datenschutz/videoconferencing systems-general) and for use
by fax (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/
transmission-personal-data-by-fax) published. Furthermore have
I published an article on the use of e-mail in the 49th activity report.
Due to the injuries now more than three years ago
of the protection of personal data and a renewed incident in the year
2020 is a special sensitization for the topic from the association
expected phishing. The use of other communication media must also be considered
be made in compliance with data protection law. The publications cited
DSK and my authority bid for the respective communication media
guidance and assistance.

Against this background, I have audited selected processing
Activities with regard to the use of certain data protection law-compliant

communication media started. According to the focus of

official publications I have in advance the communication

media use of VKS, e-mail and fax selected for the test. Around

to enable an efficient and proportionate examination, I have that

The aim of the test is clearly defined in advance, for example to expand the test

on processing activities that go beyond employee data protection

lying to avoid.

The technical-legal focus of the examination is based on

the categories of affected persons of the previous incidents, the employees

data protection. Based on initial findings indicating that

that in the processing activities of the person responsible

workers based in countries outside the scope of the GDPR

be used, another focus will be on the international

data transfer lie. Likewise, colleagues from the

areas of club data protection and technical and organizational data protection

contribute their expertise to the examination.

272

technology and organization

The test is structured in such a way that initially based on the test order and

of the test objects contained therein an overview of possible ones

Procedures using the relevant communication media from the Ver-

responsible was requested. This overview had to be on a high

level of abstraction, only the designation of the procedures, the categorical

en of data subjects and the communication media used

contain. From this first statement of the person responsible

already recognizable that this no longer uses the fax and this as

Test object could thus be omitted. Along with this procedural

overview, information on the structure of the association was also requested, since

the association is made up of several bodies, which

Processing of personal data on the basis of order processing

28 DS-GVO enter into a relationship with each other.

The process overview allowed me to target processing activities

to select which are to be subjected to an examination. I have therefore in

Following this, according to Art. 30 Para. 4 DS-GVO, the corresponding excerpts

the list of processing activities of the person responsible as well as

the association's internal business management and order processing

lazily requested. These contracts also include overviews of the

taken by the individual controllers and processors

technical and organizational measures. In addition, there was now two

unequivocally recognizing that external processors are based in the USA

come into use. Since such data transmission is currently regular

can only take place on the basis of suitable guarantees in accordance with Art. 46 DS-GVO,

I also asked the association to introduce a so-called transfer impact

Assessment in accordance with Clauses 14 and 15 of the Standard Data Protection Clause

to be submitted to the European Commission. Such a transfer impact

Assessment must show what risks the person responsible has in the

Data transfer to the third country is taken into account and which supplementary

Measures he takes to ensure that in this processing

a level of protection for the personal data is achieved that

comparable to that within the area of application of the GDPR. In the

assessment of the adequacy of such supplementary measures

Among other things, I follow the EDSA recommendations 01/2020 (https://edpb.

europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_sup-

complementarymeasurestransferstools_en.pdf) on this topic.

The association has given my authority all the documents required so far

averages At the time this activity report went to press, they were in

in the detailed examination by my employees.

17.5

Privacy-related vulnerabilities in self-developed

software

Errors in the context of the in-house development of software can occur during the

operational use significant negative impact on protection

have personal data. This has an impact on

the entire life cycle of IT systems and IT services from internal

operation until disposal. Therefore, those responsible must already

implement the requirements of data protection during development and

take appropriate technical and organizational measures (TOM).

During the reporting period, I received complaints and reports of injuries

protection of personal data according to Art. 33 DS-GVO,

associated with exploitable vulnerabilities in self-developed

ter software. Mobile applications were particularly affected

(apps) and web applications, the use of which leads to violations of the

Protection of personal data within the meaning of Art. 4 No. 12 DS-GVO and

to the disclosure of unprotected data structures. ursa

were u. a. Authentication and authorization vulnerabilities

as well as other, well-known vulnerabilities, such as those found in e.g. Am

the Top 10 of the Open Web Application Security Project (OWASP Top 10)

finds. OWASP is a non-profit organization that aims to

improve the security of applications and services on the Internet. The

identified vulnerabilities were due to programming errors

attributed.

weak spot

In the following, vulnerabilities are to be understood as errors in the software

s that can make IT systems and IT services vulnerable to

become threats. This results in concrete dangers for the

processing of personal data. Will such vulnerabilities

successfully exploited, violations of the provisions of Art. 32 Para. 1 Letter b

DS-GVO specified protection goals confidentiality, integrity, availability

and resilience of the systems and services (see also 50th task

activity report, chap. 18.3).

individual software

Self-developed software (individual software) is an individual for the

needs and requirements of an individual organization or authority

de developed software. Unlike standard software, it won't

technology and organization

for a large market of potential users, some of whom are still unknown

developed. Individual software is used in the cases considered here by

an organization or authority's own software developers

created for their own use.

Identified vulnerabilities

In the following I will go by way of example and not conclusively on selected ones

Vulnerabilities from incidents that became known to me during the reporting period

a. These incidents all occurred in connection with custom software.

A company portal was accessed via an app, actually

Customers should only be allowed to see their own data. However could

on structured stored documents with personal data of others

Customers not protected by authentication and authorization measures

be accessed. Due to an incorrect authorization concept,

both in the area of the app used and in the company

tal, were involved in developing the connection between the app and the

Company portal authentication and authorization mechanisms

implemented incorrectly.

The subject of a further vulnerability were the person responsible

applied hyperlinks that allowed users to navigate through the web application

application to access personal data. As authentication and

The authorization feature was an identification number in the hyperlinks

included, which was assigned to the respective user. In the present

case could be changed by changing this identification number to personal

personal data of other users can be accessed. Since the identification

cation number was assigned consecutively, it was easily possible to find valid ones

guess identification numbers. Due to this vulnerability, without

other authentication features Unauthorized insight into partially special

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

be taken. Attacks that use these or similar vulnerabilities

also known as "Web Parameter Tampering" (OWASP) or para-

meter manipulation known.

In another case were entered in a web application after

the user name and the password these authentication features

transmitted in plain text as a parameter of the Uniform Resource Locator (URL).

In principle, by making authentication

characteristics, beyond the affected IT application, far-reaching risks

arise for the person concerned if they are used several times.

At the same time, such access can cause damage to the person responsible

arise themselves.

Possible actions

The following listed requirements and measures for the

In-house development of software focus on the presented

vulnerabilities and are not exhaustive. In the following, the goal is one

to give an initial impression of concrete options for action in order to

to prevent vulnerabilities during development. Further

Measures should be taken from the relevant regulations.

In this context, by way of example and not conclusively,

extensive information on suitable measures by the BSI and the

OWASP will be directed.

Developers should already in the development phase of a software

data protection requirements and possible TOMs for their implementation

know setting. In this way, you can help right from the start

the software can later be used in compliance with data protection law.

An important prerequisite for the in-house development of software is the

initial and ongoing quality assurance. In particular,
the aspects of data protection are also sufficiently taken into account
become. Is quality assurance an integral part of the development
zess, the probability increases that vulnerabilities are already in the
recognized as part of the implementation and before the software
goods can be remedied. Some of those featured in this post
Weaknesses would have, for example, in the context of suitable function tests
can be detected and remedied (BSI, IT baseline protection compendium,
"CON.8 software development", as of February 2022, https://www.bsi.bund.
de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grund-
schutz_Kompendium_Edition2022.pdf). Communicated by manufacturers
Weak points and other information, for example in articles, contributions in the
Internet or from institutions such as BSI, HBDI or Hessen CyberCom
petenceCenter (Hessen3C), should also be used with self-developed software
be given attention.
If new software is not tested sufficiently, errors in the software can occur
be overlooked. Such mistakes not only endanger personal data
Data in operation, but possibly also other applications and
IT systems in the productive environment. Are safety functions, e.g. B.
the implementation of basic protection requirements, not tested, is not
ensures that the later use of the software meets the requirements
of Art. 32 (1) GDPR. Depending on each
exploitable vulnerabilities can consequently personal
data is disclosed, manipulated or destroyed without authorisation.

In terms of vulnerabilities in proprietary software, it shouldn't
only the self-created source code should be considered, but also
built-in libraries and frameworks. As an example at this point
the vulnerability in the framework that became known in December 2021
Log4J should be mentioned. This allowed attackers under certain
Conditions to exclude own program code on the affected servers
to lead. The freely available framework was among other things in a multiplicity
different individual software have been integrated, whereby the on these
based IT systems and services were at least potentially vulnerable.
Security updates should therefore be identified and distributed as promptly as possible
Consideration of the operational needs recorded as quickly as possible
become. Are the libraries and frameworks in use reaching the end of their
life cycle, this must be recognized proactively and taken into account in such a way
that obsolete components are replaced at an early stage. So that vulnerabilities
detected and fixed when using libraries and frameworks
must also have procedures for periodic review
established and applied. The same applies to self-designed
developed software used runtime environments.
In addition to a continuously accompanying check, the regular
Implementation of penetration tests (pen tests) among other measures
to consider. Pentests are comprehensive tests
the security of IT systems and IT services, in which software-related
vulnerabilities can be identified. The focus will be at
such tests for vulnerabilities that are suitable for unauthorized use
invade IT systems and services. Pentests go through the auto
automated use of vulnerability scanners.

In conclusion, it should be borne in mind that the approaches described above and

Procedure not only for the first project for the initial implementation of

developed software should be used. Rather, you will

also required in all subsequent projects, for example as part of further development

the software.

Conclusion

There is no software without bugs. This also applies not least to self-

developed custom software. The cases shown are examples of im

Personal protection violations that occurred during the reporting period

ner data due to exploited vulnerabilities in individual software.

They show examples of the processing of personal data

Data using self-developed software associated risks for the

Rights and freedoms of natural persons based on exploitable

vulnerabilities. It should be noted that such risks not only

are limited to in-house developments and individual software, but

also go hand in hand with standard software. It must therefore always be suitable

Methods and procedures are defined and lived, so that risks

recognized and suitable TOMs derived for this purpose as well as already during the

Creation of the software can be implemented successfully. Indispensable

is a procedure for testing and regular review, evaluation

and evaluation of the effectiveness of such measures in self-developed

Software, even beyond the self-programmed source code. supplementary

Finally, pen tests can be used. The use of valid information

tion sources are an important tool to start with when creating
Software, but also to be able to identify and eliminate risks afterwards. This
includes in particular the possibility of rapid identification and
Implementation of necessary updates, e.g. for integrated libraries
and frameworks as well as for runtime environments. The same applies to any
Announcements of impending end of life of integrated
components and the resulting need for replacement.

17.6

Notification of those affected in the event of misuse of e-mail
accounts

If a responsible body determines that its communication services are through
taken over by an attacker and used to send phishing messages
are misused, it is obliged to do so on the basis of a risk assessment
Check whether those affected should be notified of the incident. At a
such examination there is a risk that the responsible body the amount
of the personal data concerned is not fully recorded and only
considered a subset. The report shows an example of such a case
from a recent report by a commercial entity.

During the period under review, I saw an increase in reports about
Violations of the protection of personal data according to Art. 33 DS-
GMOs resulting from the illegal takeover of email accounts.
Attackers successfully hijacked third-party e-mail accounts and misused them
then use them to send malicious phishing emails. At
With this form of attack, the attackers tried to be more trustworthy
senders and designed their messages as if they were
legitimate requests. The aim of the attackers is to lure the recipient into a prize

be personal information such as bank details, credit card numbers or

to move access data. For example, with reference to

278

technology and organization

previous conversations "changed bank details" by the attackers

submitted to commit wire fraud. Hy-

perlinks to rogue login masks created by the attackers

Distributed to services such as server portals in order to access further access data.

