annual report

the Berlin Commissioner for Data Protection and

Freedom of Information as of December 31, 2021

The Berlin Commissioner for Data Protection and Freedom of Information has dem

House of Representatives and the Senate annually report on the result

their activity (§§ 12 Berlin Data Protection Act, 18 Para. 4 Berliner

Freedom of Information Act). This report closes on April 8th

Annual Report 2020 submitted in 2021 and covers the period between

January 1st and December 31st, 2021 onwards.

The annual report is also available on our website, see:

www.datenschutz-berlin.de

imprint

Publisher:

Berlin Commissioner for Data Protection

and freedom of information

Friedrichstr. 219

10969 Berlin

Phone: 030 138 89 – 0

Fax: 030 215 50 50

Email: mailbox@datenschutz-berlin.de

Internet: www.datenschutz-berlin.de

Layout:

april agency GbR

Sentence:

Print:

LayoutManufaktur.de

ARNOLD group

Contents

List of abbreviations 8th

foreword 13

1 focus areas

1.1 International data traffic one year after "Schrems II" 16

1.2 Digitization of schools — continued 22

1.2.1 Legal basis for school digitization 24

1.2.2 School Data Ordinance and “Digital Learning Materials Ordinance”. 26

1.2.3 "Berlin learning space" - What has happened?. 27

1.2.4 Teachers-Teaching-School Database 28

1.3 Corona vaccination management of the State of Berlin. 30

1.3.1 Online appointment booking with private companies 30

1.3.2 The issue of earmarking 32

1.4 Data processing by corona test centers. 34

1.5 Attendance documentation and contact tracing 38

2 Digital Management

2.1 Status of digitization projects. 43

2.2 Use of video conferencing systems. 45

2.3 Implementation of the online access law in the federal and state governments. 46

3

Home and Sports

3.1 Police unlawfully transmit meeting data. 50

3.2 Rights to information from the police possible without a copy of ID. . . . 55

3.3 How anonymous are the police information portals? 56

3.4 Disclosure of a complainant's data to the

Complaint affected employees. 57

3.5 Lack of identification of the applicant at the

Online application for simple registration information. 58

3.6 Data processing during parliamentary elections 61

3.7 Posting Photos and Other Data on the Website

from sports clubs. 65

3

Contents

4 Judiciary and Legal Profession

4.1 Radio cell query transparency system finally in use. 68

4.2 Right to information from the examination file in legal training. . . 69

4.3 Implementation of the JI Directive in prisons. 70

4.4 Bailiffs: The "speaking" reference. 73

4.5 Restriction of the right to information from the

legal profession 74

5 Youth, Education, Science and Research

5.1 Implementation regulations for youth welfare - data protection from

thought through from the start. 77

5.2 Unencrypted dispatch of copies of certificates 79

5.3 Corona self-tests in schools 80

5.4 Digital blackmail: what to do about ransomware. 82

6 health and care

6.1 Contact tracing in health authorities. 85

6.2 Digital vaccination certificates: prevent counterfeiting, check securely 87

6.3 Maximum periods are not mandatory storage obligations. 89

6.4 Deleting an entry about an unconfirmed

child endangerment 91

6.5 Appointment management in doctor's practices - what should be considered?. 92

6.6 With a click to the appointment — appointment booking portals and how to use them

with the data of the patients. 94

6.7 Easily looted patient records. 95

7

integration, social affairs and work

7.1 Complaints office for refugees 99

7.2 Accommodation for the homeless "at the push of a button". 100

8 Employee data protection

8.1 A list of information about all employees on probation. . . 102

8.2 Must legal trainees submit their application to the Superior Court of Justice

state of health? 104

8.3 Free access to applicant data. 105

9 Housing, urban development, services of general interest and the environment

9.1 Online broker publishes tenant data on the Internet. 108

9.2 Data processing by smoke detectors? 109

9.3 Misappropriation Prohibition Act 110

9.4 Consequences of the bursting of the rent cap under data protection law. 112

9.5 Radio-based heating cost meters 113

9.6 Dispute among allotment gardeners — Does the GDPR apply? 114

9.7 Publication of membership lists in the association for assertion

of minority rights. 115

10 economy

10.1 "Responsible data processing" by banks 118

10.2 Transparency in Scoring Procedures 120

10.3 Consent to advertising during telephone calls. 121

10.4 Unsolicited advertising after alleged participation in a

Sweepstakes — proof of declaration of consent 123

10.5 Applicability of the GDPR in favor of legal entities? . . . 124

10.6 The – limited – powers of group data protection

commissioned 125

11 Transport, Tourism and Credit Bureaus

11.1 "Jelbi" - the mobility app of the BVG - an interim conclusion 128

11.2 Check-In/Check-Out via smartphone in public transport. 129

11.3 Processing of utility contract data

credit bureaus 131

12 video surveillance

12.1 Bodycams at Deutsche Bahn 133

12.2 Information rights in the case of video surveillance. 135

13 sanctions

13.1 Corona cases 138

13.2 Fines for Unauthorized Use of the Police Database

POLICIES 138

13.3 Unauthorized database queries by job center employees. 140

13.4 Order and fines due to illegal video surveillance. . 140

13.5 Data protection is a management issue, but not like this. 142

13.6 Publication of data to enforce a claim

settlement 143

14 Telecommunications and Media

14.1 Deficiencies at all levels: We confront website operators

with unlawful tracking. 145

14.2 The Telecommunications Telemedia Data Protection Act —

More legal clarity for cookies. 147

14.3 Need for improvement in the online guide to test centers 149

14.4 Processing of personal data in the Internet offer

Wikimedia Foundation Inc. - Wikipedia. 152

15 Political parties and society

15.1 Electronic doorstep campaigning 155

15.2 There are also rules for non-profit organizations

Email Promotion 157

16 Europe, certification

16.1 New guidelines from the European Data Protection Board. 160

16.2 Developments in the Service Center for European Affairs 162

16.3 Accreditation and Certification News 164

17 Freedom of Information

17.1 Developments in Germany 167

17.1.1 Outcomes of the Freedom of Information Conference

commissioned in Germany. 167

17.1.2 New federal legislation 168

17.2 Developments in the State of Berlin 169

17.2.1 New state legislation — successes and failures. 169

17.2.2 Increased number of complaints — Also due to massive

structural deficits in some administrations 171

17.2.3 Individual cases 172

18 House of Representatives

18.1 Deletion moratoriums — Now also with a legal basis. 183

18.2 Parliament as a legal vacuum 185

19 From the office

19.1 Developments 187

19.2 Citizens' input from the work of the Servicestelle — Trends and

focus 188

19.3 Data protection and media literacy 190

19.4 Cooperation with the Berlin House of Representatives. 192

19.5 Collaboration with Other Bodies 193

19.6 Public Relations 194

19.7 Public Relations. 196

19.7.1 Events and Lectures 196

19.7.2 Publications 197

19.7.3 Outlook 199

20 statistics for the annual report

20.1 Complaints. 200

20.2 Consultations 201

20.3 Data Breaches 202

20.4 Remedial Actions 203

20.5 Formal support for legislative projects 204

20.6 European Procedures 205

7

List of abbreviations

Abghs.-Drs.	House of Representatives printed matter
Inc	District Court
ArchGB	Archive law of the state of Berlin
ASOG	General safety and order law
AsylbLG	Asylum Seekers Benefits Act
AsylG	asylum law
AV JugSchul Kinderschutz	Implementation regulations for cooperation between schools
AV child protection JugGes	
BAG	
BDSG	
BfDI	
Civil Code	

BGH

BlnBDI

BlnDSG

BlnTranspG

BLUSD

BMG

BMGVwV

BORON

BRAOO

BSI

BVerfG

BVerwG

BVG

and district youth welfare offices in child protection

Implementing regulations for the implementation of

child protection measures

Federal Labor Court

Federal Data Protection Act

Federal Commissioner for Data Protection and the

Freedom of Information

Civil Code

Federal Court of Justice

Berlin Commissioner for Data Protection and

freedom of information

Berlin Data Protection Act

Berlin transparency law

Berlin teacher teaching school database

Federal Registration Act / Federal Ministry of Health

General administrative regulation for the implementation of the

Federal Registration Act

professional regulations for lawyers

Federal Lawyers Act

Federal Office for Security in Information Technology

Federal Constitutional Court

Federal Administrative Court

Berlin transport company

8th

List of abbreviations

BVR

CDN

CoronaVaccinationV

DAkkS

DB

DEMIS

DNG

GDPR

DSK

eAT

EDSA

EfA principle

ground floor

EGovG

EU

ECJ

EEA

GDG

GG

GStU

GVBl.

heating costs regulation

HZI

IFK

IfSG

ICT

Association of German Volksbanks and

Raiffeisen banks

content delivery networks

Coronavirus Vaccination Ordinance

German Accreditation Body

Deutsche Bahn

German electronic reporting and information system

Data Use Act

General Data Protection Regulation

Conference of the independent data protection supervisory

federal and state authorities

electronic residence permit

European Data Protection Board

One-for-all principle

recital

E-Government Law

European Union

European Court of Justice

European Economic Area

Health Services Act

constitution

City-wide control of accommodation

Law and Ordinance Gazette

Ordinance on consumption-based billing

the heating and hot water costs

Helmholtz Center for Infection Research

Freedom of Information Commissioners Conference

Germany

German Infection Protection Act

Information and communication technology

List of abbreviations

IT

IWG

IWGDPT

JAG

YES

JB

JGG

JVollzDSG

KtDat

KV

LABO

LAF

LBG

LfD/LfDI

LHO

LMÜTranspG

LobbyRG

MFA/2FA

nPA

OLAV

OLIWA

OLMERA

public transport

OVG

OWiG

OZG

POLICIES

information technology

Information Reuse Act

International working group on data protection in the

Technology (Berlin Group)

Legal Education Act

Legal Education Regulations

annual report

Juvenile Court Act

Prison Data Protection Act

Committee on Communications Technology and

data protection

Association of Statutory Health Insurance Physicians

State Agency for Civil and Regulatory Affairs

State Office for Refugee Affairs

State Civil Service Act

State Commissioner for Data Protection / State Commissioner

tragte:r for data protection and freedom of information

State Budget Code

Food Control Transparency Act

Lobby Register Act

Multi-Factor Authentication

New identity card

Online registration of poll workers

Online application for poll workers

Online registration information

Transportation

Higher Administrative Court

Administrative Offenses Act

Online Access Act

State police system for information and communication

and processing

RKI

saLzH

SARS-CoV-2

SchoolG

School HygCov-19-VO

SenGPG

SenIAS

SenSW

SGB

SORMAS

StGB

StPO

road traffic regulations

penal law

TMG

TTDSG

UbebegG

UWG

VG

VPN's

VwGO

VwVfG

ZwVbG

Robert Koch Institute

school-led learning at home

severe acute respiratory syndrome 2 (coronavirus)

school law

School Hygiene Covid-19 Ordinance

Senate Department for Health, Nursing and

equality

Senate Department for Integration, Labor and Social Affairs

Senate Department for Urban Development and Housing

social code

Surveillance, Outbreak Response Management and

Analysis System (surveillance, outbreak response and

analysis system)

criminal code

Code of Criminal Procedure

Road Traffic Regulations

Penitentiary Act

Telemedia Act

Telecommunication Telemedia Data Protection Act

Accommodation Complaints Act

Unfair Competition Law

administrative court

Virtual Private Networks

administrative court order

Administrative Procedures Act

Misappropriation Prohibition Act

foreword

The year 2021 was in many ways a continuation of 2020. While we

but in 2020 from the corona pandemic and its effects on society

were taken by surprise, in 2021 people got used to the state of emergency to a large extent

a. Measures initially intended as temporary solutions, e.g. B. working

from home, conducting video conferences or teaching our

of children in “homeschooling”, became established and became a matter of course

part of our everyday life. It quickly became clear that the new social

reality has many points of reference to data protection. With increasing digitization

of social processes have also opened up a wide range of possibilities that

People - often unnoticed - down to the core area of their private life

investigating into it. However, private, unobserved areas are basic

suspension for the free development of personality and thus for a democratic

established society committed to fundamental rights.

Some of the issues were addressed last year and could be addressed this year

year to be finally clarified. A good example of this is the use of digital

Teaching and learning materials in Berlin schools. For a long time this was lacking

of data protection-compliant regulations in the school law on extremely shaky feet.

With the changes we are proposing, the law now contains a legal

basis for the processing of personal data of students

Teachers are explicitly allowed to use digital teaching and learning materials. For the schools

the necessary legal certainty was finally created. Another relief

the schools have learned that they are responsible for the (pre-)selection

of data protection-compliant digital tools now centrally by the Senate

administration for education is done. This means that Berlin now has more than

one of the most modern school laws that makes digital teaching data protection-compliant

allows.

We were also able to make some improvements when using video conferencing systems

register. We have revised our advice on this and our support

for those responsible for the selection of data protection-compliant services.

13

With some providers we were able to make progress in data protection law.

At the same time, however, we had to

identify violations of the law when using video conferencing systems. Straight

The public administration should be aware of its pioneering role here and

pay particular attention to compliance with data protection regulations.