In the second quarter of the reporting period, I received a notification pursuant to

Art. 33 DS-GVO of a listed company about the successful

Acquisition and the subsequent misuse of the e-mail function mail

times a branch of the company. Via the hijacked email account

A mid four-digit number of phishing e-mails were sent to customers and

employees sent. Upon discovery of the incident and initiation of

technical and organizational measures to terminate the same

reported the responsible body that the data subjects in accordance with

Art. 34 DS-GVO on the data protection violation by a letter

had been notified.

As part of the clarification of the facts, I asked questions about the incident

as well as the types and categories of personal data affected,

in the content and attachments of the emails of the email account concerned

tos were included. The responsible body replied that the

affected e-mails only personal data in the form of first name

and name of the respective e-mail recipient. In the course of

Further communication turned out to be the responsible body

only the recipients of the sent phishing mails as those affected

considered and thus only informed them about the incident.

The procedure of the responsible bodies that only the recipients of the

sent phishing messages were notified of the incident,

I observed a large part of the incoming reports in the same

stored cases. Regularly the options presented to the attackers

offer when taking over an e-mail account, not fully considered.

It can always be assumed that the attackers gain access not only to

Send malicious phishing emails. In addition, they get access

to the content and attachments of the e-mails in the transferred e-mail inbox

and can thus become aware of the personal data contained therein

obtain. Thus, in addition, there is a breach of confidentiality

data given. This circumstance makes it necessary that in the context

a risk assessment according to Art. 34 Para. 1 DS-GVO not only the recipients

of the phishing messages are taken into account as data subjects.

In addition, those persons whose personal

Data stored in the content of the email account taken over or

processed, included in the considerations. Likewise are

possibly to check further functionalities of e-mail services. in service

such as calendars, calendar attachments and address books can add more

personal data and be affected by the incident. Further

I have observed in previous reports of similar cases,

that attackers use their access to e-mail accounts, for example

create automatic forwarding or deletion rules. With such

Rules can, for example, include incoming information from suspicious recipients

Phishing mail deleted immediately or new e-mail messages automated

forwarded to an external e-mail address.

According to Art. 33 Para. 5 DS-GVO, the responsible body has the obligation to

in connection with the violation of the protection of personal data

Data standing facts to document me a review

make possible. Of course, such documentation includes

also the identification of those affected and the risk assessment. Think

Authority demands when processing reports according to Art. 33 DS-GVO

regularly review this documentation and check it for completeness and

traceability. If this documentation is not complete,

constitute a breach of duty.

Is there anything unclear about the subject areas at the responsible office?

Assess the risk, report to the regulator and report to

those affected may use the guidelines for reporting injuries

of the protection of personal data of Art. 29 Data Protection Working Party

(https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/

wp250rev01_de.pdf) as well as the short paper no. 18 of the DSK (https://datenschutz.

hessen.de/sites/datenschutz.hessen.de/files/2022-08/kp_18_risk.pdf) as

use guidance. The guidelines deal with Chapters 3 and

4 with information on the three subject areas and in Appendix B of the guidelines

a list of case studies in different scenarios is presented.

In turn, the DSK describes in detail in its short paper its

agreement on how the GDPR will be applied in practice

should, and here it focuses in particular on the points of determination and assessment

and risk mitigation.

In the present case I have the responsible body over the above

Circumstances informed and an extension of the risk assessment

on the content of the e-mails and their attachments in the e-mail account concerned

asked. The responsible body has confirmed to me, as part of a

the content and attachments of the e-mail in the new risk assessment

affected account into account.

280

technology and organization

17.7

No backup? no pity! – Ensuring availability

Ensuring the protection of personal data includes

ensure their availability. An essential building block for this is the

Regular execution of data backups. Not least

the increasing number of successful ransomware attacks shows that the

Demands on effective backup concepts have increased. Hereinafter

an overview of the possible effects of missing or inappropriate

extensive data backups in the event of data protection incidents. on this

building on those responsible and processors in

requirements for backup concepts to be taken into account in each case are outlined.

motivation

"No backup? No pity!” This statement has meanwhile become a

has become a widespread proverb in IT-savvy circles and is mostly used with

recited with a slightly mocking undertone. Coffee mugs, t-shirts and others

Merchandise items with this saying are considered ideal gifts

advertised for IT administrators and computer scientists. What might turn out to be a

A typical saying from IT people may sound like, but it also has a legal meaning

Correspondence in the GDPR. Because to the principles of data protection
according to Art. 5 Para. 1 Letter f DS-GVO, processed personal
data against loss, destruction or damage by appropriate
technical and organizational measures to protect. The implementation
of regular and effective data backups is probably the
most common appropriate measure used for these purposes.
The existence of an existing backup and the question of how this
can be set, often only becomes relevant when due to a
Data backed up from an incident should or need to be restored.
This is the case, for example, if something is accidentally deleted or
was overwritten, a hard disk only produces errors when accessed
or an IT device fails or is lost. In these cases it shows
that by a missing, an ineffective or an insufficient
Backup the availability of personal data may be at risk
can. This entails corresponding risks for the rights and
freedoms of data subjects.
The category of data protection incidents in which the relevance of complete
properly implemented backups are the most descriptive
so-called ransomware attacks. In summary, it is
in the case of ransomware attacks, attacks on IT systems or IT networks
with criminal intent. The aim of these attacks is to hit the target successfully

to encrypt data stored on compromised IT systems and
for providing the keys required for decryption

demand payment of a ransom. Because backups serve the goals of

grabs, attackers usually look specifically for these,

to encrypt them as well or make them unusable. In my

50th activity report (chapter 18.2) for the year 2021, I have dealt with

somware attacks in more detail.

Examples from supervisory practice

The following examples of data protection incidents reported to me in the

reference period illustrate the relevance of backups.

The first example relates to a small company that is

vante carried out all data processing on a central server.

This also included backing up the data on this same system. Through

a successful ransomware attack on this server were all

Company data, including backups, are encrypted and thus

rendered unusable. Not all data could be obtained from "analogue" sources

such as paper, printouts or the like. This example

clearly illustrates that not every form of backup is sufficient

Measure is to ensure the availability of data reliably.

So how important is it to back up data on an external, non-vulnerable

data carriers connected to the IT infrastructure, a so-called offline

Backup, demonstrates the second example from a larger IT company,

which was also affected by a ransomware attack. The company

had a dedicated backup system as a so-called online backup.

The backup system was integrated into the normal IT infrastructure and

was able to back up data directly from the other IT systems.

However, the attackers managed to gain access to this online backup

to provide system. You were thus able to not only all backups

on this system, they also had access to the

the company's relevant data concentrated at one point. How

the IT forensic analysis of the incident revealed that the extensive

Exfiltration of company data from this backup system.

But since there was another backup system that backed up the data

magnetic tapes – as an offline backup – it was the company

possible to restore at least all relevant data.

It doesn't always have to be a ransomware attack due to a

insufficient preoccupation with the effective implementation of a backup

significantly increases the severity of a data breach. An example of this

is a responsible person who has his e-mail infrastructure from a contract

let the processor operate. At the beginning of the contract was the creation of backups

of the e-mail accounts are part of the service catalog of the processor. After

for some time the backup functionality was provided by the processor

however, removed from the scope of services booked by the person responsible.

The person responsible did not respond to this. This led to the at

e-mails that were specifically deleted after a hacker attack

chen relevant email accounts could not be recovered.

This example shows that it is not sufficient to start a new one

Processing activity to set up a measure once and then apply

assume that these over the entire life cycle of a processing

activity remains effective. Rather, technical and

organizational measures are regularly reviewed, assessed and evaluated

become. Adjustments must also be made if necessary.

Data protection assessment with legal justification

The basic data protection requirement to guarantee

the availability of processed personal data results from

Art. 5 Para. 1 Letter f GDPR. After that, personal data must

Art. 5 Para. 1 Letter f GDPR

processed in a manner that ensures appropriate security of personal data

Data guaranteed, including protection against unauthorized or unlawful processing

protection and against accidental loss, accidental destruction or accidental damage

Damage through appropriate technical and organizational measures ("Integrity and

Confidentiality"); (...).

The effective implementation of a backup concept would be a technical and

organizational measure (TOM) to protect against "unintentional

loss, accidental destruction or accidental damage".

The other requirements to be met for such a concept are

in Art. 32 Para. 1 and 2 DS-GVO to ensure the availability of personal

of specific data.

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.

In Art. 32 Para. 1 Letter c DS-GVO as a basic ability of a backup

required that data be recoverable in the event of an incident.

In Art. 32 Para. 1 Letter d DS-GVO it is required that the technical

and organizational measures, such as backup, regularly as a result

checked, evaluated and evaluated whether the effectiveness continues to be

is guaranteed. For a backup, this means that not only the successful

creation must be checked regularly, but also the restoration

recovery of data from a backup. As part of the organizational

Measures related to backup include having appropriate processes

exist, are documented and the persons responsible for the backup

practice restoring data regularly.

The development of a backup concept also includes the implementation of a

Risk analysis to meet the requirements of Art. 32 Para. 2 DS-GVO

to be able to. In connection with Art. 32 Para. 1 Letters b and d GDPR

but this cannot be a one-time affair at the beginning of development

be. Rather, the concept must also be critically reviewed on a regular basis,

evaluates the effectiveness with regard to changed framework conditions

evaluated and adjusted if necessary.

Practical minimum requirements for a backup concept

There are a number of aspects involved in creating a backup concept

to consider. The corresponding BSI IT basic

Protection module "CON.3 data backup concept" with the associated

provide implementation instructions.

technology and organization

The so-called 3-2-1 strategy is often used as a backup strategy

backups referenced. This one is about how many copies of data

how and where should be held. 3-2-1 means that at least

at least three copies of the data to be protected including the original data

are to be kept ready. These three copies should be at least

stored on two different storage media. Of that should

at least one copy must be kept at a separate location.

This strategy already helps against many relevant risks, from accidental

chem deletion of data to damage to a storage medium

to catastrophic damage to a site. For protection against

Targeted attacks on the IT infrastructure like a ransomware attack

however, this may not be sufficient.

As the examples above show, attackers try to compromised

IT environments usually gain access to relevant IT systems

and actively look for backup systems to make them unusable

make. Accordingly, these systems are also explicitly against you

to protect against unauthorized access from within your own IT environment.

An obvious measure would be to create offline backups, like

for example by means of magnetic tapes that are accessible to potential attackers

are effectively withdrawn.

The manual effort usually associated with offline backups is eliminated

towards the goal of having access to the most up-to-date data copies possible. With

online backup systems fully integrated into the IT environment,

can, on the other hand, be automated regularly and at shorter intervals

Data backups are performed. Even with these, the risk can be reduced

of a successful attack when designed

and implementation, these backup systems are secured in a similar way to IT systems

tems or services that are directly accessible via the Internet and thus

could be attacked at any time. Depending on the application

it may be useful to have appropriately secured online and offline backup

to combine systems. It is important that the overall concept for the

implemented backup strategy is consistent.

As detailed in the legal requirements section, it is necessary-

manoeuvrable to ensure that backups are performed successfully and

that restoring data from backups in the required time

functions. Depending on the processing activity, sole access to

the data may not be available without the IT systems and services that process them

be sufficient to ensure the availability of the data. To the-

Accordingly, it is necessary according to Art. 32 Para. 1 Letter b DS-GVO,

also the availability of these IT systems and services through corresponding

to ensure measures in the long term. Appropriately well-documented
Emergency or recovery processes must consider this holistically
consider. The effectiveness of these processes is also regularly increasing
checked and also practiced by the responsible personnel. Just the latter is
against the background that the need to access backups in
emergency or stressful situations occurs, very important. It therefore makes sense that
Conducting these tests should be rotated among the responsible employees
and to ensure that this also applies accordingly in substitution situations
trained and experienced staff is available.

Data backup is data processing

From the point of view of data protection, the guarantee goal is availability by means of
performing backups of processed personal data
ensure. The data backup is itself a separate processing
activity, for those responsible and processors the corresponding
must meet the requirements of the GDPR. Among other things, should
Creation of a backup concept the rights of data subjects, their
data are processed, are taken into account at an early stage and continuously.
This starts with the right to information in accordance with Art. 15 DS-GVO, which also extends to
can obtain data that may still be stored in backup systems.
Similarly, the right to correction according to Art. 16 DS-GVO, the
Right to deletion according to Art. 17 DS-GVO and the right to restriction
the processing according to Art. 18 DS-GVO data within the backup system
affect me. The possible effects must therefore be investigated and

to provide appropriate technical and organizational measures,

to ensure the exercise of rights.

Data backup as a processing activity must also

Requirements of Art. 32 GDPR for the security of processing

meet personal data. The integrity and confidentiality of

secured data must be guaranteed accordingly. One

A suitable measure for this is the encryption of the data, if these

properly designed and implemented. More details on this

Topics in connection with data backup using cloud services

ten can be found in the previously referenced IT basic protection module "CON.3

Data backup concept" of the BSI corresponds to the standard

requirement "CON.3.A9 Requirements for online data backup".

286

technology and organization

Conclusion

So it remains to state that regular and effective data backups

Personal data processed through backups, usually to the

necessary technical and organizational measures in order to

the security of the processing, in particular with regard to availability

to be able to guarantee. Bodies processing personal data

must therefore actively and continuously deal with the topic,

especially with regard to the threats of attacks. Because like says

already the saying popular with IT people: "No backup? No pity!”

287

public relation

18. Public Relations

public relation

In 2022 I have a stronger focus on public relations

placed. On the one hand, I have staff in my public relations department

increased by one position. On the other hand I have with her in the

External presentation of new event formats. As a result falls

the balance of the events for the year 2022 is very positive.

DataTuesday

The year started with my participation in the Safer In-

ternet Day on February 8, 2022 in cooperation with colleagues from

LDA Bayern and the Museum for Communication in Frankfurt. The topic

was “Together for a better internet – challenges over

Perspective of data protection supervision”. At DataTuesday, experts

Experts Topics to do with data protection and IT security come and go

then talk to the museum audience to raise awareness

for data protection issues. I have in my lecture

on the occasion of Safer Internet Day 2022 not only current fields of action

taken up, but also to structural issues in use

of the Internet by companies and authorities.

CAST Forum on Improvements in Data Protection Law

On March 17, 2022, the CAST forum on the subject of "Ver-

Improvements in data protection law - How can the projects of the

Implement traffic light coalition?” instead. The event was organized by Competence

Center for Applied Security Technology (CAST), the Privacy Forum and

performed on me. The coalition agreement between SPD, Bündnis 90/Die

Greens and FDP promise an "alliance for freedom, justice and

Sustainability". The coalition sees itself “at the beginning of a decade

upheaval". The “necessary modernization” of state and society

Above all, she wants to achieve this through the digitization of the economy and society

"propel". The coalition agreement lists 155 projects, the most

sense of privacy, self-determination and data protection affect or

affect these values. With its program, the coalition wants to

Sustainably improve the conditions for realizing these fundamental rights. Goal

of the forum moderated by me was the programmatic statements

of the coalition agreement then to analyze how the abstract specifications

need to be fleshed out with practical experience in order to actually make progress

in individual fields of digitization and data protection.

The event addressed the current situation in six lectures

Data protection law and data protection practice, informed about the

abstract projects of the coalition, placed them in the context of the current one

Privacy discussion and presented proposals how these projects

to improve data protection law and data protection practice

can be specified. The presentations covered the topics of

Transfer of personal data to third countries, strengthening of the

rights through a right to encryption, a right to anonymization

and through specifications for IT vulnerability management, how to deal with

research data and the introduction of new institutions such as data markets

and data trustees, the legal assessment of AI applications in

of the EU AI Regulation and national supplements, improvements in

Employee data protection and the introduction of an overall monitoring

bill for surveillance laws.

Authorities Day Hesse and Rhineland-Palatinate

On June 28, 2022, in cooperation with the State

data protection officer of Rhineland-Palatinate and the professional association of data

Protection Officer of Germany (BvD) e. V. for the first time the “Authorities Day

Hesse and Rhineland-Palatinate”. The all-day event was aimed at

to official, municipal and company data protection officers. The

Conference gave in particular data protection officers of public bodies the

Opportunity to meet with professionals from regulators on issues

to exchange information that they deal with in their everyday professional practice. In addition

included current issues of international data transfer in the year under review

and artificial intelligence in public administration as well

the structure of the state data protection laws and their interaction with

European regulations such as the General Data Protection Regulation and

the data protection directive in the field of justice and home affairs. Also current

Practical topics such as cookies, social media fan pages and video conference systems

tems as well as the rights of those affected have been implemented in a total of 17, partly in parallel

keynotes, specialist lectures and panel discussions that take place

tet. In addition to the exchange among themselves, the participants were able to

with their questions directly to the experts from the supervisory authorities

approach. This applied both to the conference breaks and to the inter-

active final panel "The supervisory authorities answer your questions".

The very well-attended Data Protection Day was an important one for everyone involved

Element of professional training, mutual understanding

for each other and the exchange of experiences. It's very special to me

Concern to accompany and support this professional exchange.

public relation

That's why we already have the 2nd Hesse - Rhineland-Palatinate authorities day for

scheduled for July 5, 2023.

Open days in the Hessian state parliament

On September 24th and 25th, 2022, my authority took part in the days of the

open door of the Hessian state parliament. Under the motto "Democracy

to touch" the Hessian state parliament had all citizens

at the weekend to the open house days in Wiesbaden

State capital invited. At my agency's stand, many took the

Opportunity to find out about the data protection supervisory activity

inform. My public relations department had a stand with me

Information materials and various posters prepared, about mine

Staff with the citizens in brisk

exchange came.

Celebration of 50 years of data protection in Hesse

In 1970, the Hessian state parliament with the Hessian data protection

Act (HDSG) passed the first data protection law worldwide. In the

the following year, Hessen became the first data protection officer in the world

established, who published his first activity report in 1972. After

the celebrations planned for these anniversaries in 2020 and 2021 pandemic

dings were not allowed to be carried out, they were all three on October 6th

Made up for in a ceremony in 2022.

The President of the Hessian State Parliament, Astrid Wallmann, opened the

design. Among other things, they acknowledged that the Hessian state parliament in

wrote international data protection history in 1970. The

Law has the Office of the Hessian Commissioner for Data Protection as
independent control authority created. It was also emphasized how important
and forward-looking this decision was, what has been seen to this day
be hen In the digital age, data protection is particularly important
Challenges.
The Minister for Digital Strategy and Development in Hesse, Prof. Dr. cris
tina Sinemus, congratulated on behalf of the state government. The data protection
have gained even more relevance with increasing digitization.
Personal data in particular, such as in the health sector, is extremely important
asset worth protecting. So you need a good balance between that
Use of data and protection of data. Then a responsible
efficient digitization for the benefit of everyone in society.
291
The Hessian Commissioner for Data Protection and Freedom of Information
51. Activity report on data protection
In the keynote speech, Prof. Dr. Thomas von Danwitz, judge at the ECJ and
Rapporteur in many court cases on data protection that still exist today
current objectives and specifications of the first Hessian data protection
law, which were also reflected in European data protection law. He
outlined the main ideas of the case law of the ECJ and concluded
with the realization: “A democratic society that takes its citizens seriously
and - like the Charter of Fundamental Rights - the people in the Central
point of their actions” is realized in the age of digitization
also and above all through high-quality data protection. This enables
public institutions of the state and business enterprises
equally in free self-determination at eye level.

(https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/

datenschutz_in_hessen_und_europa_6_10_22_von_danwitz_kv.pdf).

The ceremony was rounded off with a historical arch. In my

I have attached statements to the conditions of data processing and the

Data protection 50 years ago with "area data centers, punch cards and

magnetic tapes" and have them with today's challenges

through the data power of global internet corporations and globally networked

Data processing contrasted. With the statement: "Especially given

of these radical changes, the objective of the first still applies

Hessian Data Protection Act that freedom rights and democracy

Require containment of information technology. Only if they

data protection guidelines and data protection-compliant technology design

be protected, we can be sure that we are using information technology

live better than without them", I closed the ceremony (https://

datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/rossna-

gel_lecture_ceremony_50_years_data_protection_in_hessen.pdf).

25th Wiesbaden Data Protection Forum

The afternoon concluded on the subject of "Data protection strengthens research".

October 6, 2022, the 25th Wiesbaden Data Protection Forum. After

After a break due to the pandemic, the specialist audience met in Hessian

state parliament and devoted himself to the relationship between research and data protection.

Both are often seen as conflicting interests. However

must both – freedom of research and informational self-determination

– are seen as fundamental rights that require attribution

restricts the other fundamental right as little as possible. So be it

A prerequisite for gaining the trust of patients

who should consent to the use of their data. To the forum

invited four speakers, who are in different

292

public relation

approached the topic “Data protection strengthens research” in a logical way.

The Federal Commissioner (BfDI) Prof. Ulrich Kelber went in his lecture

"Scientific research - of course with data protection".

Ask what legal policy framework is necessary to achieve the goal

achieve responsible data use. For this he formulated ten

bids – e.g. B. Supporting public interests in research that

active participation of data subjects, the protection of personal data

Data through anonymization, pseudonymization and encryption,

the use of data trustees and protection against re-identification.

Prof. Dr. Franziska Boehm from the Karlsruhe Institute of Technology (KIT)

examined in her lecture “The special protection of research in the

General Data Protection Regulation”, which special consideration of

Research interests the DS-GVO provides and how these special rules

can be applied in practice. She pointed to exceptions

men z. B. from earmarking, data minimization, storage limitation,

Certainty of consent, rights of data subjects and of

Requirements for data transfer to third countries. Also offer

the GDPR offers the Member States opening clauses for research purposes

further to be preferred. These should also be used in German

Right to harmonize different legal regulations on research.

Prof. Dr. dr Eric Hilgendorf from the University of Würzburg reported in his

nem lecture “Data protection in the future regulation of European

Research Data Spaces” of a total of 49 legislative acts or initiatives

tives of the European Commission on the digital transformation of Europe.

To facilitate the use of data - in particular for research purposes

– primarily served the Data Governance Act and the drafts for a

Data Act and to regulate a total of 13 European data

men. He found that data protection in these legislative

files are not systematically taken into account. So he advocated

a moratorium to safeguard against adverse effects on

adequately adjust fundamental rights. Prof. Dr. Hannes Federrath from

of the University of Hamburg showed in his lecture “Privacy Protection

Methods of research data processing” on how the most modern methods

of computer science can contribute to effective research processes without

to allow privacy issues. As protection possibilities he gave five

Privacy design strategies: Minimize (restriction to necessary data

ten), Separate (decentralized data analysis at the storage location), Aggregate (from

abstract personal reference), pertubate (personal reference through noise

exclude) and hide (prevent access to personal data).