The trust of citizens in public administration is significantly dependent

of the transparency of their actions. For this, the administration has to open up further. Before

Against this background, we have worked hard to ensure that the outdated Berliner

Freedom of Information Act is modernized. The submission of a draft for a

liner Transparency Act at working level was accordingly first

expressly welcomed. After the legislative process, contrary to that of us

practiced criticism, extensive area exceptions were introduced, we have it

does not regret that the draft law was passed shortly before the end of the legislative period in

ordnenhaus has failed. We hope that the project will be taken up again soon

fen and by the legislature in a transparency law comprehensive regulations for

a modern and transparent administration should be created.

In its Schrems II decision, the European Court of Justice stated that

personal data of EU citizens no longer based on the "EU-US Pri-

vacy shield" can be transmitted to the USA. For the use of standard data

data protection clauses as the basis for data transmissions, he also has high requirements

ments. A year after this landmark judgment, we have, as part of a

cross-border control of data transfers by companies in states

checked outside of the European Union or the European Economic Area.

In doing so, we had to realize that many companies were already doing the basic

have still not implemented the requirements of the Schrems II decision.

We are convinced that in many cases this can be done in a cooperative dialogue with

can be made up for with the companies concerned. However, where this is not the case

possible, sooner or later we will use the resources available to us

have to react to official measures.

Our very special concern is to prepare children and young people for the

mentary importance of data protection and give them the necessary

knowledge and skills to protect their person in the digital world

average We have therefore expanded our media education offer. for basic

Foreword We offer e.g. B. a new workshop format as a teaching unit. In this

the students can playfully discover what personal data is,

why and by whom they are processed, why they are worth protecting and in particular

special how to move safely on the Internet. The great demand has us

showed that there is a great need in schools for children to learn about media education

about the dangers and their rights in the digital age.

In view of the increasing digitization of our society - the pandemic

has again experienced an immense boost - many of those affected are

unnerved. Often the social transformation process in which we

where we are, also occupied with the fear of change. That many citizens

In view of this, there are also increased thoughts about the protection of their personal

Making data shows the high number of requests for advice and complaints that

reached us again this year. The new can also be an opportunity for

more participation, inclusion and transparency. In order to gain the necessary acceptance here

to establish the data subject, data protection must be implemented when digitizing

planning projects must be considered from the outset.

Berlin, May 2022

Volker Brozio

Acting Head of Department

15

Foreword 1 Priorities

1.1 International traffic one year after

"Schrems II"

s

i

x

a

right

P

right

e

i.e

s

and

A

One year after the judgment "Schrems II" of the European Court of Justice (ECJ)1 shows

a legal opinion obtained by us together with other supervisory authorities

that most of the previously customary data exports to the USA are no longer permitted

are - and that the use of US-linked service providers: even then critical

is if they process the data in Europe. Various individual

drive, as a concerted examination of many German supervisory authorities shows,

that numerous companies even the obvious requirements of the judgment

still not implemented.

With its judgment, the ECJ declared the decision of the EU Commission to be invalid,

after which the regulations of the "Privacy Shield" the transmission of personal

Data allowed in the US. For the use of standard contractual clauses, the

ECJ set high requirements.2

a) Ex officio examinations and on the basis of complaints, as well as consultations

After the "Schrems II" verdict, we received more and more complaints and information about

illegal data exports. In addition, we have also dealt with the topic proactively

works.

An important subject of our consultations with the BVG in the matter of “Jelbi”3 and

"Check-In-Check-Out-App"4 were, for example, international data flows and the

set of US intertwined service providers. The BVG did not succeed in explaining how

related data processing should be lawful. Because the included

In order to fulfill their tasks, service providers must provide the personal

1 ECJ, judgment of July 16, 2020 – C-311/18, “Schrems II”

2 See 2020 Annual Report, 1.2

3 See also 11.1

4 See also 11.2

process relevant data in plain text. That in this case no technical

Measures are in place to prevent US authorities from gaining unauthorized access to the data

ruled out, we had already reported.5 The BVG had the mission in particular

isolated hardware6, which basically provides a sensible technical security

security measure. However, this can result in access from service providers: in-

and thus the possibility of access by the US authorities cannot be ruled out.

We also took part in a cross-state test campaign by the German authorities

supervisory authorities involved in the implementation of the “Schrems II” judgment.7 We have

around 900 Berlin companies with regard to possible data exports to countries

Outside the European Union or the European Economic Area (third countries)

subjected to an automated preliminary check. We have over eighty companies

then asked for an opinion on the basis of the findings from the preliminary examination, because

we had found indications of illegal data exports. The one of us

The catalog of questions used was based on the transnationally coordinated, in

Questionnaire published on the Internet8.

In the course of the proceedings we have conducted, we have regularly found that

the companies were completely unaware that pure support or ad

ministrations accesses or short-term decryptions9 requiring justification

Show data exports.

b) Opinion on the legal situation in the USA —

Effects on data processing in the EU

In the "Schrems II" judgment, the ECJ already dealt with the legal situation in the USA in a very comprehensive manner

checked. Nevertheless, some questions remained unanswered, particularly with regard to corporate

who are not traditional IT service providers. Together with the Germans

regulators, we have a legal opinion with Professor Stephen I. Vladeck,

University of Texas at Austin. Professor Vladeck is more renowned

5 JB 2020, 1.2

6 so-called nitro enclaves

7

See also press release dated June 1, 2021; https://www.datenschutz-berlin.de/fileadmin/

user_upload/pdf/pressemitteilungen/2021/20210601-PM-Schrems_II_Pruefung.pdf

8 See, for example, at https://datenschutz-hamburg.de/pages/fragebogenaktion/

9

Such as services for detecting and defending against attacks on websites and content

Delivery Networks (CDN)

17

Connoisseur of US secret service law and had in the "Schrems II" case

already prepared a legal opinion for Facebook. Some key findings

from his report10 are singled out here:

• According to the "Schrems II" judgment of the ECJ, which is not compatible with the European

right compatible US law affects very many companies. Because among the inso-

far relevant term "electronic communication service provider" not only fall

classic IT and telecommunications companies, but also, for example, banks,

Airlines, hotels or shipping service providers. In addition, it is

chen subcategories of this term do not even require the services

be made available to the public, but it may suffice, for example,

that a company provides its employees with an e-mail service. The

The term also includes providers of “remote computing services”, i.e. classic

cal cloud, computing or hosting services, and not just traditional ones

Telecommunications providers.

• Even if a company only with regard to very few or even just one

individual service (e.g. e-mail service for employees) as "electronic

tion service provider”, the access rights of the US authorities are not

limited to data related to this service. Rather "infected"

even the slightest classification as “electronic communication service

provider" all data of the company, even if this communication

service has nothing to do with the actual entrepreneurial activity.

• Uses a not to be regarded as an "electronic communication service provider"-

of the company services of an "electronic communication service provider",

then the data there is subject to access by the US authorities.

• US law11, which is problematic according to the assessment of the ECJ, not only intervenes

when data is processed in the USA, but also when US companies

10 Stephen I. Vladeck, “Memo on Current State of U.S. Surveillance Law and Authorities”, available

bar at https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/datenex-

porte

In this respect, Section 702 of the US Foreign Intelligence

gence Surveillance Act of 1978 (FISA), also 50 U.S. Code §§ 1881, 1881a because about this

Companies and employees can be forced to release data.

11

take or its affiliates process data outside of the United States –

about in Europe. US law is extraterritorially applicable in this respect. US corporate

men cannot defend themselves with the fact that the release of the data after the

General Data Protection Regulation (GDPR) is not permitted.

• European companies that are active in the USA can also

matic US law. However, this probably does not apply to parent companies,

which are not active themselves, but only through their subsidiaries in the USA.

c) Recommendations of the European Data Protection Board (EDPB)

on additional protective measures for data exports

As reported last year,12 the EDPB has drawn up recommendations on how

Those responsible and processors who process personal data in third parties

countries want to transmit should proceed. Also involved in the revision of this

missing after public consultation, we participated. The recommendations that

coordinated in detail with the new standard contractual clauses of the EU Commission13

are now available in the final version 2.0.14

The final version essentially only contains clarifications. the one for the public

Consultation provided version 1.0. In particular, the EDPB – in accordance

with the case law of the ECJ – the so-called risk-based approach15 for data exports

again expressly rejected.

Version 2.0 of the recommendations also deals with the case that the legal situation in

third country is unclear.16 In this case, after proper examination, the

Situation revealed that no additional protective measures are required.

12 JB 2020, 1.2

13 See 1.1.d

14 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to en-

ensure compliance with the EU level of protection of personal data, available at https://

edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommenda-

tion-best-practices_en

15 In a risk-based approach, the probability of occurrence and impending damage

evaluated in order to then accept a certain level of risk, above a certain risk

assessment to provide further protective measures and not to accept excessive risks,

but to refrain from data processing.

16 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure

compliance with the EU level of protection of personal data, paragraph 43.3

The condition for this is that the data exporter: in a detailed report

can prove that the law of the third country is neither interpreted nor in practice

xis is applied in such a way that the respective data and/or the respective recipients

catcher:inside concerns. So it is not only a question of the application in practice,

but also on the interpretation of the unclear law. Only that problematic

cal law is not applied in practice does not suffice for the intervention of the latter

exemption. Consequently, it is not sufficient to point out that

problematic right to not a single comparable company and not a single

comparable date has ever been applied. Rather, this non-application

be a consequence of the fact that the law of the third country is interpreted in such a way that it

does not apply to the companies and data in question.

In the case of the USA, which is particularly relevant in practice, it should be noted that US law is partly

does not meet European fundamental rights standards. For a consideration of

However, there is no room for practice if the legal situation is already deficient. In addition

In many practice-relevant cases, US law does not allow precise statements on

the existence or non-existence of access by the authorities. In such cases

The practical experience of the data importer cannot be taken into account.17

d) New Standard Contractual Clauses

In June, the EU Commission decided on new standard contractual clauses. There are

now a single comprehensive set of standard contractual clauses for data exchange

ports to third countries.18 Unlike the old standard contractual clauses, these include

also the regulations for order processing and are mandatory in this respect if a

Data export is justified via the standard contractual clauses. About it

In addition, there are standard contractual clauses for data processing contracts within

of the EEA,19 whose use is optional. The new standard contractual clauses apply

17 Recommendations 01/2020 on measures that supplement transfer tools to ensure compli-

ance with the EU level of protection of personal data, paragraph 47

18 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard

contractual clauses for the transfer of personal data to third countries in accordance with the

Regulation (EU) 2016/679 of the European Parliament and of the Council, C/2021/3972,

OJ L 199 of 7 June 2021, pp. 31-61

19 Commission Implementing Decision (EU) 2021/915 of June 4, 2021 on standard procedures

contractual clauses between controllers and processors pursuant to Article 28, paragraph 7

of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29

Paragraph 7 of Regulation (EU) 2018/1725 of the European Parliament and of the Council,

C/2021/3701, OJ L 199 of 7 June 2021, pp. 18-30

20

Chapter 1 Focus 1.1 International data traffic one year after "Schrems II"

among other things, the "Schrems II" judgment of the ECJ and are coordinated in detail

to the recommendations of the EDPB to supplement protective measures.20 The after the

The tests and additional protective measures required by the case law of the ECJ

are now expressly regulated in the standard contractual clauses.21

In practice, it should be noted that other agreements of the parties in no case

directly or indirectly contradict the Standard Contractual Clauses

or restrict the fundamental rights or freedoms of data subjects

allowed.22 Such a contradiction can also exist, for example, if payment

regulations, the effective effect of obligations and rights from the standard

contract clauses is jeopardized. Such initially purely economic agreements

without any reference to data protection law, violations of the data

evoke protective rights. A case-by-case assessment is always required here. flat rate

Remuneration regulations for all services provided by processors should

be inadmissible, however, because this means that such controls23 are also subject to a fee

which are only necessary because processors oppose

breached data protection obligations. As a result, those responsible

che are prevented from carrying out controls that are mandatory under data protection law

to perform. The same applies to other support obligations.

Transfers of personal data to third countries without the EU Com-

mission attested adequate level of data protection also with the

new Standard Contractual Clauses a challenge. The required exam

20 See 1.1.c

21 Clause 14 of the Data Export Standard Contractual Clauses Annex to the Implementing Decision

(EU) 2021/914 of the Commission of June 4, 2021 on standard contractual clauses for the

transfer of personal data to third countries in accordance with Regulation (EU) 2016/679 of

European Parliament and of the Council, C/2021/3972, OJ L 199 of 7 June 2021, pp. 31-61

22 Clause 2 a) of the Data Export Standard Contractual Clauses, Annex to the Implementing Decision

(EU) 2021/914 of the Commission of June 4, 2021 on standard contractual clauses for the

transfer of personal data to third countries in accordance with Regulation (EU) 2016/679 of

European Parliament and of the Council, C/2021/3972, OJ L 199 of 7 June 2021, pp. 31-61;

Clause 2a) of the Data Processing Standard Contractual Clauses, Annex to the Implementation

Commission Decision (EU) 2021/915 of June 4, 2021 on Standard Contractual Clauses

between controllers and processors in accordance with Article 28(7) of the Regulation

(EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of the Regulation

Regulation (EU) 2018/1725 of the European Parliament and of the Council, C/2021/3701, OJ L 199

7 June 2021, pp. 18-30

23 See Article 28 (3) subparagraph 1 lit. h GDPR

the legal situation and practice in the third country concerned is limited to

the specific data transfer, but must be comprehensive in this respect. Often he will

The associated effort is disproportionate to the benefit of the data export

hen. Especially in the area of using IT services, the pragmatic

Away, therefore, with a waiver of data exports to third countries that are not recognized as secure.