From Hesse to the world

With the topic "From Hesse into the world: The development of data protection

in the interplay of communication technology and law” dealt with am

2 November 2022 an event organized by my authority in cooperation

with the Forum Privatheit and the Museum for Communication in Frank-

furt organized. At the dialogue event, Dr. H. c. maritime

Hansen, State Commissioner for Data Protection Schleswig-Holstein, and I

as spokesman for the "Privacy Forum" and Hessian representative for data

protection and freedom of information moderated by Dr. Ulf Buermeyer

LL. M. (Chairman of the Society for Freedom Rights e. V. and host of the

Political podcasts "State of the Union") with 50 years of data protection history

te apart. The history of data protection law began with

Hessian data protection law of 1970, the first data protection law

of the world. That a lot has happened since then and data protection has changed

Hessen made its way around the world showed our common

mer lecture - a path that was characterized by an interplay between

Innovations in information and communication technology on the one hand

and in data protection law on the other hand. We found that

new technical developments always new challenges

mean for data protection law, which in turn with new

regulations and laws. This in turn stimulate new technical

Developments to meet the legal requirements - or to them

evade. Marit have this interplay between technology and law

Hansen from the point of view of the computer scientist and I alternately illustrate

light. Telecommunications took place in 1970 at the time of the first Hessian

Data Protection Act still anonymous and without data storage. Today,

at the time of the European General Data Protection Regulation, in the

electronic communications collected so much data that with them by

complete interest, relationship and movement profiles for all users

are possible and there are interests of state and private bodies, these

evaluate for their purposes. The focus was on questions such as E.g.: Which

Risks to fundamental rights are associated with the development of information technology

tied together? What regulations does data protection law have against these

developed? How can law and technology work together to

improve privacy? And: How can they do this – given global

operating companies – do worldwide?

In addition, at the end of the year under review, the website of my

authority updated. HZD IT support for the old site has expired.

The new site is more modern and thematically more attractive. Current

the departments revise their contributions and thus guarantee that

next year a lot of new interesting content.

19. Labor Statistics Privacy

Labor Statistics Privacy

19.1

facts and figures

The statistical evaluation of the workloads in this chapter 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

arrangements)

(4) according to Art. 58 Para. 2 i (fines)

(5) according to Art. 58 Para. 2 h (revocation of certification

gene)

case numbers

01/01/2021

case numbers

01/01/2022

until

until

12/31/2021

12/31/2022

5.179

4,474

(of that

953

(of that

736

taxes)

taxes)

2.123

1,334

2.016

1,754

(1) 1

(2) 28

(3) 3

(4) 29

(5) 0

(1) 1

(2) 37

(3) 16

(4) 113

(5) 0

295

The Hessian Commissioner for Data Protection and Freedom of Information

51. 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 ff.)

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) 47

(2) 16

(3) 1011

(1) 11

(2) 2

(3) 982

34

35

19.2

Supplementary explanations of facts and figures

The following illustrations explain and supplement the evaluations

in chap. 19.1 also in comparison with the previous year and the other work

offer in the reporting year. Overall, the number of cases stabilized at seven

years after the entry into force and five years after the entry into force of the

GDPR at a very high level. It can be observed that

in many areas the quality of the complaints and the need for advice

changes. While at the beginning questions about more formal requirements

of the GDPR were in the foreground (e.g. after the obligation to place an order

a data protection officer, on information and access rights

of the person concerned), there are many questions that I dealt with in the reporting year

had to deal with in more depth and raise fundamental questions.

Complaints and Advice

Even if the complaints and requests for advice in connection with

COVID have declined, the pandemic still has a lasting impact

on the workload in my agency. As before, he gets through

the digitization push triggered by the pandemic also via the pandemic

In addition, there is a very fundamental and very labor-intensive need for advice

with himself. In the year under review, it became apparent that technical solutions

such as video conferencing technology, which is quickly used in the pandemic

were brought to schools, colleges, factories and administration

to keep it running, also be used beyond the pandemic

men. Since the introduction had to be done in a hurry, we now had to do it afterwards

the requirements of data protection are brought to bear. Also

other major digitization projects such as the implementation of the

Online Access Act, which obliges the federal, state and local governments to

by 2022 their administrative services via administrative portals also online

offer are not reflected in the statistics to the same extent as they are

actually employ my agency.

In almost all areas in which my authority is active,

towards the question of the requirements for GDPR-compliant international

data transfers play a major role.

It is gratifying that the number of complaints is declining in some areas.

Even if it is difficult to name the specific reasons for this,

I observe, for example, that more and more websites offer the possibility

all non-essential for the use of the website with one mouse click

refuse cookies. In the area of trade, commerce and handicrafts, the

Complaints about requests for information not being answered or not being answered correctly

back. Such developments I attribute to the gratifying circumstance

back that in these and similar questions there is now a certain

exercise that gives less cause for complaint.

A clear increase in the numbers in the area of traffic is due to

lead to numerous supermarket car parks by specialized

Companies are monitored with video technology.

The following overview shows the number of submissions (complaints and

consultations) of the reporting year compared to the previous year:

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

634

132

772

255

413

314

212

220

Number 2021

Number 2022

loading

ratun-

gene

11

811

56

208

74

9

53

49

inputs

in total

difficult-

loading

the

645

943

828

463

487

323

265

269

485

97

436

280

408

306

135

288

loading

ratun-

gene

2

200

63

151

80

5

15

22

inputs

in total

487

297

499

431

488

311

150

310

297

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

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

222

8th

108

153

97

302

80

63

71

18

51

22

12

0

13

2

18

0

60

3

107

193

143

100

35

4

76

31

13

2

7

0

1

0

5

7

4

0

53

15

329

201

251

253

132

306

156

94

84

20

58

22

13

0

18

9

22

0

113

18

4.226

2.123

6,348

3,738

1,334

5,072

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

census

Miscellaneous topics <

10 (e.g. chambers,

foreign affairs,

finance)

Subtotal

complaints and

consultations

298

Labor Statistics Privacy

40

10

2.016

8,404

6,384

1,754

6,836

4,644

14,788

11,480

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 Corona

regulations. Examples of such phone calls in November, as a month without

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 33 requests for information from citizens

processing of your data at the HBDI and 10 corresponding ones

consultations carried out.

299

– Regular consultations

With the internally appointed data protection officers from various

public areas (e.g. of ministries, cities and municipalities,

universities and the European data protection supervisory authorities)

exchanges were maintained and e.g. T. regular consulting services

rendered.

– Press and public relations

I had 90 press inquiries in 2022. Numerous publications

and assistance (e.g. on the subject of video conferencing technology).

Those responsible, citizens on my homepage

provided.

– training services

Seven trainee lawyers were elected in their elective or

Management stations trained.

– Training and lectures

Employees of my authority have 33, sometimes lasting several days, data

Intellectual property training, seminars and advanced training in public

and non-public areas. I myself have 15 public ones

Lectures held on a wide variety of data protection issues and 14

scientific papers published.

– 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 DSK meets every week

for a one-hour jour fixe via video conference. The results of

2022 are listed in Appendix I, but also in detail

the homepage of the data protection conference www.datenschutzkonferenz.

en to read.

Labor Statistics Privacy

In the working groups of the DSK my authority is in all areas

involved. Also in the sub-working groups and task forces that

cial topics are used, employees get involved

workers of the HBDI. In the working groups organization and structure as well as

Science and research, I chair the working group

credit bureaus and the co-chair of the research data task force. In

numerous EU bodies (e.g. International Transfers Expert Subgroup,

Border, Travel, Law Enforcement Expert Subgroup, Financial Matters

Expert Subgroup, CSC, SCG SIS II, SCG Eurodac, SCG VIS).

contribute to the HBDI. In addition, support

services to the EU Commission, e.g. B. by participating

and contributions within the framework of 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

2021

1

28

3

29

0

61

Number

2022

1

37

16

113

0

167

Number

2021

24

2

Number

2022

13

4

Other

In total

* Of which 3 ECJ preliminary ruling proceedings, 11 proceedings before the VGH in the 2nd instance,

3 proceedings before the Federal Constitutional Court, 1 summary proceedings.

18*

35

8th*

34

301

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

Reports of data protection violations according to Art. 33 DS-GVO and

§ 60 HDSIG

general overview

Ground

Number

2021

647

579

144

121

98

Number

2022

661

475

135

189

90

73

44

38

12

7

253

2.016

85

69

22

2

12

14

1,754

cases

2021

640

399

288

cases

2022

533

367

267

Incorrect dispatch/misallocation of data/documents

Hacker attacks, phishing, malware, vulnerability

Loss/theft of documents, devices etc.

Unlawful disclosure/sharing of data

Impermissible inspection (incorrect setup of access

rights etc.)

Open mailing list

Abuse of Access Rights

Prohibited Posting

Non-compliant disposal

Unencrypted e-mail transmission

Other

In total

areas most affected by data breaches

Credit industry, credit bureaus, trade and commerce

Employee data protection

health sector

302

Appendix to I

Appendix to I

1. Selected Resolutions of the Conference of Independents

Federal and state data protection supervisory authorities

Appendix to I

1.1

Parliamentary committees of inquiry and deletion moratoria:

Data protection through clear specifications and processing

restrictions for authorities from 03/23/2022

https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschluss-

sung_Loeschmoratorien.pdf

1.2

Scientific research - of course with data protection

from 03/23/2022

https://www.datenschutzkonferenz-online.de/media/en/DSK_6_Entschluss-

sung_zu_scientific_research_final.pdf

1.3

The time for an employee data protection law is "now"! from the

05/04/2022

https://www.datenschutzkonferenz-online.de/media/en/Entschluss_For-

derungen_zum_employee data protection.pdf

1.4

Petersberger declaration on data protection-compliant processing

of health data in scientific research

11/24/2022

https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Ent-

closure_Petersberger_Declaration.pdf

305

2. Selected decisions of the Conference of Independent

Federal and state data protection supervisory authorities

Appendix to I

2.1

To the task force Facebook fan pages of March 23, 2022

https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Fa-

cebook_Fanpages.pdf

2.2

Information from the DSK – data protection-compliant online trade using

Guest access from 03/24/2022

https://www.datenschutzkonferenz-online.de/media/dskb/20222604_be-

schluss_datenminimierung_onlinehandel.pdf

2.3

For the processing of personal data in connection with

the facility-related vaccination requirement of April 13, 2022

https://www.datenschutzkonferenz-online.de/media/dskb/2022_13_04_be-

schluss_DSK_20a_IfSG.pdf

2.4

Summary of the report on the DSK working group "Microsoft

Online Services" from November 25, 2022

https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_fest-

lege_MS365_summary.pdf

2.5

Specification for the working group DSK "Microsoft online services" dated

11/25/2022

https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_fest-

lege_MS365.pdf

307

The Hessian Commissioner for Data Protection and Freedom of Information

51. Activity report on data protection

2.6

Impact of new consumer regulations on digital

Products in the BGB on data protection law" from November 29th, 2022

https://www.datenschutzkonferenz-online.de/media/dskb/20221129_dskb_08_

Resolution_Consumer Regulations.pdf

2.7

Final report of the working group DSK "Microsoft online services"

from 07.12.2022

https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festle-

gung_MS365_final_report.pdf

308

3. Selected guidance from the Conference of

independent federal data protection supervisory authorities

and the countries

Appendix to I

3.1

Guidance from the supervisory authorities on processing

of personal data for direct marketing purposes

under the General Data Protection Regulation (GDPR) of

02/18/2022

https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Feb-

ruar%202022_final.pdf

3.2

FAQ on Facebook fan pages from 06/22/2022

https://www.datenschutzkonferenz-online.de/media/oh/20221121_oh_Fan-

pages_FAQ_Stand2022_11_21.pdf

3.3

Guidance from the supervisory authorities for providers of

Telemedia from December 1, 2021 Version 1.1 from December 5, 2022

https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Tele-

media_2021_version_1_1_template_104_DSK_final.pdf

3.4

Evaluation Consultation on guidance for providers of

Telemedia from 05.12.2022

https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Aus-

evaluation_consultation_for_orientation_aid_for_suppliers_of_teleme-

dien_final.pdf

309

II

Second part

5. Activity Report on Freedom of Information

5. Activity Report on Freedom of Information

The Hessian Commissioner for Data Protection and Freedom of Information

introduction

Introduction Freedom of Information

introduction

This fifth activity report on freedom of information describes

and analyzes the freedom of information in Hesse in the year 5 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. Information access is at

Public bodies excluded, insofar as he is responsible for the fulfillment of these tasks

jobs would hinder. The Hessian Commissioner for Data Protection

also holds the office of the Hessian Freedom of Information Officer

true. It is the supervisory authority for the implementation of freedom of information.

Citizens who are affected in their freedom of information

see, can turn to him with a complaint.

This regulation for the implementation of freedom of information is as follows

objective based. In a democracy, public administration may

no longer be a closed area, but their actions must be open and

make transparent. On the one hand, citizens should be able to

ability to change the actions of those you have chosen and will be back soon

Understand the election of the upcoming head of public administration and

to rate. On the other hand, they should be informed about the basic knowledge

and options for action by the administration can participate in this,

how the common good is substantiated by administrative action. You should

their experiences and ideas in the current public discussion

can contribute. Opposed by the right of access to information

public authorities give citizens the opportunity to

to gain direct insight into the processes of public administration.

This allows you to understand decisions made by the administration,

stand and accept more easily. Freedom of information thus has an important

democratic and constitutional function, strengthens civic

Participation and the control of state action.

313

The Hessian Commissioner for Data Protection and Freedom of Information

5. Activity Report on Freedom of Information

The Federal Republic of Germany and thirteen federal states have since

many years freedom of information laws restricting access to information

open to all public bodies. In some federal states, these

laws have since been developed into transparency laws that

public administration oblige themselves to provide as much information as possible

to make public. The current coalition agreement between SPD, Bündnis90/

The Greens and FDP also see a federal transparency law for the federal government

before (coalition agreement, p. 11).

Hesse was a latecomer in this development and only did five years ago

enact freedom of information regulations. It has its own rules for this

development concept that has only been adopted by Saxony and itself

from the regulatory concepts of all other freedom of information laws in

Germany differs. The right of general access to information

does not apply to all public bodies in Hesse, but only to the

state administration. The communities and districts that have the most civil

have contacts should each decide for themselves by statute,

whether they provide access to information about their files. Such information

So far, however, only a few districts, cities

and communities approved. Applies to most administrations in Hesse

therefore no freedom of information. Accordingly, the information
Freedom of freedom in administrative practice in Hesse, even to a lesser extent
Measures pronounced and must still develop in the future (see Chapter 2).
In the meantime, however, it has become apparent that the data on public authorities
available, not only of great importance for democracy and the rule of law
are, but also business and science benefit greatly from them
could pull. Therefore, all digitization strategies look to Union,
federal and state level to oblige public authorities to
to make suitable data publicly available. Accordingly sees
the coalition agreement for the federal government an open data regulation (coalition
contract, p. 17). In Hesse, the parliamentary groups of the CDU and
Bündnis 90/Die Grünen, after the draft for an open data law of the
FDP parliamentary group failed in the previous reporting year (see 4.
dir, chap. 5), on January 23, 2023 a draft law on open
Data from the public administration bodies in the legislative process
submitted (LT-Drs. 20/10379).
In the Union, the legislature has in Art. 3 et seq. of the Open Governance Act dated
May 30, 2022 (EU OJ L 152 of June 3, 2022, 1) Regulations on further
use of data held by public bodies.
In the draft for a Data Act of February 23, 2022, the European
Commission (COM(2022) 68 final) Rules for fair access to data

and a fair data use of this data proposed (see also
51. Activity report on data protection, chap. 1). The Commission aims to
to create a total of 13 public data rooms, and has to for the

the first European data room on health data on May 3, 2022

Draft regulation (COM(2022) 197/2).

In these developments towards open data, it is always also - even primarily

gig – about the free use of data from public authorities. As far as it goes

personal data, this always requires an agreement

with the requirements of data protection. As far as this succeeds

this development in the interest of the protection of fundamental rights, of participation

and development opportunities in business, science and civil

welcome social engagement. That fits into this development

restrained regulatory model of freedom of information in Hesse

hard in.

As Freedom of Information Officer, I had many interesting

te answer questions about freedom of information, supported citizens

and citizens in enforcing their claims, I participated in the

Discussion on the legal-political development of freedom of information

and worked with other freedom of information officers in Germany

in the Conference of Freedom of Information Officers (IFK). To

The fifth activity report offers a small selection of these fields of activity.

It presents the development of freedom of information in Hesse in the reporting year

dar (Chap. 1), examines the question of how freedom of information by design

Implementation of freedom of information through technology design can promote

(Chap. 2), asks why no information access to data from

Chambers of commerce is granted (chap. 3) and explains how with excessive

Freedom of information requests can be circumvented (Chapter 4).

1. Development of freedom of information

development of freedom of information

On the positive side, the country's public authorities are quite familiar with the domestic

information access to official information and records discontinued

have. A negative aspect is that the municipal area in particular

largely excluded from access to information. Especially in this one

There is a need for legislative, or at least municipal, action.

Freedom of Information Officer as “Complaints Office”

As a freedom of information officer, I deal in particular with

Submissions from citizens who object to their right to information

mation access violated.

In § 89 paragraph 1 sentence 1 HDSIG it is regulated that anyone who is in his information

freedom of information according to §§ 80 ff. HDSIG violated,

can “call” me as Freedom of Information Officer. From this right

the citizens made annually in the middle two-digit range

area use. Responds to requests for advice, mostly from authorities

are similar in numbers.

If I am called within the meaning of Section 89 Paragraph 1 Sentence 1 HDSIG, I will deal with it

me with the subject of the complaint. I come to the conclusion that

access to the information is wrongly denied, then according to § 89

Para. 3 S. 3 HDSIG request the public body to internalize this violation

to be fixed within a certain period of time. This request is legal though

not a (binding) administrative act within the meaning of § 35 HVwVfG, but a

Appeal to the body by the law according to § 89 Abs. 3 S. 4 HDSIG

planned notification of the supervisory authority of the public body

of course contains a certain emphasis.

By and large, information access requests become out of sight

of the freedom of information officer of the public authorities correctly

destined Violations of the provisions of Section 87 HDSIG are more common

statutory notice periods. In terms of content, they behave

public authorities but mostly correct.

The question of whether in the case

against a rejection by me as freedom of information officer

about the complainant, according to § 89 para. 3 sentence 3 HDSIG against the body

to take action, the complainant then took legal action against me

can proceed. On the other hand, the legislature in § 87 para. 5

HDSIG administrative court legal protection only against the body itself,

from whom information is requested, but not in Section 89

HDSIG to the Freedom of Information Officer.

Quite apart from that, however, a judicial

hen against the freedom of information officer the need for legal protection

are missing because, as I said, this is not the point anyway,

may oblige to provide information. This obligation can, however, precisely in the case

administrative court action against the public body itself

in the procedure according to § 87 para. 5 HDSIG in the case of the merits of the action

be obtained. This suggests that the judicial legal protection

the public body and the freedom of information officer

is excluded in this respect. Of course, the administrative court can

men of his process design regarding the lawsuit against a public

Hire me as Freedom of Information Officer.

Insufficient opening of information access

Persons who contact me as freedom of information officer about not

complained about the access to information granted, I often had to report that

the municipal area, unlike in the other federal states, from

Legislators are "privileged" at the expense of freedom of information. Only

if a municipality according to § 81 Section 1 No. 7 HDSIG in a municipal

Articles of Association stipulate that the fourth part of the HDSIG also applies to them

§§ 80 et seq. HDSIG also apply to them.

§ 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 legal situation comes up against the citizens who contact me

turn, since the beginning of freedom of information in Hesse in 2018

justifiably to great misunderstanding.

The statutory special treatment of the municipal sector would have changed

then, of course, for freedom of information – at least in practice – not

particularly detrimental when the municipalities are overwhelmingly

Articles of association that provide access to information within the meaning of Section 81

Para. 1 No. 7 HDSIG would have met.

Unfortunately, however, the opposite is the case: In Hesse there are 21 districts and only

four of them have introduced information access since 2018 (Marburg-Bie-

denkopf, Groß-Gerau, Darmstadt-Dieburg and the Main-Taunus-Kreis).

almost exactly only a fifth of the counties. In the larger cities it looks

no better for freedom of information: Only Wiesbaden, Kassel and

Darmstadt have freedom of information. After all, the state capital

access to information, unlike the other municipalities

limits the area of self-government, but also the authority to issue instructions and

Order matters included.

But not only the municipal area, but also the design

of freedom of information regarding the state area still offers

Reason for criticism: In particular the rigorous exclusions of the information

access regarding the police authorities (§ 81 Para. 2 No. 1 HDSIG) and the

Chambers of Commerce (§ 81 Para. 2 No. 3 HDSIG) should be mentioned here.

In my capacity as Hessian Freedom of Information Officer

I therefore make another appeal to the state parliament and the state government

Times, the Hessian freedom of information law as in most others

Federal states to check in particular in these points. Simultaneously

I appeal to the municipal sector, access to information, so far

did not happen to open by statute as long as the statute reservation

remain in force by law. The state capital Wies-

Baden, which has opened up unrestricted access to information.

2. Freedom of Information by Design

Freedom of information by design

In the area of freedom of information, the possible
Access to official information when carrying out digitization
planning projects to consider from the start. The contribution illuminates
what the so-called “freedom of information by design” is all about
and what opportunities and risks public authorities should consider.
In my last activity report, I explained why the
the provision and use of open data is to be promoted (4th activity report,
Cape. 5). In this connection I mentioned that the European
data strategy make the EU a role model for a digital society
should. The provision of open data is a so-called "obligation to deliver".
public sector when it comes to the provision of information
on goes through government agencies. That is the freedom of information as
so-called “obligation to collect” from the citizens. About this one
to facilitate the exercise of freedom of information rights and the trans-
the concept of promoting parency in public administration
of the so-called "freedom of information by design". The conference
the Freedom of Information Officer (IFK) in its 37th meeting on 12.
June 2019 created a position paper (https://datenschutz.hessen.de/
sites/datenschutz.hessen.de/files/2022-08/positionspapier_informations-
freedom_by_design.pdf). Similar to the basic idea of Art. 25 GDPR
(Data protection through technology design and through data protection-friendly
Defaults) should already have freedom of information requirements
right from the start by public authorities in the design of their IT systems
and organizational processes. According to the IFK
According to the definition, “freedom of information by design” includes the entirety
technical and organizational instruments, taking into account the

State of the art required for the exercise and fulfillment of rights

the freedom of information and access to information laws, environmental information

mation laws and transparency laws of the federal and state governments

serve. Some federal states have adopted the concept of “freedom of information by

Design” has already been included in their state regulations. This

has not been the case in Hesse so far.