In the case of the USA, this is usually the only legally compliant solution, since the

The legal situation has been determined by the highest court to be insufficient and additional protective

measures are only considered in a few exceptional cases. responsible

che, which impermissibly transmit personal data to third countries - be it

directly or through service providers or their subcontractors

Stop the data exports immediately and retrieve transmitted data. violations

can not only entail orders that prescribe business operations

can pose significant problems, but also high fines. Furthermore-

from arise from the extraterritorial applicability of the US

Surveillance law comparable problems when US companies, subsidiaries

affiliates of US companies or other companies operating in the USA

Offer IT services in Europe.

1.2 Digitization of schools — continued

Last year we discussed in detail the deficits in the field of digital

ment of the schools reported.24 This year we were again with this

subject concerned. Despite some improvements, the goal is a privacy-friendly

Digitization of schools still far away.

s

i

x

a

right

P

right

e

i.e

s

and

A

Until well into the spring, the students became the majority

taught exclusively in school-led learning at home (saLzH). Next to

the serious effects of the lack of face-to-face teaching on development

of the students showed clearly that even after many months of the pandemic

mie had not been able to function across the board and comply with applicable law

provide appropriate digital infrastructures and provide schools with legally secure

To provide software solutions for effective distance learning. We have

These are also intensive consultations with school administrations, teachers and parents

24 JB 2020, 1.4

year continued. We have also repeatedly given our companies to the education administration

support was offered, but unfortunately not always accepted. In the

for the schools difficult time of the pandemic we are with our supervisory activities

Wisely pursued and have resorted to drastic measures as far as possible

waived. The temporary waiver of supervisory measures against the deployment is not

of data protection-compliant solutions must not, however, lead to this being understood

takes. We therefore expect that the schools, if they have not already done so,

immediately switch to data protection-compliant solutions and configurations

complete.

We have made it very clear publicly25 that individual schools

as those responsible for data protection under the Berlin Schools Act (SchulG).

alone are not able to carry out a comprehensive test for every product to be used

compliance with all data protection requirements and an assessment of the

to ensure the security of the data. We see the educational administration as having a duty

to take on this task and to support the schools in order to

to ensure legal certainty. The schools are equipped with the necessary checks of the

The tools used are overwhelmed, since it is not just about the evaluation

the pedagogical suitability of digital teaching aids, but also one

Examination of complex data protection issues is required. school boards

and teachers are neither trained for this nor do they have the necessary skills

time resources. There is a need to define minimum standards for the

set of digital teaching and learning materials and a pre-selection of pedagogically suitable ones

and lawful use of digital services and products by the educational

administration. We have urged such a task of educational administration

also to be anchored in school law in order to achieve the necessary binding nature.

It is very gratifying that the legislature has taken up our suggestions and kept them short

before the end of the legislative period important decisions for a data protection

right digital school lessons.26 Now it is up to the school administration

obligation to comply with these legal requirements.

25 Press release of January 22, 2021; see https://www.datenschutz-berlin.de/fileadmin/

user_upload/pdf/pressemitteilungen/2021/20210122-PM-Digitaler_Unterricht_Misstaende_

fix.pdf

26 See 1.2.1

1.2.1 Legal basis for school digitization

Due to the lack of a legal basis in the SchulG, the use of digital teaching and learning

means in the classroom since the beginning of the pandemic has only been possible if an effective,

i.e. H. informed and voluntary consent of parents or adult students

Template. However, this practice practiced in schools encounters considerable data protective concerns. The use of digital tools brings a whole new Quality of the lesson design with itself and is at the same time with an extensive processing of personal data. This differs in their Scope very significantly from the analog school lessons take place data processing and has a significant impact on personal rights of the students and teachers. The creation of a legal regulation for the Processing of personal data was therefore necessary. This is already evident from the materiality case law of the Federal Constitutional Court.27 Consent Genes as a basis for data processing are not suitable here. Given the school conditions shaped by the state education and upbringing mandate28 There is a superior/subordinate relationship between students and schools. The condition of voluntariness necessary for the effectiveness of a consent29 can hardly be fulfilled in this respect. We have been pushing for many months that the necessary changes to be made in the SchulG in order to benefit everyone involved To create legal certainty for the use of appropriate tools. We have it therefore basically welcomes that the education administration in the spring a draft bill submitted for an adjustment of the SchulG. Unfortunately, the draft only got to us very much submitted late as part of the participation of interested specialist groups and associations. It would have been more effective to involve us in the development of the draft the, because unfortunately this encountered in large parts very significant data protection critical criticism. In addition, we had to realize that ours were repeatedly submitted suggestions were not considered.

In particular, our proposal to establish a binding obligation of the digital teaching and learning materials suitable for schools to be anchored in law, leaning. The education administration shied away from the expenditure of resources and expressed the

27 See 2020 Annual Report, 1.4.4

28 Art. 7 para. 1 Basic Law (GG)

29 See EG 43 GDPR

Concern that pedagogical freedom could be compromised by a central definition of digital methods
serve to be restricted. However, this concern is unjustified. A bundling of
Capacity in education administration ultimately leads to a relief
of the schools, which can then put their resources into the pedagogical work.
Complex multiple tests by the schools are thus prevented.
Since the education administration was not willing to accept our proposals for the change and
To implement the supplement to the SchulG, we have decided to carry out concrete research
to develop mulling proposals. It was important to us that in the SchulG not just one
Authority to process personal data when using digital teaching
and learning resources including those provided by the Education Administration
learning management system is created when fulfilling school-related tasks,
but also a basis for data processing when using digital
Communication tools, which include not only video conferences but also data protection
compliant messenger or email services count. The education administration in the
The regulation proposed by the ministerial draft would not have covered such services. loading
It was particularly important to us to make the determination in the SchulG that
Design of data processing in a separate "Digital Learning Materials Ordinance"
to settle. Such a regulation offers the opportunity to quickly respond to changes at any time
React to circumstances due to new technologies and make the necessary adjustments
to be able to do.
As part of our statutory mandate30 to advise the House of Representatives,

we have submitted our wording proposals to the coalition factions of the

netenhauses presented. We very much welcome the fact that our proposals have subsequently been

the SchulG, which was passed in September, have been included. Berlin

thus has a modern SchulG, which lays the foundations for a data protection-compliant

creates lessons.

It is particularly gratifying that the legislator has taken up our suggestion

to legally oblige the education administration to make a selection for the

len digital teaching and learning materials to be considered and thus the

Train the necessary assistance in the selection of data protection-compliant digital

30 Article 57 (1) (c) GDPR, Section 11 (1) sentence 1 no. 3 BlnDSG

to provide tools.31 The regulation comes into effect at the beginning of the school year

2022/2023 in force.32 The time should be used by the education administration so that

the schools can rely on it for the next school year at the latest

to be able to use data protection compliant tools.

1.2.2 School Data Ordinance and "Digital Learning Materials"

Regulation"

With the adoption of the SchulG, the legislature has the necessary legal

created the basis to enable digital teaching and in this

Framework to legitimize the processing of personal data. However, can

the law only provide the framework for this, which is to be filled with life in practice

must. The education administration is now obliged to implement the relevant legal

to issue regulations.

First of all, the completely outdated school data regulation from 1994 needs to be amended.

lol We have been pushing since 2018 not only to overhaul them cosmetically, but

instead to completely restructure them.33 Unfortunately, the education administration

tion has not yet taken up our suggestion. Since our last extensive

Statement from February on the present draft and a discussion in

Expert Committee of the House of Representatives in March34 we were no longer in the

matter involved.

The School Data Ordinance primarily contains regulations relating to school

everyday life and thus relate more to school administrative processes. She controls the content

and dealing with student documents (student documents, student

personal sheet, student files, student files, etc.) as well as storage

deadlines, for example in relation to certificates, documents from the school psychological service

or special education reports. These regulations are urgently needed

the update, but are not subject to the constant changes caused by the

31 § 7 paragraph 2a sentence 2 SchulG

32 Section 129 (13) SchulG

33 See Annual Report 2019, 5.4

34 ITEM 3 of the 38th meeting of the Communications Technology and Data Protection Committee

(KTDat) on March 22, 2021

Digitalization. It is therefore expedient, in addition to the school data regulation, to

To enact the “Digital Learning Materials Ordinance”, which sets out the regulations of the SchulG for the

Use of digital teaching and learning materials as well as digital communication tools

specified and the data protection requirements defined.

Since the digitization of schools will continue to require adjustments in the future

legal regulations to the changing future technologies

is required, two separate ordinances are required in order to react quickly to changed circumstances

to be able to react without immediately adapting the entire school data regulation

to have to. We welcome the fact that the legislator has followed our proposal in this respect
is and the education administration has obliged, in addition to the school data regulation
to enact such “Digital Learning Materials Ordinance”.35 In this ordinance, the
data protection requirements from a legal and technical point of view
so that they can be implemented in everyday school life. We expect,
that the education administration involved us early on in the development of the "digital learning
tel regulation" and the necessary amendment of the school data regulation
planning is now completed quickly.

1.2.3 "Berlin learning space" - What has happened?

In our last annual report36 we reported extensively on the
The current project “Lernraum Berlin” reported. Due to the corona pandemic, he got
"Lernraum Berlin" as the learning management system of the state of Berlin suddenly had a special
their importance, since digital teaching was implemented in many schools.
Unfortunately, this project, in which we had not previously been involved,
ren, various deficiencies in relation to data protection and data security. We stand by this
still in contact with the education administration. Regarding data protection
we were able to make some progress. This is how it was before the change
of the SchulG for the use of the “Berlin learning space” in the classroom context
Declaration of consent revised and adapted several times in consultation with us.
In addition, a data protection-compliant video conferencing solution was available from January
Use of the open source software Big Blue Button integrated into the "Lernraum Berlin"

35 Section 64 (11) sentence 2, Section 64c (3) sentence 2 SchulG

36 JB 2020, 1.4.1

grated. The use of the previously used video conference system, which we previously used as a
is not classified in accordance with data protection regulations,37 could be reduced in this way. after one

extensive correspondence with the education administration, they finally

secured, the data protection questionable video conferencing solution with the beginning

switch off completely during the Christmas holidays.

With regard to the video conference system now used, a concept was presented to us

provides, with which teachers have the opportunity to parents for parents' evenings or

Parents talks provide temporary IDs for the video conferencing system

deliver. We very much welcome this possibility, since such recourse to other –

non-compliant with data protection - video conferencing systems and the misappropriation of the

Student access can be avoided for this.

With regard to the data protection deficiencies that we identified last year

the lack of multi-client capability or the lack of deletion routines38 could also

progress is being made. Erasure routines were coordinated with us and measures

measures taken that could significantly improve the overall security of the system. middle

Meanwhile, the responsible senate administration has given us a concept for separating clients

presented, which seems very viable and the division of the learning space on each

because it provides for a single instance per school. With the implementation of this concept would be

this long-standing deficiency has finally been remedied.

We will continue to support the further development of the "Berlin learning space" and

are also available to advise the educational administration on other projects.

1.2.4 Teacher-Teaching-School Database

The Berlin teacher training school database (BLUSD) is an IT process

used by schools for school administration. personal data

ten from all students, parents and teachers as well as other school

Employees are responsible for the tasks assigned by the SchulG in this

Processes processed automatically, e.g. B. to organize the lessons, the application

37 See also 2.2

38 See 2020 Annual Report, 1.4.1

security check or the creation of certificates. access to this system
are only provided to a limited extent, essentially by the school management
see. In principle, the use of the BLUSD according to the SchulG is mandatory for all schools
binding. However, the process of connecting all schools to the system is still ongoing
not completed. We have been supporting the project since 2016. After a long time
We have seen that there was hardly any exchange with those responsible for the project
of the numerous current projects in the further development of the BLUSD since the beginning
this year intensified the exchange with the education administration. In regular
constructive meetings, pending changes are now communicated early and
discussed. Advice and suggestions on our part were taken up and widely used
Parts also implemented.

Since it is apparently planned to use the personal data processed in the BLUSD
also for other purposes, e.g. B. the school portal for Berlin teachers39, can be used
make, special attention must be paid to the fact that this is only possible within the
prior to statutory purposes and with the security architecture of the BLUSD
is compatible. An example is the use of the personal data contained in the BLUSD
Genetic data for the provision of user access in the educational
administration provided learning management systems. To use the
personal data of the students stored in the IT technical process, the
are subject to special protection and a strict earmarking, also for this
to enable, it was necessary to adapt the SchulG and the data processing
ment to be explicitly regulated by law.40 If other extensions or changes
of the technical realization are in the planning phase, close monitoring is required in order to

to ensure compliance with data protection and technical requirements.

We will therefore also continue this project by continuing the constructive exchange

continue to accompany.

The data protection-compliant digitization of schools remains a special

challenge. With the adjustment of the school regulations is an important one

step done. It is now the task of the education administration to

to create clarifications at the regulation level. A particularly important

The task also consists in the mandatory selection provided for in the law

39 See https://schulportal.berlin.de

40 See Section 64a Paragraph 10, Section 64c SchulG

of data protection-compliant digital teaching and learning materials and the

develop the necessary professional competence in educational administration. There is a hurry

necessary, so that at the beginning of the new school year 2022/23 there is actually one

Listing for schools is available. We expect that the educational

administration takes this obligation seriously. Our repeated in the past

The offer made for advice on data protection issues continues.

1.3 Corona vaccination management of the State of Berlin

s

i

x

a

right

P

right

e

i.e

s

and

A

1.3.1 Online appointment booking with private companies

At the end of 2020, Berlin - like all other federal states - saw itself

confronted with the task of vaccinating citizens as quickly as possible

to organize against the pathogen SARS-CoV-2. With the technical processing

The responsible Senate Department for online vaccination appointments

Health, care and equality entrusted to a private company. Against

there would be basically nothing to object to, insofar as the company was commissioned with a

speaking order processing contract would be based and the company

Limits that are set for him as a processor, would also comply. straight last-

however, res is not the case. The focus of our criticism is that the citizens

as part of the online appointment booking process with the creation of a usage

account also has to have its own contractual relationship with the private company

have to enter.

For vaccinations against SARS-CoV-2, which took place in the vaccination centers and further

take place, Berliners have to make a specific appointment. First

In the course of the year, vaccinations were also carried out in certain vaccination centers without prior

Appointment made. In addition to booking an appointment by telephone via a

Vaccination hotline was and still is the possibility to book a vaccination appointment online

to book online. For this online appointment booking, the Senate Department for

health, care and equality the service of a private company. Although has

the National Association of Statutory Health Insurance Physicians (KBV) offers an online appointment

booking system provided by some countries - e.g. Brandenburg – too

has been deployed. However, the use of this system was not for the countries

mandatory and was not initiated by Berlin. Would Berliners want to

line book a vaccination appointment in a vaccination center, you can therefore use it

of the system operated by the private company.

In their "Data protection information on vaccination against SARS-CoV-2 (corona vaccination) in

Vaccination centers" informs the Senate Department for Health, Care and Equal Opportunities

The Berliners said that they said that for online appointments

companies and this company acts as a processor for them

become. Against the use of a private company as a processor is - how

mentioned at the beginning – basically nothing to object to.

However, a processor may only process the data on behalf of and on

process the instructions of the person responsible. That is with the present integration

of the company is not the case. Because the appointment booking via the system used

tem requires the creation of a user account with the private company. There-

This creates a contractual relationship between the company and the individual

users. The company's data processing in connection with the

The user account is created for the purpose of carrying out the between

contract concluded between him and the respective user. This leaves that

Undertakes its role as processor for the responsible Senate administration

and acts as the person responsible for data protection.

Because people who want to be vaccinated against SARS-CoV-2

be forced to enter into a contractual relationship with a private company

hen, not only bothered many people willing to be vaccinated, who subsequently dealt with the corresponding

questions and complaints to us. We too had the Senate administration

for health, care and equality and the company at an early stage

drawn attention to the existing problem and pointed out that the

Integration of the company can also be designed in accordance with data protection.

A data protection-compliant procedure requires u. provided that the usage accounts that the

Berliners have invested with the company only on behalf of and on instruction

the responsible Senate administration - and not for the company's own purposes

take – may be created and used. The responsible Senate administration is

therefore held, vs. to instruct the company to delete the user accounts

sen as soon as they have served their purpose.

31

If a company processes data for a Senate administration as a processor

should work, this may only be done within the framework of the instructions of his client.41

If a responsible person determines data protection violations by their processor,

does she have the processor with the means of contract law to a

to urge conformist behavior. That we take immediate action in this respect

expect from her, we have the Senate Department for Health, Care and Equal

position communicated.

If citizens would like to receive a vaccination appointment via online registration, it remains

so far they often have no choice but - mediated by the Senate Department for

Health, care and equality - customers of a private company

become. This can neither be in the interest of the citizens nor of the administration.

It is incomprehensible to us that the responsible senate administration

obtained information on the manner in which the company was involved as an order

processors for booking appointments at vaccination centers has so far ignored. The of

the measures we expected to take to create a data protection-compliant state

have not been met so far. We will therefore continue to work towards

the personal data of those willing to be vaccinated only within the framework of the law

Permitted to be processed.

1.3.2 The purpose limitation issue

s

i

x

a

right

P

right

e

i.e

s

and

A

Through a press release from the Senate Department for Health, Care and Equal

position, we had to learn that this was with the Association of Statutory Health Insurance Physicians

(KV) Berlin has agreed that KV Berlin will accept invitations to claim

vaccinations against the pathogen SARS-CoV-2 to around 400,000

Persons who, due to an existing chronic illness, have a priority

have certified vaccination eligibility. The invitation should be "on behalf of" the

Senate Administration and on the basis of the billing available at KV Berlin

planning data take place. This procedure was neither permissible nor necessary.

The KV provide in Germany u. a. the outpatient medical care of the

lich health insured. The contract doctors calculate all services that

41 See Art. 29 GDPR

they provide for those with statutory health insurance, quarterly with the relevant health insurance company away. This billing data also contains information about the medical diagnoses.

The data is therefore particularly worthy of protection for good reason Social data, the processing of which is limited by the Social Security Code (SGB)42 is subject.

In principle, the KV may only use the social data for those specifically specified by law process tasks. The identification and notification of persons entitled to be vaccinated falls but not in this list of tasks.

A so-called "purpose-changing further processing" of the billing data also came here not considered. Such would only have been permissible insofar as it was regulations of the SGB or according to the Infection Protection Act (IfSG) or would have been permitted.43 However, this was not the case. In particular, the IfSG no obligation of the KV Berlin to vaccinate persons under the statutory to identify and contact lich health insurance. Rather, it sorts it out

The law only states that the KV Berlin requires certain information about already carried out vaccinations in a pseudonymised44 form to the Robert Koch Institute and the Paul-Ehrlich-Institut.45

A legal basis for the procedure of the health administration and the KV Berlin therefore did not exist. We have pointed this out to the State Secretary responsible.

But is data protection - as malicious gossip has it - once again the Fighting the corona pandemic in the way? – Not at all!

According to the legal requirements, the chronically ill would very well can be informed of their prioritized eligibility to vaccinate. Just not through them KV, but by the statutory health insurance companies and the private health insurance

ments. Because for these are by the federal legislature precisely for this purpose

42 Here in particular through § 285 SGB V

43 Section 285 (3) sentence 1 SGB V

44 Pseudonymisation is the replacement of identifying information such as name, address, birth

date or other unique identifiers or characteristics with a different designation

(e.g. a serial number) in such a way that a conclusion can be drawn about the person without knowledge of the

assignment rule is not possible or only possible with disproportionate effort.

45 Section 13 (5) sentence 1 IfSG

Legal bases have been created to ensure utilization and security

of the vaccines.46 Incidentally, the advantage would have been that of

This variant could also have benefited the chronically ill people who

are privately insured. Because for this group of people, the KV naturally does not exist

billing data. Privately insured, due to an existing chronic

disease have a prioritized eligibility to vaccinate were therefore still

instructed to first obtain a medical certificate in order to schedule a vaccination

to be able to agree.

The processing of particularly sensitive social data will not be processed

made high demands for no reason. These specifications may also at times

of a pandemic cannot simply be ignored. A lawful way would have

been available.

1.4 Data processing by corona test centers

With the introduction of free rapid corona antigen tests (so-called citizen tests47)

Corona test sites shot up in large numbers. At times there was alone

in Berlin well over 1,000 test sites. With data protection and data security

many test sites didn't take it that seriously.

s

i

x

a

right

P

right

e

i.e

s

and

A

As the supervisory authority, we are responsible for those test sites whose operators:

are based in Berlin. There have been a number of data breaches and

numerous other data protection violations.

Many test centers offer citizens the opportunity to apply for a test

appointment to register. The collection of the personal data required for the test

ment-related data is thus simplified. In addition, it is possible in this way

Citizens to submit their test results electronically so that they do not

have to wait on site for the result.

46 § 20i paragraph 4 sentence 2 SGB V; Section 6 (7) CoronaImpfV (as of March 10, 2021)

47 See Section 4a of the Coronavirus Test Ordinance (TestV)

A number of test centers required, in addition to the necessary

necessary information other personal data necessary for the implementation of the

Citizen testing is not required. This is how some test centers made the appointment booking

dependent on the fact that, for example, the health insurance or the identity card number

mer is specified. However, since there is no legal basis for this, we gave such

suggest testing sites to remove these queries from their appointment booking forms.

Some test sites sent the tested people their test results by email

E-mail. It happened as it had to happen: Some test centers sent tester

results to wrong recipients. We gave the respective test sites concrete

Instructions on how the information is transmitted to the tested persons in compliance with data protection

can be averaged.

We also referred them to the guideline "Measures to protect personal

personal data when transmitted by e-mail" of the conference of independent

pending data protection supervisory authorities of the federal and state governments (DSK)48. The

In particular, the guidance provides the existing requirements for the

coding of the messages. These are based on the risks for those affected

Persons. The unauthorized disclosure of information about an infection is such

risk. To avert this, a qualified transport encryption is necessary

agile, but not sufficient on its own. If the tested citizens, like the

As a rule, there is no way to receive end-to-end encrypted emails

then the file with the test result must be encrypted. to develop

the citizens get a sufficiently long code in the test center,

randomly generated password.

Furthermore, some test centers used the e-mail addresses of the people tested,

to give them advertising that had nothing to do with testing (e.g. for sports courses).

send. The requirements for the permitted use of e-mail addresses for advertising

purposes were regularly not fulfilled.

Finally, data leaks occurred at a number of test sites, which

allowed third parties to retrieve data about the tested citizens.

48 Available at https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/ orientation aids

This often did not hit a single test center, but a whole series of them. The misery-
agile software and the server infrastructure is regularly not used by the test
programmed and operated by ourselves, but as a service provided by third
bought. Data breaches caused by incorrect implementation of the software
lie, therefore regularly affected several test sites, often in different ones
states.

On the one hand, we learned about these data breaches from the data breach reports
operators. On the other hand, security researchers also shared data breaches with us
that they noticed during a security vulnerability check.

The biggest problems were with the software for providing the test results
over the internet. It may only allow a tested person to call up their own tester
results and only after logging in with at least the user name and
enable a password. Attempts to access other test results must
disable the software. Alternatively, the tested person can still be in the test center
an internet link or code to retrieve the test result will be provided, provided
Link or code contain as many random characters (numbers and letters) that it
practically impossible by simply trying someone else's code
Identify the person and find their test results.

However, some test centers we checked used links that each
contained the number of the test performed. Simple counting up or counting down
Lending to this number provided test results from other people. In other cases were
easily decode the retrieval codes. With simple programs, many possible

tested codes, test results could be obtained from hundreds or thousands of people

be retrieved.

Sometimes they found themselves hidden, but easily found with specialist knowledge, on the web

on the part of the test centers also access data to other service providers used:

who, for example, took over the sending of e-mails and SMS messages. With these

Access data could in turn be viewed, which allows conclusions to be drawn about the data

tests carried out and contact details of tested persons.

There is a simple measure to reduce the risk of unlawful

Processing of the data provided by the test centers for the tested persons

be asked. It consists of this data - as legally required anyway - so

to be deleted as early as possible.

Those responsible have usually informed us of the data breaches described within

reported half the time allowed by law. We then, if ne-

tig, further investigations into the facts made and recommendations or also

Requirements regarding the technical and organizational measures to be taken

men pronounced. In addition, we have requested that the

affected persons will be informed.

We also have ex officio investigations into a larger number

initiated by test centers. These were aimed at ensuring that the protection of

data of the citizens is not weakened by the fact that the test centers

providers outside of the European Economic Area.

The software applications of many test sites make significant use of cloud

Services for operating the websites and for storing data, e.g. B. the test

results. There are also e-mail and SMS sending services. These services will

often operated by US service providers. Or from service provider:in-

who in turn are US service providers as sub-service providers

ter: use inside. The websites also often have content from external servers

integrated and thus inadmissible personal data to their operator:in-

NEN disclosed, often here again US companies. This creates risks for

the persons concerned.49

Most of the testing sites we contacted voluntarily turned off the violations and

For example, the service providers for booking the tests, operating the

website or sending e-mails. They also removed inadmissible third-party content

from their websites. In a number of cases, we first had to carry out basic

explanation, because the data protection dimensions are not explained at all

had been known. A test site that proved to be particularly problematic was

the entire e-mail communication a private customer account of a US service

ters used.

49 See 1.1

Due to the large number of test points we have received and always

We have information about incoming inquiries and complaints on our website.