My agency is currently working with other representatives

representatives of the IFK in the development of principles for the "information

freedom by design” with. These principles will be revised in due course

completion will be published. You set the focus on one hand

organizational measures, on the other hand on information-friendly

technical defaults.

Basically, the chances of "freedom of information by design" lie in

that the transparency of the public sector is further promoted. However

there are also often risks: On the one hand, checking the data quality is

difficult for citizens. Second is the data

not understandable without meta information. If you ask the interested

querying only columns of data available, with no other information

to provide their meaning, the data are not usable. This meta

information should also support “freedom of information by design” from the outset

to be considered. If the authority has an information advantage,

that is relevant to the interpretation or analysis of the data, it should

the applicant the necessary information on the

provide. In addition, the body responsible for information must be aware of this

be aware that technical means made available and prepared

provided data can often be linked and thus a personal reference restored

could be or other rights of third parties such. B. Trade Secrets

could be injured. This is especially important with large amounts of data

are taken into account, which are available via machine-readable interfaces (automatic

sible) can be made retrievable. Data protection and the rights of third parties

must not be undermined by freedom of information – even then

Not if “freedom of information by design” is guaranteed.

322

(No) information access to economic chambers

3. (No) access to information from economic chambers

(No) information access to economic chambers

The absolute exclusion of information access to the industrial

and chambers of commerce and chambers of crafts is not legally stringent.

The rules already existing in the Hessian freedom of information law

measures to protect personal rights and business secrets

and other rights are sufficient. The chambers for z. B. Lawyers,

Notaries and doctors get by with these regulations.

The current legal situation

The Hessian state legislature has, in contrast to others

Federal states decided that the chambers of industry and commerce and the

Chambers of crafts to be completely excluded from access to information.

This regulation can be found in § 81 Para. 2 No. 3 HDSIG.

§ 81 HDSIG

(2) The provisions of Part Four do not apply to

(...)

3. the chambers of industry and commerce and the chambers of crafts,

(...)

Evaluation

In the legislative process it was definitely seen (LT-Drucks. 19/5728,

p. 150 f.), that the freedom of information in Hesse anyway

existing protective regulations, for example in Section 82 Nos. 3 and 4 and Section 83 HDSIG

in favor of the protection of data protection and the protection of business

secrets of the chamber members are sufficient in themselves.

That might also be the reason that other chambers in the area

professional self-government (Bar Association, Chamber of Notaries

and also the medical association) access to information in accordance with the

§§ 80 ff. HDSIG are subject.

Since the Hessian freedom of information law came into force

Hessian Freedom of Information Officer accordingly as a result of

Freedom of information complaints according to § 89 HDSIG information access

Applications have become known from professional chambers in Hesse

had to be approved in accordance with §§ 80 ff. HDSIG.

323

The Hessian Commissioner for Data Protection and Freedom of Information

5. Activity Report on Freedom of Information

That the chambers of commerce are privileged in that they

access to information is absolutely impossible can be compared

to the other Chambers do not justify.

Therefore it is in the sense of an appropriate equal treatment of the

mers and, above all, adequate access to information

Chambers of Industry and Commerce and the Chambers of Crafts the others

Equal to chambers, where access to information is tailored

80 et seq. HDSIG has been opened from the outset. Also in the

most other federal states are subject to all professional associations

chambers for access to information.

Addressing this access to information, the Conference of Information

tion commissioners from the federal and state governments in 2015

Resolution drafted:

“Chambers are also obliged to transparency

Again and again professional chambers refuse the trans

parency requirements of the respective information access laws.

Professional chambers take on sovereign tasks

and country level true. There is one for each professional group

legal obligation to be a member, the chambers are responsible for

and often have far-reaching sanction options.

Information that arises in the course of their work falls under the

Federal and state information access laws. this is also valid

for annual financial statements and information on income, expenses and

Provisions of the chambers. For the obligation of the Chambers

It is irrelevant whether applicants are chamber members and which ones

motives that led to the application. Public Bodies

are in large areas not in competition with market

takers – Competitive disadvantages usually cannot arise.

Consequently, trade and business secrets worthy of protection

generally do not oppose access to information.

Claims for access to information must be made immediately, at the latest

but within the limits set forth in federal information access laws

or to meet the deadlines specified by the countries. A decision may

not postponed to committee meetings, but should be in the context

of the regular management. Incidentally are

information subject to transparency requirements from the professional chambers

to be published in the existing registers of information.

324

(No) information access to economic chambers

The freedom of information officers in Germany therefore call for the

professional chambers to meet their transparency obligations

to comply."

I therefore call on the state parliament and the state government to provide information

vis-à-vis the chambers of commerce in Hesse

open by law.

325

Excessive freedom of information requests

4. Excessive Freedom of Information Requests

Excessive freedom of information requests

Excessive freedom of information requests must be handled by public authorities

not disclosed in accordance with the Hessian freedom of information law

become. This is also appropriate because even in data protection law

those affected (after all by data processing) have no claim

have access to information in the event of excessive requests for information.

An example

At the beginning of 2022, the Darmstadt regional council informed me about

the following freedom of information request that he had received, and

asked for advice. The request was worded as follows:

“A request is made to allow me access to information on the following

grant questions:

1. How many external service providers does your authority have in 2019

and commissioned in 2020?

2. Which specific external service providers have been commissioned?

3. For which specific tasks/consultation/services

were the external parties commissioned?

4. Which respective costs (total in gross, net and sales tax

he) are for the respective externals for which respective task/

Advice/service created?

5. What was the content of the respective contracts of the respective ex-

to the respective tasks/consulting/service?”

The Darmstadt Regional Council was of the opinion that the disclosure

this application is associated with a disproportionate effort, and

it therefore intended to reject this request for access to information

modest. I did not raise any objections to this, because the Hessian

Freedom of information sees in § 85 HDSIG for such constellations

refusal to proceed by the public authority.

§ 85 HDSIG

"(2) (...) An application that is aimed at general official action and relates to domestic

information relates to a large number of file processes or information carriers

need to be collected, may be refused if access to information

would only be possible with disproportionate administrative effort."

This provision in the Hessian freedom of information law makes perfect sense.

Because even in data protection law, which after all is about the processing

Para. 5 DS-GVO excessive requests for information are not met.

Art. 12 GDPR

(5) (...) In the case of ... excessive requests from a data subject, the controller may ...

refuse to act on the application.

So if even in data protection law, when it comes to the processing of personal

son-related data of those affected, the responsible bodies

Excessive requests - despite the associated processing of the data -

the fundamental rights affected - do not have to comply, then it is only

quite appropriate to also provide for this in the right to information, because

there the freedom of information requests are basically “unconditional”,

i.e. without being legally affected, are permissible and according to § 87 HDSIG

In accordance with Sections 80 et seq. HDSIG.

Excessive freedom of information requests and municipal

Statutory autonomy

Subsequent to the process at the Darmstadt Regional Council

As a result of many municipal (advice) requests, it turned out that

the applicant, at least in Hesse, also submits his application across the board

had sent to other Hessian municipalities. Since most municipalities

in Hesse no freedom of information statutes within the meaning of Section 81 (1) No. 7

HDSIG have issued, they are not even to the decree of the

Applicant obligated (was) since the obligatory to the decision

Regulation of § 87 HDSIG for these municipalities without statutes also not

is applicable. Nevertheless, I have suggested to the municipalities that the applicant

to the non-applicability of the right to information in municipalities without

refer to the statute.

That excessive requests for information access in the municipal area

for the municipal motivation to enact freedom of information statutes,

are not conducive is evident and for my opposite concern

counterproductive, for a spread of freedom of information to local

ler level to plead. In this context, however, I can at least

mention positively that now the state capital Wiesbaden

issued a freedom of information statute.

328

Labor Statistics Freedom of Information

5. Labor Statistics Freedom of Information

Labor Statistics Freedom of Information

Compared to the previous year, there was a decrease in complaints and a

increase in consultations.

IFG

complaints

consultations

2021

71

52

2022

46

64

329

ANNEX to II

Appendix to II

1. Selected Resolutions of the 42nd and 43rd Conference of the

Freedom of Information Officer in Germany

Appendix to II

1.1

No circumvention of freedom of information by establishment

of foundations under civil law! from 06/30/2022

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/42_Kon-

ferenz_Foundations-civil-law.html?nn=253070

1.2

SMS to file: Regulatory communications subject

comprehensively the rules of freedom of information! from 06/30/2022

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/42_Kon-

ferenz_SMS-in-die-Akte.html?nn=253070

1.3

Lower Saxony: The time for a transparency law has come

from 26.10.2022

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/42_43_

Resolution%C3%9Fung Transparency Act.html?nn=253070

333

List of Abbreviations

List of Abbreviations

The Hessian Commissioner for Data Protection and Freedom of Information

51st activity report on data protection / 5th activity report on freedom of information

List of Abbreviations

Section.

AES

AGG

AIA

apartment

oh

apartment

ArbR

kind

ATD

ATDG

edition

GCU

BaFin

BAG

BCR

Unit volume

Advanced Encryption Standard

general equality law

Artificial Intelligence Act

mobile application

tax code

mobile applications

work and law

Article

anti-terrorist file

Anti-Terrorism File Act

edition

Order Processing Agreement

Federal Financial Supervisory Authority

Federal Labor Court

Binding Corporate Rules (binding internal

data protection regulations)

Federal Data Protection Act

Federal Commissioner for Data Protection and Information

onfreedom

Civil Code

Federal Law Gazette

Federal Court of Justice

Federal Criminal Police Office

Federal Registration Act

Federal Ministry of the Interior and Homeland

Federal Office for Security in Information Technology

For example

Borders, Travel & Law Enforcement (Subgroup)

Letter

BDSG

BfDI

Civil Code

Federal Law Gazette

BGH

BKA

BMG

BMI

BSI

E.g.

BTLE

letter

335

The Hessian Commissioner for Data Protection and Freedom of Information

51st activity report on data protection / 5th activity report on freedom of information

Federal Administrative Court

Federal Constitutional Court

Collection of decisions of the Federal Constitutional

court

respectively

Approximately

Coronavirus disease 2019

Coronavirus SARS-CoV-2

Computer-aided transaction processing -Pre-

police procession system

Criminal Research Investigation Management Software

ware of the police

Data Act

Data Government Act

That means

Digital Market Act

Digital Services Act

General Data Protection Regulation

Conference of the independent data protection supervisory

federal and state authorities; short: data

protection conference

Data protection regulations of the Hessian state parliament

European Data Protection Board

electronic mail

recital

et cetera

European Union

Court of Justice of the European Union

Registration office

the following

following (pages) / subsequent

Federal IT cooperation

BVerwG

BVerfG

BVerfGE

or.

approx.

COVID-19

COVID-19

ComVor

crime

THERE

DGA

i.e. H.

DMA

THE

GDPR, GDPR

DSK

DSO

EDSA

e-mail

recital

Etc.

EU

ECJ

EWO

f.

onwards

FITKO

336

DeadlinesVO

acc.

GG

possibly.

GVBl.