Information is provided on particularly frequently asked questions.50

In connection with the citizen tests, the test centers process personal

related data of a large number of citizens, including health

health data. The large number of complaints about test sites and notices

to security issues that reached us show along with the kind and the

The scope of the violations we found that the issue of data protection at a

large number of these entrepreneurs is not present, or the test centers have the data

simply ignore the legal requirements. The consideration of data

intellectual property requirements for the approval of the test centers and the reference

to offers for data protection training would have been desirable.

This would have avoided many data protection violations and the data of citizens:in-

can be better protected.

1.5 Attendance documentation and

contact tracing

s

i

x

a

right

P

right

e

i.e

s

and

A

To combat the pandemic, the legislator has ordered that organizers:

ers, restaurant operators and other bodies or persons about the presence

must keep accounts of guests in their rooms. As an electronic system for this

An application sponsored by many federal states established itself for this purpose. We con-

trolled the operator of this application for security and data economy

enforce.

An essential method of combating the corona pandemic is that

the health authorities determine the contacts of infected people and record them

demand to isolate themselves and be tested in order to break chains of infection.

The infected people know some of the contacts from their personal environment.

Other people you might meet at events, in the bar or in a

shop, or in the vicinity of which they are, for example, in a restaurant or

stopped at a football stadium are not known to them. Therefore he

50 https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/teststellen

Chapter 1 Focus 1.5 Attendance documentation and contact tracing

Legislators the organizers and operators of restaurants and many

other establishments are obliged to keep accounts of their guests.

In the case of small institutions in particular, this was initially done mostly with paper lists

ten or slips of paper on which the guests wrote themselves. This procedure raised problems

when guests enter the names and addresses of other people in the same restaurant

the organizers could misuse the collected data for other purposes

needed or government agencies wanted to gain unauthorized insight into the lists. Not

most recently, the sometimes required transmission of attendance data to health

health authorities by fax, post or, after a scan, by e-mail, which is time-consuming and insecure.

It therefore made sense to replace this paperwork with an electronic process.

A large number of providers entered the market. One of those offers – one

App and the system behind it - was able to assert itself with priority. As a matter of fact

something spoke for this system: It simplified the recording of data and the

Handover to the health authorities for the organizers drastic. Simultaneously

it secured the names and address data of the guests by encrypting them before entering

view of the organizers and unauthorized third parties.

For this reason, thirteen of the sixteen federal states decided to do this

Promote the system and recommend the application. The state of Berlin adjusted its

SARS-CoV-2 Infection Protection Measures Ordinance accordingly and reduced
some requirements for the attendance documentation to the organizer
the use of the system in accordance with the provisions of the law on protection against infection
to allow.
A small application grew into an infrastructure for almost the entire federal
desrepublic. According to the operator of the application, installed more than 35
Millions of people the app and use the system. In fact, in many places it was used for
citizens an arduous option to do without the app.
It would have made sense to transfer this infrastructure to the public sector. With
the Corona-Warn-App, which uses Bluetooth signals to identify people
nals of their smartphones and the warning of the contacts upon detection
allowed an infection, the federal government had found an exemplary solution. But at
the system described here, the operation remained in private hands.
39
At the same time, the pandemic and the workload of the health authorities developed
further. With high numbers of infections, it was hardly possible for the health authorities to
To interview infected persons individually and contact persons about the risk of infection
and to inform their resulting obligations. Collected mountains of data
contact the operator of the described system without the health authorities
accessed the data. A number of Berlin health authorities have the software
required to retrieve data from the system was never used productively.
Despite the advice of the data protection supervisory authorities, including our authority,
the legal regulations remained in place, which required the organizers to
that they register the name and contact details of their guests. The Corona warning app
does not record the names and contact details of its users for the purpose of warning
as they are not required for this. Using them alone was the organiser:in-

However, this is prohibited under infection protection law. When updating the infectious

Our authority was not heard of protective regulations.

After increasing criticism of the private operator's system,

under our leadership, the DSK developed three statements on contact

tracking in general and on the system in question in particular. Except-

the DSK spoke out clearly in favor of the opportunities offered by the Corona warning app

and highlighted the advantages of this procedure51.

At the same time, as the responsible supervisory authority, we checked the procedure for

driver of the system and held intensive talks to rectify any identified problems

defects.

A first legal deficiency consisted in the fact that the operator of the system

responsible for the data of the users and process it in the further course

tete without having a legal basis for it. She relied on a contract with

the user, which was designed so vaguely that the data subjects could

couldn't tell what exactly they were getting themselves into. The operator of the system

also reserved the right to change the terms of use and thus the contract and

to unilaterally adjust their authorization for data processing at any time.

51 DSK press release of April 30, 2021; available at https://www.datenschutzkonfe-

renz-online.de/pressemitteilungen.html

A choice for those affected, the data processing on the transfer of the

to restrict the data entered to the organizers concerned

not her.

This does not correspond to the close connection with the processing of data via the

security of persons at events to the purpose of infection protection law,

specified by the legislature. This specification is based on the sensitivity of these

Data that offers a deep insight into the social life of citizens.

From this character of the data and the area-wide use of the method

follow high security requirements. In any case, it became

point of our examination. In the course of the year, the operator

then, however, at different points, the security properties of the used

Systems and services strengthened.

However, the problem remains that the system is highly centralized. It doesn't save

only the data of the citizens. At the time of testing, it also largely controls the

Data processing by the organizers and the health authorities. unauthorized persons who

could gain control of the system, all information would

to disclose through the possibility of manipulating the organisers: inside and

health authority software also the double-encrypted name and address data of the

Citizens.

In addition, in many cases the identity of the persons concerned could also be determined without

Determine decryption. This is because the app often messes with the system of

Operator communicates. The resulting traffic data often allow the

Identification of users of the app. About those identified in this way is then also the

Presence known at the locations where they used the app. Because the

Location and time details are not different from the name and address data of the user

stored encrypted. This communication behavior of the app would not be

necessary: The system has an operating mode with comparatively low

Changes an operation without any communication between the app and the system

operator allowed. The user simply indicates this with their smartphone

a QR code, i.e. a square grid of dots that encodes their contact details

picks up. The organizers read this out with their own app and save it

the encoded data. The submission and verification of digital vaccination certificates with the apps

41

CovPass and CovPassCheck or the Corona-Warn-App show that the prerequisites

tongues are given to the organizers and their guests.

We confronted the operator of the system with the deficiencies and asked them to

submit and work through an action plan to eliminate them.

We have heard of further measures (e.g. a ban on operation) so far, e.g.

Apart from that, in the current pandemic situation, the organizers are not allowed to work

to fulfill their obligations under infection protection law

take. Instead, we continued to influence the operator to make a conversion

to move their system.

However, it is better to use a decentralized system, as is the case with the

Corona warning app is given. The health authorities can also use one

system based on their expertise to control the warning of endangered people and

Gain insight into places with a high risk of infection. The key that

that opens the door to this path is not in the hands of organizers or the

operators of apps, but in the hands of the legislature.

A nationwide system that collects data about the social life of a very large

Number of citizens recorded without giving them a great freedom of choice in the

Use remains, belongs in the public domain. It must be competent from the ground up

and under public observation, data-sparing, with strong earmarking and

be made safety-oriented.

42

Chapter 1 Focus 2 Digital Administration

2.1 Status of digitization projects

The corona pandemic has left the administration behind in digitization for many

positions disclosed. From the point of view of the use of information and communication

on technology in the administration coordinating ICT control at the Senate administration

However, the crisis of digitization also has an impact on internal affairs, digitization and sport

given new impetus. Many central projects are now to be implemented in quick succession

be set. We advise the ICT management intensively with regard to the many

open questions.

A

and

s

i.e

e

right

P

right

a

x

i

s

After the ICT control last year the basic ICT service "digital

trag" into regular operation,52 the project "Digitale

Files" in focus. It is a central building block for modern digital administration and

enables electronic and media-break-free file management and processing.

In accordance with the specifications of the Berlin E-Government Act (EGovG Bln).

this basic ICT service will in future allow document management to be carried out digitally

ments, process processing and audit-proof long-term storage

ensure and thus strengthen the efficiency of the administration.

With the introduction of the "digital file", which is installed at approx. 80,000 administrative
must be made usable, it is a major project. we are from
been involved in the project from the beginning of the pilot phase and advise the ICT control
information on the sometimes very complex data protection issues associated with this.
Projects of administrative digitization like this regularly refer to a very
large number of public bodies at different administrative levels. Also at
of the "digital file" it is first necessary to clarify which participants are responsible for which
data processing operations are responsible and what rights the
affected persons, e.g. B. for information, correction or deletion, to ensure them
have. To assume in general that the authorities involved are responsible for the data processing

52 See 2020 Annual Report, 2.1

jointly responsible,53 leads to considerable difficulties in delimitation
of practice and does not comply with the applicable data protection regulations
bring. The lack of a legal basis for a
Data processing by the Senate Department for the Interior, Digitization and Sport,
where the ICT control is located. It is also important to worry from the outset
responsible for ensuring that the roles and authorizations within the individual administration
genes for access to the personal data processed with the "digital file".
Data are defined in such a way that the data protection requirements
be respected.
As part of our consultations, we have the project managers with regard to
sensitized to these requirements and are still in intensive exchange.
The EGovG Bln, which lays down the legal conditions for the conversion of the administrative
procedures and structures on the use of central information and communication
creates technical structures, obliges the Senate to evaluate the law.54

This took place in May of this year. It turned out that data protection

not perceived as a serious obstacle to administrative digitization

men will. That's what the officials interviewed for the evaluation called the

Data protection only in 7th place out of 11 possible obstacles to administrative digitization

ization.55 Instead, they pointed primarily to the lack of centrally developed IT solutions

genes and standards, a lack of budgets and a lack of digitization skills

towards the employees.56 In practice, data protection is different from what is often portrayed

So not the big stumbling block in the digitization of administration.

i. S.v. Art. 26 General Data Protection Regulation (GDPR)

53

54 § 26 EGovG Bln

55 See "Evaluation of the Berlin E-Government Act" of May 21, 2021, p. 48 f.,

Berlin House of Representatives, H-18/2765.E; https://www.parlament-berlin.de/

adosservice/18/main/process/h18-2765.E-v.pdf

56 See "Evaluation of the Berlin E-Government Act" of May 21, 2021, p. 178,

Berlin House of Representatives, H-18/2765.E; https://www.parlament-berlin.de/

adosservice/18/main/process/h18-2765.E-v.pdf

With the introduction of the "digital file" in administration, many data

protection challenges. It is important that ICT governance and

administrations involved use the pilot phase to

implement requirements. We support this process with our advice.

2.2 Use of video conferencing systems

Video conferencing systems were also of particular importance this year

the functionality of the administration and the economy in times of the pandemic

to maintain. We have our support for those responsible at the

Selection of data protection-compliant services expanded, but also due to procedures

the use of illegal video conferencing services. While we at man-

chen providers have been able to make significant advances in data protection law,

we had to do when using video conferencing systems in administration

often identify significant violations of the law.

A

and

s

i.e

e

right

P

right

a

x

i

s

Our "Notes for Berlin Responsibilities", which were published for the first time last year

Information about providers of video conferencing services” was updated this year

and expanded.57 A pleasing result was that we - after sometimes very extensive

chemical exchange and extensive changes among the providers – now in total

including eleven providers on the legal level through the proven traffic light system

rated “green”. We then have this subjected to a technical test

subjected. Also with other providers who were ultimately not rated “green”.

we were able to achieve significant, albeit insufficient, improvements.

On the technical level, the information is now clearly differentiated and

sen different use cases. For three different scenarios, sub-

take, authorities and clubs recognize at first glance which of the tested

Video conferencing services come into consideration for them: There is one for every use case

own traffic light. For each of the 23 tested services or service groups

the paper also contains some very detailed explanations of the deficiencies and information on

Configuration.

57 See https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientation aids/

2021-BlnBDI-Notes_Berliner_Responsible_to_Providers_VideoconferencingServices.pdf

We also have a very extensive administration when it comes to tendering for

Successors of the previous centrally procured video conferencing solutions under-

supports. While this collaboration has been very constructive and successful,

we have no possibility in cooperation with the Senate Chancellery and the ICT control

find one of some Senate Departments and the Senate Chancellery in various

forms used cloud service legally compliant. We have the concern-

the senate administrations and the senate chancellery then asked to stop using it

set. They weren't ready for that. The Senate Chancellery as negotiator

but offered technical and organizational changes to make a transitional

achieve a tolerable design. The relevant talks could

reference period has not yet been completed. In contrast, the “learning space Berlin” uses

now a data protection-compliant video conference system.58

There are a variety of legally compliant video conferencing services for the different

most practical purposes. The corona pandemic cannot prevent the use of

justify services.

2.3 Implementation of the Online Access Act in the federal government

and countries

s

i

x

a

right

P

right

e

i.e

s

and

A

The federal, state and local governments are implementing the Online Access Act

(OZG) continues to be under pressure.59 By the end of 2022, they must transfer their administrative services

Also offer administration portals online. The identified 575 to be digitized

Administrative services are assigned to the individual federal states according to subject areas

arranges. Digitization is carried out based on the so-called "one-for-all principle".

zip" ("OfA principle"). This means that each federal state has administrative services

digitized from his subject area in such a way that the developed solutions differ from the

whose federal states can be adopted and used.

Since data protection issues in connection with the OZG implementation, all federal states

and thus also affect all data protection supervisory authorities, the conference has

the data protection officer of the federal and state governments (DSK) in autumn 2020

58 See 1.2.3

59 See also 2020 Annual Report, 2.2

Sub-working group tasked with dealing with the data protection issues that
in the development of administration portals and other specialist applications
provide, deal with and evaluate and at the same time an exchange with the Federal
Ministry of the Interior and Homeland and Federal IT Cooperation and
to act in a coordinated manner. We have been actively involved in this working group from the very beginning.
As part of the implementation of the OZG, the State of Berlin, together with the Federal Ministry
Ministry of the Interior and for Homeland and the states of Brandenburg, Hamburg and Thü-
are responsible for the topic of "cross-sectional services". In this area
most recently, the "basic component verification retrieval" was developed. This sub-
supports a digital and media-break-free provision of evidence when applying
of administrative services. Both citizens and companies should
Possibility to provide the authorities with certain evidence, e.g. B. a birth certificate,
a registration certificate or a certificate of good conduct, to be provided electronically. With
the "Basic component verification retrieval" should be possible through the connection
of application and specialist procedures with the corresponding registers via a
to enable a central service. We have the ICT control at the center
Within the framework of the realization of this project, our support
offered.
Another project presented as particularly innovative as part of the OZG
The requirement is the “digital school certificate”. As part of a pilot project60 in Ber-
lin the solution developed by Saxony-Anhalt together with Bundesdruckerei
to digitize school reports. With this project it should
educational institutions are enabled to provide forgery-proof digital certificates
to create. Blockchain technology is used for this. basis is

thereby creating a public blockchain used exclusively by those in the cooperative
"govdigital" connected public data centers is operated. project manager
In addition to the Bundesdruckerei in Berlin, the Senate Department for Education,
youth and family, as well as the IT service center, which us at an early stage
involved in the project.
60 In addition to Berlin, the federal states of Rhineland-Palatinate and North Rhine-West-
fall involved.
47
The Senate Department for Education, Youth and Family approved the project in October
received the Berlin administration award in the innovation category. This has us
amazed, because the legal requirements for the start of the project are currently in place
not yet available: According to current legislation, the issue of digital certificates is
situation both in terms of school law61 and administrative procedural law62 in Berlin
closed, what the education administration told us about. was granted. Also missing
currently the complete technical documentation of the project.
In addition to creating the necessary legal basis is in technical terms
to consider that the data stored in a blockchain, independent
of who operates them can never be erased. So it has to be
be made sure that the data subjects exercise their right to erasure or rectification
of their personal data. The project planning sees this
before, the personal data contained in the certificates only as a "hash
values", i.e. H. as cryptographic checksums, stored in the blockchain. We are
It is important that those responsible for the project evaluate exactly whether the data
later point in time cannot simply be guessed by trying it out and thus the respective
gen persons can be reassigned. Since in the blockchain used
which "govdigital" all parties involved trust by definition, costly

Various test methods when creating a new block. With this, the blockchain
ultimately only used as a simple database. So the question arises
what added value the new process brings from a technical point of view and whether
from supportable goal of making the school reports available digitally
cannot also be achieved with the digital signature provided in the concept anyway
leaves. We will continue to support the project and stand by the project managers
tively on hand, but expect that the necessary legal prerequisites
be created now.
The OZG implementation is also a special one in terms of data protection law
challenge. We are convinced that a successful administrative
gitalization can only succeed if citizens are safe from the start

61 See Section 58, Paragraph 2 of the Education Act (SchulG)

62 See Section 2, Paragraph 2, Clause 2 of the Berlin Administration Procedures Act (VwVfG Bln)

can ensure that their personal data is handled with care. The
Creating transparency is of particular importance in order to
trust when using digital services.

3 Home and Sports

3.1 Police transmit illegally meeting dates

Two formal complaints vs. the police are in a single investigation
a novelty. Unfortunately, we saw each other because of the lack of cooperation
the police and a blatantly illegal data transmission by the police
compelled the administrative court to do so.

s

i

x

a

right

P

right

e

i.e

s

and

A

The reason for our test procedure was the report of a data breach by the police,

in which she informed us that she was being sued in an administrative court

risk assessment together with the relevant administrative

had sent to the administrative court in unredacted form.

The media had previously reported that the relevant police files

Lawyer in the course of an inspection of files at the administrative court

the be. The lawyer had on behalf of his client in connection with

sued at a meeting. According to media reports, when he inspected the files

Gain insight into the data of those registering counter-demonstrations.

As a result, the police answered our questions about the data breach report and shared

also stated that the report was only made as a precautionary measure due to the media reporting

approval was made, but the data was transmitted to the administrative court for admissible

be deemed significant.

From the replies of the police it was clear that in the administrative

gen sent risk assessment data from people who are similar

meetings and counter-meetings had registered or for the leadership

scheduled for such gatherings were included. In addition to pre- and

Men, this concerned police findings on these people. For example,

leads, whether and if so, which general criminal law and state security relevant

Information about the persons concerned is available. In addition, there were

The appraisal assessment contains data of other people that the police are connected to

3.1 Police unlawfully transmit meeting data

the registered meetings, because they used to have similar meetings

genes or as supporters of the registered meetings

were valid.

Aside from the threat assessment, those sent by the police included that

Files sent to the administrative court, e.g. also the e-mail of the applicant of an in-

event that is not related to the subject matter of the dispute;

Name, address, date of birth, phone number and email address of a whistleblower

bers on the disputed meeting as well as the name and e-mail address of one

media representative.

For a final assessment of the legal situation, we then asked the police

often in vain to send the statement of claim. The police finally informed us

that she unfortunately could not comply with our request because she was not the author of the

requested statement of claim and is therefore not entitled to submit it. Furthermore be

the document is not part of the files sent to the administrative court.

Here we had to make the first complaint:

The police are legally obliged to provide us with all information necessary for the fulfillment of our

our tasks are required to provide.63 There is also an obligation to work with us

to work together in the fulfillment of our tasks.64

hears it to monitor the application of the rules on data protection and

enforce and investigations into the application of the regulations on the

data protection.65 The statement of claim is required to fulfill these tasks.

derlich, because for the legal assessment of the legality of the data transfer

knowledge of the subject-matter of the dispute arising from the statement of claim is decisive.

The legal obligations of the police to provide this information as well as

for cooperation are not limited by any third-party authorship

this information. Following such a logic, it would also be for us in many

cases hardly possible to verify the legality of data processing by responsible

63 Section 13 (4) No. 2 BlnDSG

64 § 54 BlnDSG

65 Section 11 (1) sentence 1 no. 1, 8 BlnDSG

to be checked because the information available there in the form of sub-

often have authorship outside of these bodies. You come to the test

Checking the lawfulness of data processing cannot be avoided, either

to receive information of third-party authorship. Accordingly, far has the law

give our powers.

The police finally saw this and as a result of our complaints

application sent a copy of the statement of claim.

Now we were able to legally assess the data transfer described,

which led to the second complaint:

The sending of the files by the police to the administrative court without prior

redacting of the personal data described in the facts

unlawful.66

In particular, such a data transfer cannot be based on Section 99 (1) Administrative

court rules (VwGO) are supported. According to this standard, authorities are

the competent administrative court for the submission of documents or files, for the

transmission of electronic documents and is obliged to provide information. However, this can

be refused if the disclosure of the content is in the interest of the federal government or

of a country would cause disadvantages or if the operations are carried out under a law

or must be kept secret by their very nature.

According to their nature, grds.67 personal data of third parties are to be kept secret,

the documents to be transmitted for various reasons and in different

be mentioned.68 However, it is also undisputed that in the

in connection with the reference to an inherent need for secrecy

a strict standard is to be applied, because through this the judicial clarification and

law-finding activity is restricted.69 Therefore, careful consideration is required

66 Violation of Section 32 Paragraph 1 No. 1 BlnDSG i. V. m. § 99 paragraph 1 Administrative Court Code

(VwGO)

67 i.e. in general, which allows exceptions

68 st. Rspr., cf. BVerwG, decision of April 19, 2010 - 20 F 13/09, para. 22; BVerwG,

Resolution of July 28, 2015 - 20 F 3.15, para. 16 with additional evidence

69 See Schoch/Schneider VwGO/Rudisile VwGO § 99, para. 18 mwNw

Chapter 3 Internal affairs and sport 3.1 Police illegally transmit meeting data

of confidentiality interests with those in connection with the court proceedings

Existing information interests, taking into account the entire facts of the case

to be carried out on a case-by-case basis.70

In the present case it is already extremely doubtful whether a judicial

interest in the personal data of persons transmitted by the police,

who have registered similar meetings and counter-meetings

or had or were intended to lead such meetings.

For the assessment of the subject matter of the dispute, it could be of interest whether

meetings and counter-meetings held at the same time

were reported and the course of these gatherings based on earlier police reports

cher knowledge was to be expected. However, it is usually not necessary to know

which first and last names the registering or leaders of other meetings

and to which specific persons police findings are assigned.

In this respect, regularly anonymized information is sufficient. In the present case,

added that the subject matter of the dispute has no direct connection to other meetings

had lungs.

The same considerations also apply to data from people who, for example, used to be

had registered similar gatherings or as supporters of the registered

the meetings were valid. At best, in individual cases personal

drawn data in connection with the disputed meeting of

be interested. With regard to the other data of third parties, the Ver-

recognizable by the administrative court.

Even if it were to be assumed that those described in the facts

personal data of those registering at other meetings and at the

other third parties connected with these meetings an abstract

there is a judicial interest in information, the interests of the

affected by the secrecy of their personal data.

First of all, it must be taken into account that people who hold meetings

want to lead or are legally obliged to report this to the police beforehand

70 See BVerwG, decision of January 10, 2017 - 20 F 3.16, paragraph 10

to register. You can therefore regularly participate in a survey and further processing

processing of their data by the police if they exercise their fundamental right

to exercise freedom of assembly. To a purpose-changing processing

For these reasons alone, high standards should be set for this data.

In addition, for the personal data in connection with

demonstrations to the disputed meeting in the police

administrative processes are stored and from the police to the administrative court

were transmitted, there is a general risk that they could be inspected through file inspection

of the plaintiff or third parties reach unauthorized persons and

Those affected may be exposed to personal persecution as a result.

In this respect, for example, reference is made to so-called lists of enemies, in which data of unpopular

sons collected and some with explicit or subtle threats or

Notes are mainly published on the Internet.

It should also be noted that information on political opinions resulting from the registration

education or participation in meetings, to the categories special

of personal data and are therefore particularly worthy of protection.71 Also

From the point of view of those affected, findings relevant to criminal law and state security can

be very sensitive, which is why the interest in secrecy weighs heavily in this respect.

Furthermore, it must be taken into account that the persons concerned are not themselves involved in the disputed

general meeting as well as the related court proceedings, the

regularly not report on the processing of their data in this context

are informed and therefore cannot exercise their rights as data subjects.

It should also be noted that this was a meeting that happened in the past

has. In this respect, the court proceedings were not urgent. A request from

required personal data by the court would be at a later date

time was possible without any problems.

The police showed up with the complaint with regard to the data transmission

to the administrative court, but informed that the case

occasion had been taken to sensitize the employees again,

71 See § 33 i. in conjunction with § 31 No. 14 BlnDSG

to check very carefully in each individual case in future whether

current data of third parties before the transmission of administrative processes to courts

need to be blacked out.

3.2 Right to information vis-à-vis the police without ID copy possible

Every person should basically be able to find out what data the police have

she saves. The Berlin Data Protection Act provides for such an information procedure

(BlnDSG). Last year the administrative court ruled on a case

which now simplifies this procedure for citizens.72 The police have so far -

according to their own statements to prevent fraud - requests for information only processed,

if the citizens had attached a copy of their ID to their application.

A

and

s

i.e

e

right

P

right

a

x

i

s

According to the case law of the Administrative Court, however, the police may only

request additional information if there are doubts about the identity of the data subject.73

We pointed this out to the police and asked them to do the previous

change the application process. There we were assured that in the future only in

In case of doubt, a copy of your ID will be requested. Since the law “established

Doubts” calls for the police in these cases to also be able to raise their concerns

to be able to explain.

The police had planned to speed up the processing, in cases of doubt

to carry out a registration query via the IT procedure for residents (EWW). Here-

however, there is no legal basis for this, as the law only allows information

to be requested from the person concerned74. Such a query would also not be

necessary. If a data subject reports, stating their name and

home address, should the data already stored by the police

point to the correctness of the information contained. A confirmation of receipt of the application

can - if the address is given - also without prior identity check

sent, as this usually does not reveal any sensitive data.

72 VG Berlin, judgment of August 31, 2020 - VG 1 K 90.19

73 See Section 45 (4) BlnDSG

74 See Section 45 (4) BlnDSG

If an affected person reports without address data, but there are other contact channels

If necessary, you may be asked to submit address data later. Should reasoned

Doubts must be documented and the person concerned should not, despite being asked to do so

If you provide further data for verification, the application can of course not be processed further.

be worked.