GWG

HAKrWG

HBDI

HDSIG

Hesse3C

HGB

HKHG

HKRG

HLKA

HMinD

HMSI

HMWK

HSOG

HSOG-E

HVSG

HSL

HVwVfG

HZD

IBAN

I.D.M

i. i.e. R

List of Abbreviations

Ordinance laying down the rules for the deadline

th, dates and deadlines

according to

constitution

in which case

Law and Ordinance Gazette

Money Laundering Act

Hessian implementation law for the circular economy

corporate law

Hessian Commissioner for Data Protection and Information

mation freedom

Hessian Data Protection and Freedom of Information

law

Hessen Cyber Competence Center

commercial code

Hessian hospital law

Hessian Cancer Registry Act

Hessian State Criminal Police Office

Hessian Minister for Digital Strategy and Development

winding

Hessian Ministry for Social Affairs and Integration

Hessian Ministry for Science and Art

Hessian law on public safety

and order

Hessian law on public safety

and order - draft

Hessian Constitutional Protection Act

Hessian State Statistical Office

Hessian Administrative Procedures Act

Hessian headquarters for data processing

International bank account number

identity management

usually

IFK

IfSG

INA

IMI

i. s.d.

i. S.e.

i. V. m.

IP

IT

IT

IT service

IT laboratory

IT system

Cape.

vehicle

KrWG

lit.

LfV Hesse

LT Drs.

NJW

NZA

NZV

No.

or similar

OLG

OVG

OWASP

OWiG

PDF

pen test

POLAS

338

Freedom of Information Conference

German Infection Protection Act

internal committee

Internal Market Information System

market information system)

in terms of

in the sense of a

combined with

Internet Protocol

information technology

information technology

Information technology service

Information technology laboratory

information technology system

Chapter

motor vehicle

Circular Economy Act

Litera, letter

State Office for the Protection of the Constitution in Hesse

State Parliament printed matter (Hesse)

New Legal Weekly

New Labor Law Journal

New journal for traffic law

number

or similar

Higher Regional Court

Higher Administrative Court

Open Web Application Security Projects

Administrative Offenses Act

Portable document format

penetration test

police information system

PsychKHG

QR code

No./Rn.

Rs.

S

s.

s.a.

SCG

SIS II

SIS II Decision

S/MIME

so-called.

SPH

StbergG

StGB

StPO

see below

TB

TKG

TKÜ

TKÜ

TLS

TOM

TTDSG

etc.

Subpar.

List of Abbreviations

Hessian law on help with mental illness

Diseases

Quick response code

marginal number

case

page or sentence

please refer

see also

Supervision Coordination Group (SIS II SCG; the

Group consists of representatives of the national supervisory

supervisory authorities of the Member States and the EU

European data protection officer)

Schengen Information System II

Council Decision 2007/533/JHA of 12 June

2007 on the establishment, operation and the

Use of the Schengen Information System

second generation

Secure/Multipurpose Internet Mail Extensions

so-called/so-called/so-called

School portal Hesse

Tax Advisory Act

criminal code

Code of Criminal Procedure

see below

activity report

Telecommunications Act

telecommunications

Telecom Surveillance

Transport Layer Security

Technical and organizational measures

Telecommunications Telemedia Data Protection Act

among other things

subparagraph

339

Schleswig-Holstein

Uniform resource locator

Verdict

United States of America

Unfair Competition Law

administrative court

compare

video conferencing system

Virtual Private Network

Administrative Procedures Act

working paper

Article 29 Data Protection Working Party

world wide web

for example

Center for Digital Sovereignty in Public

Administration

census law

Central traffic information system

ULD SH

URL

Urt.

UNITED STATES)

UWG

VG

see.

VKS

VPN

VwVfG

WP

WP

www

e.g. B.

ZenDiS

censusG

ZEVIS

340

Register of Legislation

Register of Legislation

Register of Legislation

The versions valid at the time of processing are quoted.

Law/Regulation Reference(s)

oh

AGG

ATDG

BDSG

BDSG

BDSG

BDSG

BDSG

BDSG a. f

Civil Code

Civil Code

Civil Code

Fiscal Code in the version published on October 1

2002 (Federal Law Gazette I p. 3866; 2003 I p. 61), last amended by Arti-

Section 1 of the law of July 12, 2022 (Federal Law Gazette I p. 1142)

General Equal Treatment Act of August 14, 2006 (Federal Law Gazette I

p. 1897), last amended by Article 4 of the law of 19 December

December 2022 (BGBl. I p. 2510)

Law establishing a standardized central anti-terrorist database

federal and state police and intelligence services

(Anti-Terrorism File Act ATDG)

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

changed by Art. 12 Second Data Protection Adaptation and Implementation

11/20/2019 (Federal Law Gazette I p. 1626)

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

changed by Art. 12 Second Data Protection Adaptation and Implementation

11/20/2019 (BGBl. I p. 1626)

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

amended 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)

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,

calculated 2022 I p. 1045)

Federal Data Protection Act old version in the version of the notice

from 14.01.2003 (Federal Law Gazette I p. 66), last amended by law from

30.10.2017 (Federal Law Gazette I p. 3618) m.W.v. 11/09/2017. expired

on May 25th, 2018 due to the law of June 30th, 2017 (Federal Law Gazette I p. 2097)

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)

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. 9 of the law of November 7th, 2022 (Federal Law Gazette I. S. 1982)

Federal Hunting Act of September 29, 1976 (Federal Law Gazette I p. 2849), last amended

by Article 291 of the Ordinance of June 19, 2020 (Federal Law Gazette I p. 1328)

Federal Criminal Police Office Act of June 1, 2017 (Federal Law Gazette I p. 1354; 2019

I p. 400), last amended by Article 3 of the law of 19 December

December 2022 (BGBl. I p. 2632)

Federal Registration Act of May 3, 2013 (BGBl. I p. 1084), last amended

changed by Article 4 of the law of July 21, 2022 (Federal Law Gazette I p. 1182)

Federal Registration Act of 03.05.2013 (Federal Law Gazette I p. 1084), last amended

22 of the law of December 19, 2022 (Federal Law Gazette I p. 2606)

Law on Nature Conservation and Landscape Management (Federal Nature Conservation

law) of June 29, 2009 (Federal Law Gazette I p. 2542), last amended by

Article 3 of the law of 8/12/2022

Professional Code for Lawyers, last amended by resolution

from 06.05.2019

Federal Forest Act of May 2nd, 1975 (Federal Law Gazette I p. 1037), last amended

by Article 112 of the law of August 10, 2021 (Federal Law Gazette I p. 3436)

Data protection regulations of the Hessian state parliament, Annex 4 to the

Rules of Procedure of the Hessian State Parliament of December 16, 1993 (GVBl.

I p. 628), last amended by resolution of the state parliament of

February 23, 2022 (GVBl. p. 130)

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

tes of April 27, 2016 for the protection of natural persons in the processing

processing of personal data, the free movement of data and

Repeal of Directive 95/46/EC (General Data Protection Regulation)

(OJ EU L 119 p. 1)

Basic law of May 23, 1949, last amended by Art. 1 Amendment Act

(Article 82) of December 19, 2022 (Federal Law Gazette I p. 2478)

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

by Article 23 of the law of February 22, 2023 (Federal Law Gazette 2023 I No. 51)

Hessian implementing law for the circular economy law

of March 6, 2013, last amended by Article 15 of the Law

from May 3, 2018 (GVBl. p. 82)

Commercial Code Law of May 10, 1897 (RGBl. I p. 219), last

changed by law from July 15th, 2022 (Federal Law Gazette I p. 1146) m. W. v.

01.08.2022

Hessian Municipal Code in the version of the announcement

of March 7, 2005, modified by art. 3 of the law of December 11

December 2020 (GVBl. p. 915)

BJagdG

FCAG

BMG

BMG

BNatSchG

BORA

BForestG

DSO

GDPR

GG

GWG

HAKrWG

HGB

HGO

342

HDSIG

HDSIG

HDSIG

HKHG

HKRG

HSchG

HSOG

HVSG

HVSG

HVwVfG

HWaldG

IfSG

KrWG

Register of Legislation

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 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)

Second law for the further development of the hospital system in

Hesse (Hessian Hospital Act 2011 – HKHG 2011) from

21.12.2010, last modified by article 6 of the law of 9.

December 2022 (GVBl. p. 752, 757)

Hessian Cancer Registry Act of October 15, 2014 (GVBl. p. 241)

FFN 351-91, last amended by Art. 8 G to strengthen health

9.12.2022 (GVBl. p. 764)

Hessian school law from 06/30/2017, last changed by

Law of December 7th, 2022 (GVBl. p. 734)

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)

Hessian Constitutional Protection Act of June 25, 2018, promulgated

as Article 1 of the law on the reorientation of the protection of the constitution

zes in Hesse on June 25, 2018 (GVBl. p. 302)

Hessian Constitutional Protection Act (HVSG) to footnote [1] dated

June 25, 2018 (GVBl. p. 302) FFN 18-7

Hessian Administrative Procedures Act (HVwVfG) in the version

of January 15, 2010, last amended by Article 2 of the Law

from September 12, 2018 (GVBl. p. 570)

Hessian Forest Law Hessian Forest Law (HWaldG) from

06/27/2013, last amended by law of 06/19/2019

Law on the Prevention and Control of Infectious Diseases

in humans of July 20, 2000 (Federal Law Gazette I p. 1045), last amended

by Art. 8b Hospital Care Relief Act of December 20, 2022 (Federal Law Gazette

I p. 2793)

Circular Economy Act of February 24, 2012 (Federal Law Gazette I p. 212),

last modified by article 20 of the law of August 10, 2021

(BGBl. I p. 3436)

Aviation Security Act of 11 January 2005 (Federal Law Gazette I p. 78), most recently

amended by Article 1 of the law of April 22, 2020 (Federal Law Gazette I

p. 840)

Law on administrative offenses in the version of the notification

19.02.1987 (Federal Law Gazette I p. 602), last amended by Article

31 of the law of October 5th, 2021 (Federal Law Gazette I p. 4607, 4617)

Hessian law on help for mental illnesses (Psychiatric

Swiss-Krankenhilfe-Gesetz - PsychKHG) from 4.05.2017, last

amended by Article 4 of the law of December 9, 2022 (GVBl.

pp. 764, 765)

Broadcasting contribution state treaty from 15.-21. December 2010, last
amended by the State Media Treaty from April 14 to 28, 2020, in
came into force on November 7th, 2020, Hess. GVBl. 2020 p. 607 ff.
Directive (EU) 2016/680 of the European Parliament and of the Council
of April 27, 2016 on the protection of natural persons in the processing
processing of personal data by the competent authorities
Prevention, investigation, detection or prosecution purposes
criminal offenses or the execution of sentences and the free movement of data
and repealing Council Framework Decision 2008/977/JHA
The second book of the social code - basic security for work
relevant (Article 1 of the law of December 24, 2003 (Federal Law Gazette I p. 2954), in
Came into effect on January 1, 2004 and January 1, 2005, last amended by
Law of December 16, 2022 (Federal Law Gazette I p. 2328) with W. v. 01/01/2023
Social Code (SGB) Fifth Book (V) - Statutory Health Insurance
security - from 20.12.1988 (Federal Law Gazette I p. 2477), last changed by
Art. 1, 1a, Art. 1b Hospital Care Relief Act of December 20th, 2022
(BGBl. I p. 2793)
The Tenth Book of the Social Code - Social Administration Procedures
and social data protection in the version of the announcement of 18.
January 2001 (Federal Law Gazette I p. 130), last amended by Article 19 of the
Law of July 20, 2022 (Federal Law Gazette I p. 1237)
The Twelfth Book of the Social Code - Social Assistance - (Article 1 of the
of December 27, 2003, Federal Law Gazette I p. 3022, 3023), last amended
changed by Article 5 of the law of December 16, 2022 (Federal Law Gazette I
p. 2328) m. W. v. 01/01/2023
Council Decision 2007/533/JHA of 12 June 2007 establishing

management, operation and use of the Schengen information system

tems of the second generation (SIS II)

Tax Advice Act in the version of the notice of 4.