For information rights vs. to assert the police regularly does not have to

Copy of ID will be presented. An informal letter is sufficient. It is

Of course, it is still appropriate to provide information that allows the location of the

also allow stored data. The information is free of charge.

3.3 How anonymous are the police information portals?

s

i

x

a

right

P

right

e

i.e

s

and

A

The introduction of an anonymous whistleblower system by the tax administration in

Baden-Württemberg has nationwide for discussions about the pros and cons of

reporting portals of public bodies on the Internet. In this context we have

menhang asked the police how anonymous their offers to report

possible violations of the law.

The “internet watch”, the “anonymous

Whistleblower system” and the “Berlin whistleblower portal”.

The "Internet Watch" makes it possible to report, to give tips, but also

Ask questions, register meetings or file complaints. Here-

for the users do not have to provide any personal information other than the notice they want to give

specify personal data. Each entry is checked by a police officer

further processed, who can ask if necessary, if voluntary contact details

have been specified. The collection and storage of your IP address must be

Zer:innen by setting a tick on the "Internet Watch" page, however

agree if you want your entry to be processed. Using the IP address, the

Police if there is reasonable suspicion of a criminal offense or in the event of certain dangers

Court order to determine the owner of the connection through which the

information was given if this information was used to clarify the facts

is required.75

The police would like information on corruption via the “anonymous whistleblower system”.

make possible. In principle, whistleblowers do not have to provide any personal information

Enter wisely so that the process is processed. For further inquiries from

investigators can set up their own mailbox, which can only be accessed

certain investigators should have access.

The "Berlin information portal" is only activated temporarily. The last three occasions

at the time of our inquiry there were calls for witnesses to an attack with a

a broken bottle, to a bank robbery and to a robbery

money transporter.

In the last two systems, complete anonymization stands for the police

of offers in the foreground. The police assured us that if the

"Anonymous whistleblower system" and the "Berlin whistleblower portal" do not have IP addresses

be stored by users.

3.4 Disclosure of a Complainant's Data

to the person affected by the complaint

Employees

When dealing with a complaint against a police officer, the

Complaint to the employee concerned along with the personal

data of the complainant have been passed on.

Citizens can inform themselves about the behavior of employees at any time.

Complaints about authorities - that is about the right of petition in the Basic Law (GG)

guaranteed.76 In the case of civil servants, the law stipulates that they

statements and reviews that are unfavorable to you or become disadvantageous to you

A

and

s

i.e

e

right

P

right

a

x

i

s

75 See § 100j Code of Criminal Procedure (StPO)

76 See Art. 17 GG

are to be heard before they are included in the personnel file.77 Regardless of this

it may also be necessary to pass on the content of the complaint if such a

Change in behavior or a rethinking of one's own position in terms of the

deführer:innen can be initiated.

In order to enable employees to recognize the facts in question

ing, it may also be permissible to identify the name of the complainant

to let - but here, too, special circumstances can speak against it.

However, it is not necessary to regularly - as in the present case,

hen - the transfer of contact details, such as home address and telephone number of

complainants. The current business instructions of the police for handling

with complaints does not provide for any blacking out of personal data. The

we have complained.

The police complaints offices and the central complaints management

ment took immediate action to collect data from the complainant:in-

protect them better in the future. The police promised us the relevant

to revise business instructions in our interest.

3.5 Lack of identification of applicants

Person in the online application of

simple registration information

s

i

x

a

right

P

right

e

i.e

s

and

A

Due to a citizen complaint, we have the online procedure for granting

checked by simple population register information from the population register. A citizen

had found that the state office for civil and regulatory affairs

(LABO) provided information from the population register based on an inquiry about him

and thus his personal data is transmitted to the requesting person

had. As part of their request for information online, this person had evidently

incorrect personal details given. So the applicant or the applicant as

77 Section 86 State Civil Servants Act (LBG)

Name "Mickey Mouse" and address "12345 Disneyland, Mausstrasse 1, Demokra-

tic People's Republic of Korea".

In principle, the federal legislature has the basis in the Federal Registration Act (BMG).

created so that private individuals or private bodies, such. B. company, on

application for information from the population register.78 Accordingly,

authorities, for example, issue a so-called simple registration register information on a person

including surname, first name, doctoral degree, current address and

if the person is deceased, communicate this fact to a private third party.79

The simple population register information can also be sent electronically or by

automated retrieval via the Internet.80 In Berlin there is an online

line procedure for applying for and issuing simple information from the register of residents

(Online population register information - OLMERA), which is operated by LABO. Over
a website can provide information from the current database of the population register
be applied for.81
Non-registered users can also obtain information via the online application
obtained from the population register. So far, this was designed as follows: If the
or the user assured by selecting the appropriate text field that the
information provided is not used for commercial purposes, he or she was informed
an input mask in which personal information had to be entered.
There the applicant had to provide the following information about
state: surname, first name, postal code, city, street and house number. Additionally
the country and the e-mail address could be entered.
So far, however, neither an identity check nor a plausibility check has been carried out
with regard to the data given. It was therefore also not checked whether the
questioning person has entered their personal details correctly or whether they are fictitious requests
gifts acts. The Federal Ministry of Health does not contain any specific regulation on the question of whether and

78 See §§ 44, 45 BMG

79 The conference of the independent data protection supervisory authorities of the federal and state governments
(DSK) has the fundamentally possible issue of
Information from the register of residents has already been criticized several times; See, for example, the resolution of the DSK
from 8./9. March 2001 to amend the Registration Law Framework Act.

80 See Section 49 (2) BMG

81 https://olmera.verwalt-berlin.de

if so, how to identify the person requesting information from the population register.
From the general administrative regulation for the implementation of the Federal Registration Act
zes (BMGVwV), the information and explanations for the application of the individual

contains the provisions of the Federal Ministry of Health, but it is expressly stated that within
The automated population register information requires an identification of the requesting party
person or body.82 Accordingly, the identification of the inquiring
person or entity required. Natural or legal persons involved in the das
Registered persons are registered through their access identifiers
identified. If there is no registration, inquirers are informed by specifying the
Name, address and, if applicable, date of birth.
Also against the background of the data protection right to information83 or to fulfill
fulfillment of the duty to provide information affected persons, whose data in the course of a
were passed on to the population register, an identification must be
tion of the querying person. For proper disclosure of information
and to enable data protection controls, the information in the context
the person or office requesting the automated information from the register
lated.84
After all, as part of the automated retrieval process, the identity of the
requesting person or body can be verified on the basis of certain information. This
means that the online procedure must be technically designed in such a way that the
Information from non-registered OLMERA users is checked and an automatic
In any case, information from the population register will not be provided if the identity is not
can be checked. By the LABO as part of the online procedure OLMERA
had not provided sufficient identification of the applicants,
has it against the obligation to comply with technical and organizational measures85
violated We have vs. LABO therefore issued a warning and it
prompted to adjust OLMERA accordingly.

82 See 49.0.1 BMGVwV

83 According to Art. 15 General Data Protection Regulation (GDPR) i. in conjunction with § 10 BMG

84 See Section 49 Para. 6 BMG i. in conjunction with § 40 BMG

85 Pursuant to Art. 5 Para. 1 lit. f GDPR i. In conjunction with Art. 32 (1) GDPR

As a result, the LABO has the technical advancement of the manufacturer at the manufacturer
Application OLMERA commissioned and internally involved in the technical integration of the new
solution that has since been implemented. Since December 1st, 2021
a person who wants online information from the civil register must use the
eID function of the new ID card (nPA), the electronic residence permit
(eAT) or the eID card for Union citizens. The basic service is used for this
eID used by the Senate Department for the Interior, Digitization and Sport
is responsible.
In particular, to guarantee individual rights of those affected, such as the law
on receipt of data protection information, it is necessary that reporting
Authorities identify the recipients of population register data and their
log data. This must be done when issuing information from the register of residents
Using an online application, it is technically ensured that the information
to verify the identity of the applicant before they issue an
comes from the population register.

3.6 Data processing in connection with parliamentary elections

Personal data is processed in connection with parliamentary elections
of the voters by various responsible persons, e.g. B. Authorities and parties, too
processed for different purposes. Since September 26, 2021 in addition to the
the general election of the German Bundestag in Berlin, also the elections
of the Berlin House of Representatives and the district assemblies as well
how a referendum took place, we already knew in the run-up to election day

intensively involved with the data processing and information material for the

public.86 In addition, we are particularly in the weeks before and

followed up numerous complaints from citizens after the elections.

A

and

s

i.e

e

right

P

right

a

x

i

s

Due to a request from the state returning officer, who is responsible for the proper

preparing and conducting all political elections as well as for the determination and

is responsible for determining the official election result, we have already established ourselves

86 See the guide “Election advertising by political parties”; available at

https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/wahlwerbung

dealt with two online forms specially designed for elections at the beginning of the year

– the "Online application for polling cards" (OLIWA) and the "Online registration of

Election workers”, which takes place via the OLAV application. Via OLAV, elective

register helping hands and via OLIWA there is the possibility for citizens entitled to vote

ger:innen to apply for a polling card or to request postal voting documents.

Both online services process personal data because the user

Zer:innen to apply or to register as election workers:innen information on their own

a person who must then submit it to the responsible public authorities

be transmitted. The data processing can be carried out in particular on optional

legal regulations such as B. the Federal Elections Act (BWahlG) and the Federal Elections

ordinance (BWO) as well as the state election law (WahlG) and the state electoral regulations

(LWO), are supported. If, however, over the legally determined data

In addition, further data of the persons concerned must be collected for this purpose.

sufficient consent to be obtained. Then we have the state returning officer

pointed out and requested that the data to be provided voluntarily in the online

applications OLIWA and OLAV must be clearly marked as such.

Furthermore, we have the adjustment of the data protection declaration stored there

required. In this must u. a. be explained transparently and comprehensibly, for

the purpose for which the data is collected and that the processing is subject to consent

based.87

Furthermore, in connection with this year's parliamentary elections, we

len primarily - due to numerous complaints - with the processing of

Data of citizens eligible to vote for the purposes of election advertising. Here-

at is between the transmission of data from the electoral register by the

LABO to parties and other authorized recipients as well as further processing

processing of the data by these recipients.

The Federal Ministry of Health allows the registration authorities to register political parties, voter groups

and other sponsors of election proposals in the six months before a party

may provide information from the population register.88 The sponsors of a

Popular initiatives and a people's and citizens' initiative may also request data.

87 This follows from the transparency and information obligations under Art. 12, 13 GDPR.

88 § 50 paragraph 1 sentence 1 BMG

The information from the population register may only be used for the purpose of voting

exercise.89 The data obtained through the information from the register of residents

must also no later than one month after the day of the election or voting

be deleted or destroyed again.90 In individual cases, the provision of information must

stay if there is a block on transmission for a specific person entitled to vote

due to an objection, a conditional blocking notice91 or a blocking of information92

entered in the register of residents.

The reporting law also stipulates that the information should only be given about individual age groups

may be granted. It is therefore not permitted to transmit the data of all of them

eligible voter. The restriction to age groups often coincides with the

Ideas of the parties, e.g. first-time or young voters or senior

aims to be able to address the respective age group with topics. Since at the

compilation of the groups of people about whom information is to be provided, by law

age alone is another selection or search criterion,

such as B. religious affiliation or gender, not permitted.

Before the elections, many parties were aware of this particular case of registration

terauskunft made use of and the LABO to the transmission of the data from

certain groups of eligible voters. When reviewing this

So far we have not been able to detect any data protection violation of the

determine LABO. The data was transmitted in accordance with the legal requirements

ben.

However, in some cases we have found that parties in further

processing of the requested data for election advertising purposes against data protection laws

violated regulations.

If parties send election advertising letters to the addresses received,

at the same time provide the recipient with certain information about the data

provide work. Among other things, it must be easy for the recipient

89 Section 50 (1) sentence 3 BMG

90 Section 50 (1) sentence 3 BMG

91 See Section 52 BMG

92 See § 51 BMG

be recognizable who is responsible for the data processing and how they

responsible persons can reach. The parties must also inform

from which source the address data comes and when it will be deleted again.

If the data is disclosed to service providers during processing,

The parties must also make this transparent, stating the recipients.93

This information was not included in all campaign advertising letters that Be-

criminal leaders were submitted for examination.

In one case, it was not even clear who was responsible for data processing.

was responsible. The party had made the election campaign letters look like

dele it concerns personal election recommendations from publicly known private

sons. For many recipients, the impression was created that the party had

passed on their data to the supposed senders of the letters, what

would be inadmissible. However, this suspicion has not changed in the course of our investigations

confirmed. Rather, the party, in consultation with the alleged sender

designed the letters and sent them yourself or with the help of a service provider.

Parties can opt out of sending election advertising letters to professional service providers

service providers if they have an effective order processing

conclude a contract.94 It is important that the service provider: in the her/him

transmitted personal data exclusively on behalf of and on instruction

of his/her client may process and after

execution of the order must be deleted again. This leaves the parties themselves

responsible for processing the data. The service providers are allowed to use the data

never use it for your own purposes or with the data of other contractors

bring donors together.