November 1975 (Federal Law Gazette I p. 2735), last amended by Article 34

of the law of December 16, 2022 (Federal Law Gazette I p. 2294)

AirSiG

OWiG

PsychKHG

RBStV

Directive (EU)

2016/680

SGB II

SGB V

SGB X

SGB XII

SIS II

StbergG

344

StGB

StPO

StPO

StPO

StPO

StVG

TestV

TTDSG

UWG

UWG

VwVfG

Register of Legislation

Criminal Code in the version published on November 13

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

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

Code of Criminal Procedure, in the version published on 7

April 1987, last amended by Art. 2 G to implement the VO

(EU) 2019/1148 of the European Parliament and of the Council of

20.6.2019

Code of Criminal Procedure in the version published on April 7th

1987 (Federal Law Gazette I p. 1074, 1319), last amended by Article 2 of the

Law of March 25, 2022 (BGBl. I p. 571)

Code of Criminal Procedure, in the version published on 7

April 1987, last amended by Art. 2 G on the determination of

Economic plan of the ERP special fund for the year 2022, for

electronic collection of the bank levy and amending the Code of Criminal Procedure

from March 25, 2022 (Federal Law Gazette I p. 571)

Code of Criminal Procedure in the version published by

07.04.1987 (Federal Law Gazette I p. 1074, 1319, last amended by Art. 2 of the

Law of March 25, 2022 (BGBl. I p. 571, 587)

Road Traffic Act of March 5, 2003, last amended by Art.

2 para. 32 G to modernize the promulgation and announcement

of 20.12.2022 (Federal Law Gazette I p. 2752)

Regulation on the right to testing in relation to a direct

Detection of the pathogen of the coronavirus SARS-CoV-2 (coronavirus test

Ordinance - TestV) from September 21, 2021, (BAnz AT September 21, 2021 V1)

FNA 860-5-77, last amended by Art. 1 Sixth Amendment of

January 11, 2023 (Federal Law Gazette I No. 13)

Telecommunications Telemedia Data Protection Act of 23 June

2021 (Federal Law Gazette I p. 1982), last amended by Article 4 of the law

of August 12, 2021 (Federal Law Gazette I p. 3544)

Law against unfair competition in the version of the

Announcement of March 3, 2010 (Federal Law Gazette I p. 254), last amended

by Article 20 of the law of June 24, 2022 (Federal Law Gazette I p. 959)

Law against unfair competition, law of 07/03/2004

(Federal Law Gazette I p. 1414), last amended by law from 06/24/2022

(BGBI. I p. 959) m.W.v. 01.08.2022

Administrative Procedures Act in the version published

from 23.01.2003 (Federal Law Gazette I p. 102), last amended by law from

25.06.2021 (Federal Law Gazette I p. 2154) w. 01.08.2021

CensusG 2022

Law on the implementation of the 2022 census in 2022 dated

26.11.2019 (Federal Law Gazette 1 p. 1851), amended by Art. 2 of the law

from 03.12.2020 (Federal Law Gazette I p. 2675)

subject index

factual terms

A

remedial actions

warning letter

clearing house

consideration

Active sourcing

address dealer

administrative assistance

adequacy decision

Unsolicited examination

anonymization

workers

working group

scope of work

Artificial Intelligence Act

doctor's office

assistance systems

retention obligation

supervisory activity

processor

order processing

recording

Provision of information

I 12.7; I 19.1

I 13.1

I 5.1

I 12.3

I 11.3

I 5.2

I 7.2

I 2

I 17.4

I 16.4

I 11.2

I 1;

I 9

I 1

I 15.4; I 15.6

I 12.6

I 12.7

I 1

I 2; I 14.1; I 17.2; I 17.3

I 3.1.; I 9; I 14.1

I 11.2

I 14.3

information

-duty

Appendix to 1 item 2

I 1; I 2; I 5.2; I 8.2; I 11.1; I 11.2; I

15.2; I 17.3

I 5.1; I 11.1; I 11.2; I 18

Employee data protection

I 11.2

Employment Type

I 7.5; I 9; I 11.2; I 13.1; I 15.3; I 19.2

Complaint

I 7.6; II 1st

Complaints Office

I 12.3; I 12.4

data subject rights

I 6.2; I 11.3

applicant

image capture

I 6.6

Internal Market Information System I 4.1

I 7.4

biometric data

I 14.3

credit check

Federal Constitutional Court

I 5.1; I 6.1; I 7.1

348

Fine-

–

–

-metering

-procedure

C

CAST forum

cloud

cookies

ComVor

Corona-

-pandemic

–

-Vaccination certificate

–

–

-Test center

cybercrime

subject index

I 5.2

I 5.2

I 5.1

I 18

I 2; I 8.1; I 11.2; I 14.1; I 15.4

I 12.2; I 12.8

I 6.1

I 1; I 3.1; I 3.4; I 17.2

I 15.5

I 5.2

I 17.2

D

dark web

dash cam

Data Act

data, biometric

DataTuesday

Data Governance Act

data breach

data protection supervision

Data protection information/

-notes/concept

Privacy check, technical

data breaches

data transfer

I 17.1; I 17.3

I 11.2

I 1

I 7.4

I 18

I 1

I 9; I 15.3; I 17.2; I 19.2

I 3.1

I 7.5; I 12.8; I 15.1

I 17.1

I 17. 2; I 17.3

I 15.3; I 17.4

349

The Hessian Commissioner for Data Protection and Freedom of Information

51st activity report on data protection / 5th activity report on freedom of information

data security

data transfers

data processing

cross border

– Security of

–

dialog

service provider

Digital Market Act

Digital Services Act

digital processes

Digital sovereignty

digitalization

digitization officer

digitization project

digitization strategies

direct mail

document collection box

third country

toleration

enforcement

E

EDSA

E-mail-

–

–

–

- Advertising

-Addresses

-Accounts

-News

350

I 2; I 17.6

I 2; I 18; I 19.2

I 3.2; I 11.2; I 4.1; I 5.1; I 6.3; I 7.2; I

7.3; I 7.4; I 9; I 11.1

I 17.6

I 4.1

I 16.3

I 15.3; I 15.4.; I 15.5; I 17.2

I 1

I 1

I 7.5

I 2; I 3.2; I 7.1

I 1; I 2; I 7.1; I 9

I 7.6

I 1; I 2; I 3.3, I 11.1

I 4; I 16.1; I 16.3; I 18

f

Facebook

fan pages

wrong shipment

fingerprint

research data

research project

photography

G

Birthday Congratulations

fine

Danger

municipal council

Court

health data

GPS tracking

Go Kart

I 2; I 4.2; I 12.2; Attachment to I No. 2.1;

Appendix to I No. 3

I 12.2; Appendix to I Zif. 2.1

I 15.3; I 17.2; I 19.2

I 7.4

I 15.1; I 16.1

I 15.1; I 16.1 I 16.2

I 7.5

I 12.5

I 5.3; I 17.2; I 19.1

I 5.3

I 7.2

I 4; I 5

I 15.1

I 5.1

I 14.4

351

The Hessian Commissioner for Data Protection and Freedom of Information

51st activity report on data protection / 5th activity report on freedom of information

Google

Google Fonts

protection of fundamental rights

I 12.1; I 14.5

I 12.1

II

H

hacker attacks

handout

house facade

HessenConnect 2.0

HessenDATA

Hessian Cancer Registry Act

(HKRG)

Hessian law on the public

public safety and order

(HSOG)

colleges

I

identity management

identification data

IMI system

vaccination card

vaccination dates

compulsory vaccination

Chamber of Commerce and Industry

information

information access

Freedom of Information

352

I 17.2

I 7.2

I 14.5

I 3.4

I 6.1

I 15.1

I 6.2

I 3.1; I 3.3; I 8

I 3.3.

I 7.5

I 6.2; I 6.4

I 14.5; I 17.1

I 7.6

I 17.1

J

Job centre

legal department

I 13.2

I 5

K

Mark

Children

legal action

coherence method

municipalities

municipal bodies

cooperation

consultation

corruption

license plate number

Hessian hospital law

(HKHG)

I 6.2; I 7.2; I 14.2

4.2

I 5 1

I 4.1; 4.2

employees

- excess

– Monitoring of

Mobile working

sample documents

N

tracking

Newsletter

contingency plans

354

I 15.1

I 14.2

I 2

I 14.2

I 6.3

I 10

I 8.1; I 8.2

I 5.3

I 12.7; I 13.1

I 8.3

I 9

I 7.2

I 15.1

I 5.2; i 7.2

I 1

I 9

I 12.3

I 17.3

user profiles

O

public relation

disclosure

Office program

One shop stop

Online Access Act (OZG)

organization

administrative offences

P

panoramic images

patient

-data

–

–

-file

identity card

personnel service provider

Petersberg declaration

phishing

platform

police

exam tools

pseudonymization

The Hessian Commissioner for Data Protection and Freedom of Information

51st activity report on data protection / 5th activity report on freedom of information

Lawyer

rules review

restaurant

ring memory

risk assessment

role concept

S

sanctions

Statutory autonomy

Schrems II judgment

School

school portal

Self-developed software

security

–

-level

–

-authorities

Social networks

memory limitation

Lock files list

language assistance systems

Public prosecutor

statistics

tax consultant

offenses

software license

subgroup

356

I 7.2

I 6.2

I 12.7; I 13.1

I 11.2

I 17.2; I 17.3

I 8.3

I 5.2

II 4

I 3.3; I 12.1

I 3.2; I 8

I 3.2; I 8.1; I 8.2

I 17.5

I 7.5

I 2

I 11.2

I 12.4; I 12.7

I 12.6

I 6.5

I 19.1

I 14.1

I 6.2

I 14.1

I 4.1

subject index

T

Technological sovereignty

telecommunications

telecommunications service

–

telecommunications tele

media data protection law

(TTDSG)

I 2

I 3.1

I 3.1

I 3.1

telemetry

test center

animal surveillance cameras

tracking

Trans-Atlantic Data Privacy

Framework

transparency

u

surveillance measures

action for failure to act

V

Responsible

Responsibility

defense of Constitution

landlord data

gatherings

encryption

administrative services

warning

I 8.1

I 15.3

I 13.1

I 2; I 5.1

I 2

I 4.2; I 11.3; I 12.2; I 14.5; I 16.1

I 2

I 5.1

I 2; I 3.4; I 12.2; I 13.2; I 17.3; I 17.6

I 2

I 6.3; I 6.4

I 13.3

I 6.6

I 3.3; I 9; I 15.3

I 7.1

I 19.1

51st activity report on data protection / 5th activity report on freedom of information

video surveillance

video conferencing systems

VKS systems

I 6.2; I 13.1

I 2; I 3; I 3.1; I 3.2; I 3.3; I 3.4

I 3.2

W

Advertising

recycling center

WI box

contradiction

Wiesbaden Data Protection Forum

trail cameras

Z

census

accesses

Cooperation

earmarking

I 12.1; I 12.3; I 12.5

I 7.2

I 7.4

I 12.4

I 18

I 13.1

I 9; I 17.2

I 15.3

I 1; I 4.1; I 9; I 17.3

I 12.2; I 12.4; I 16.1