Here, too, we had to realize that not all parties had corresponding agreements

agreements with their service providers before submitting the address data

passed them on. So far, however, we have no evidence that

Service providers actually do not have address data that they have received from parties

deleted again and/or used for other purposes.

93 The list of all information that the parties must provide can be found in

Art. 14 para. 1 and 2 GDPR.

94 See Art. 28 (3) GDPR

Even if in connection with the preparation and implementation of

lamentswahl certain data processing by authorities and parties

are permitted due to special legal regulations, the responsible

lichen strictly pay attention to the scope of the processed data and the purpose

to limit the processing in accordance with the regulations. With regard to the

Transparency obligations can be found in the general provisions of the General Data Protection

ordinance (GDPR) also applies in these cases.

3.7 Publication of photos and other data

sports club website

Having your own website is an important opportunity for many sports clubs

represent club life and for the respective sport(s) as well as a club member

to recruit membership. However, affected persons turn to them again and again

us and complain about the publication of their personal data

on the website of a sports club. When examining these entries, we

regularly finds that there are still ambiguities in the clubs as to whether and

which data may be placed on the association's own websites.

A

and

s

i.e

e

right

P

right

a

x

i

s

The publication of personal data on the Internet is a data transfer

communication to an unlimited group of people, since websites are generally available worldwide

can be called. This results in risks for those affected, because the

published information can be researched by anyone and, for example, also to

Advertising purposes and for profiling are evaluated. A special danger

also results from the fact that the data can also be accessed in countries

in which the GDPR or comparable provisions do not apply.

One possibility of a lawful publication is to get rid of those concerned

To have people (association members, third parties) give their consent. while having to

the legal requirements for effective consent are observed.95

In particular, the consent of the data subject must be based on their free decision

education. The person must do this beforehand sufficiently and understandably about it

be informed which data the association intends to process and for what purpose. To

95 See i.a. Art. 6 (1) sentence 1 lit. a, Art. 4 No. 11, Art. 7 and Art. 8 GDPR

It should also be noted that the consent can be freely revoked at any time for the future.

The person concerned should also be informed of this. A special shape

the consent is not provided for in the GDPR, so that the consent is both

in writing as well as electronically, verbally or impliedly. Due to the

However, the association should obtain written consent or the

Document the submission of consents in another way.

Personal data may also be published without the consent of

affected person if there is another legal basis for this. in

On the one hand, Art. 6 (1) sentence 1 lit. b GDPR applies here if the data processing

to achieve the purpose of the association or the membership relationship, in particular

special for the administration and care of the members is required. On the other hand

a publication of the data on the basis of Art. 6 Para. 1 Sentence 1 lit. f GDPR

GMO possible if the association or a third party has a legitimate interest in it,

and unless the interests or fundamental rights and freedoms of those concerned

person outweigh. However, the association must carefully examine this in each individual case.

For example, data from officials of an association, such as the name, the

exercised function and the association-related availability (telephone number/e-mail

address), regularly published on the website without express consent

be public, since the interest of the association in a comprehensive and complete

External presentation or the possibility of contacting the interest

of the individual basically predominates. For the publication of the private address or other

terer private contact details is a consent of the functionary or the

officer required. Furthermore, sport-related information,

such as B. match results and reports, team rosters and personal

Services are published on the website without the consent of the person concerned

if there are no conflicting interests of the data subjects that are worthy of protection

and they have been sufficiently informed in advance97. In addition,

ensures that the data is deleted after a reasonable period of time. At

the assessment of the permissible duration of the publication is above all the importance

of the event to which the publication relates, since

from which the public's interest in information is derived. When considering the

96 See Article 7(1) GDPR

97 See Art. 13 GDPR

Interests of the association or the public with the interests of the person concerned

is primarily decisive as to whether it is a public event of the

club or association and the names and the results usually

also be made public. If this is the case, this speaks grds.

to ensure that the data can be published.

When publishing photos and other personal data

Sports club websites should be used with caution. Those responsible have to

carefully check whether express consent needs to be obtained, or

whether the publication is otherwise based on a legal basis

the can. In any case, only data required for the respective purpose may be

be published online.

67

4 Justice and

legal profession

4.1 cell query transparency system finally

in action

To clear up particularly serious crimes, it is possible under certain conditions

permissible to carry out so-called radio cell queries.98 Here, criminal prosecution

authorities of telecommunications providers: inside information about the connection data

of all mobile phone calls made in a given time in a specific

area have been conducted require. Those affected often find out nothing about this.

Radio cell queries access the constitutionally protected telecommunications secrecy

nis99 and affect a large number of people who have no reason to carry out such

cher measures have given.

In 2012, we therefore stopped the practice of radio cell queries by criminal prosecutors

checked by the authorities and various deficiencies were found.100 In many cases, this was not done

For example, the legally required notification of those affected, so that they

could not exercise any legal protection.

At that time, the House of Representatives requested the Senate based on our audit results

nisse u. a. on, a generally accessible information of the public about time and

location of a radio cell query.101 As a result, the Senate Administration

started a corresponding project for the judiciary, which we are closely

slides and supported.

98 See Section 100g(3) of the Code of Criminal Procedure (StPO)

99 See Article 10 of the Basic Law (GG)

100 See Annual Report 2012, 2.1

101 See Annual Report 2013, 5.4

4.2 Right to information from the examination file in legal training

The radio cell query transparency system (FTS) developed in the project is in place

now available to all interested citizens.102 According to current

In its current state, the system meets the data protection requirements and is a

great gain for the rights of those affected.

4.2 Right to information from the examination file in the

Lawyer:internal training

The Joint Legal Examination Office of the States of Berlin and Brandenburg (GJPA)

enables access to the legal state examinations

handwritten supervision work and the evaluation sheets of the examiners

on site. In times of the pandemic, of course, this often had to be dispensed with. copies

of the examination files can only be requested against reimbursement of costs.

The exact content of the self-written exams is particularly important for candidates

dat:innen, who want to understand their evaluation or do not take an exam

have stood. The results of the exams have an impact on many candidates.

effects on the entire subsequent working life.

A

and

s

i.e

e

right

P

right

a

x

i

s

The General Data Protection Regulation (GDPR) stipulates that bodies that

process related data, provide information about them free of charge and free of charge

must provide copies of the processed data.103 As a right of the European

nian Union, this provision supersedes different regulations in the member

States basically before, because otherwise there would be a risk that Union law in the

member states applied unequally or not at all, which in turn dem

would run counter to the purpose of European integration.104

The GJPA appeals to the information procedure it uses

a provision of the Berlin Lawyer Training Act (JAG),105 which governs the application

the DS-GVO should exclude and does not consider the DS-GVO to be applicable in other respects either.

102 https://fts.berlin.de/

103 Art. 15 (3) GDPR

104 The so-called application priority, which arises from the effet-utile principle, is permanent

decision of the European Court of Justice (ECJ).

105 § 23 JAG

However, since the result of the test i.a. also decides whether the candidates

dat:innen also practice their later profession in other member states of the Union

can, the processing of personal data falls for this reason alone

under Union law. The European Court of Justice (ECJ) has already ruled

that exam answers and scores are considered personal data even then

apply if the documents are processed under a reference number.106

Why the free sending of copies of the GJPA when conducting

The examination office was not able to explain to us convincingly that examinations are affected. The

Information about processed data is one of the tasks of authorities in contact with

Citizens. Proper implementation is the responsibility of the person responsible in each case

Job. Fiscal interests must be taken into account when fulfilling a task

resign regularly within the framework of fundamental rights.

We have therefore initially warned the GJPA in an individual case that further supervisory

we reserve the right to take legal action in the future.

According to Art. 15 DS-GVO, candidates for legal examinations are entitled to

free information from their examination documents as well as free copies. This

has meanwhile also been decided by a court.107

4.3 Implementation of the JI Directive in prisons

With a delay of more than three years108, the Berlin legislature has now passed the so-called

JI Directive109 in the data protection law of the penal system, the social services of the judiciary

tiz and the management supervisory body at the regional court.110 The Senate administration

tion for justice, consumer protection and anti-discrimination, the corresponding

106 CJEU, judgment of December 20, 2017 – C-434/16, “Nowak”

107 OVG North Rhine-Westphalia, judgment of June 8, 2021 - 16 A 1582/20; not yet legally binding

108 The legislature would actually have had this obligation pursuant to Article 63 (1) sentence 1 of the JI Directive until

by May 6, 2018.

109 Directive (EU) 2016/680 on the protection of individuals with regard to the processing of personal

obtained data by the competent authorities for the purpose of prevention, investigation,

Detection or prosecution of criminal offenses or the execution of sentences as well as for free

transport and repealing Council Framework Decision 2008/977/JHA (JHA Directive)

110 See Abghs.-Drs. 18/4032

prepared the draft law, involved us at an early stage and gave us the opportunity to

given opinion.

Among other things, we were able to achieve that, in the event of a decision to defer

Restriction or omission of notification of the data subject about

processing of their data in accordance with the requirements of the JI Directive111 in each individual case

the fundamental rights and legitimate interests of that person are taken into account

must be.112

Also the regulation of case conferences of the prison system with security authorities113,

which, in particular with regard to the necessity of the data processing practiced there

processing are always problematic, it was investigated on the basis of our

improves. On the one hand, with regard to the data processing powers of the

on the other hand is now explicit in the explanatory memorandum to the law

pointed out that the powers of the other participants of case conference

limits for data processing to the penal system from their respective specialist law

must follow.

On the other hand, our criticism of Section 4 (2) of the amended Judicial

enforcement data protection law (JVollzDSG). According to this, all prisons,

the juvenile detention center, the youth detention center, the information center of the prison,

the prison hospital, the central IT office of the prisons

and the social services of the judiciary together form a single controller.

This contradicts the wording and intention of the Berlin Data Protection Act (BlnDSG)114

and the underlying JI guideline115. After that, the responsibility

ability to decide on the purpose and means of data processing.

This provision is based on the fact that each public body has its own

and areas of responsibility that lead to different data processing

exercise powers.

111 See Article 13(3) of the JHA Directive

112 See Section 30 (3) of the JI Directive

113 See Section 48 of the Prison Data Protection Act (JVollzDSG)

114 See Section 31 No. 7 BlnDSG

115 See Art. 3 No. 8 JI Directive

The task of a correctional facility is, for example, to enable the prisoners in the future

to lead a life without crime in a socially responsible manner and the general public

to protect against further crimes.116 The enforcement of youth detention should in turn

awaken the young person's sense of honor and make him aware

that he has to answer for the wrongs he has committed.117 The social services

are, however, for tasks of probation assistance, court assistance and management

responsible for supervision and the hospital of the prison naturally only and

solely for medical patient treatment. The places mentioned may indeed

be organizationally connected, but process data in the context of different

tasks and for different purposes.

In this context, it is particularly problematic that all of the above

together with the prison hospital as a unified body.

should. The protection of the special categories of personal data118 that

primarily processed at this point cannot be adequately guaranteed

become.

Insofar as data is to be exchanged between the named bodies, it is necessary

specific statutory transmission authorizations for this purpose, which refer to the respective

given by the agencies involved. A waiver of clear standardization

such data transfer authorizations for reasons of avoiding unnecessary office

cracy costs, as stated in the explanatory memorandum to the law, leads in practice to ambiguity

units in the admissibility of data exchange between these bodies and a

associated high risk of unauthorized data processing.

Another point of criticism concerns the standardization for the processing of biometric data.

Already in the previously applicable JVollzDSG, the collection was biometric for the first time

features of the face, eyes, hands, voice or signature

Allows prisoners for identification purposes. We had this rule-

already in the legislative process at that time due to non-necessity and

116 § 2 Berlin Penal Law (StVollzG)

117 Section 90(1) Juvenile Courts Act (JGG)

118 See Section 31 No. 14 BlnDSG

Disproportionate in view of the significant interference involved

criticized the personal rights of those affected.119

Now it is at least no longer possible to use voice as a biometric feature

process.120 The other biometric features should, however, continue to be

commercial purposes can be processed.

As far as we know, no biometric features are used in the penitentiary

processed, so that the practical relevance of this regulation is doubtful. of

Obviously, the penal system has so far also been dealing with the other identification services

With these measures it is very possible to check the identity of prisoners, for example in order to

to avoid confusion.

Berlin was in 2011 with the creation of a very ambitious own judiciary

enforcing data protection act nationwide pioneer. This law has now been

finally revised based on the new European legal requirements, regrettably

albeit not in all the necessary points.

4.4 Bailiffs: The "speaking"

business sign

The bailiffs play an important role in the structure of jurisdiction

position on. In principle, they are the only ones who carry out enforcement measures in the

may carry out ways of foreclosure. Delivery is also valid

Bailiffs as one of the safest ways to prove

which letter the recipient received. Since also a third party

notification, it is particularly important that on sensitive

Data from affected citizens, who are often involved in the

mentioned procedures, good care is taken.

A

and

s

i.e

e

right

P

right

a

x

i

s

In a case that we became aware of through a complaint from a person

den, a bailiff had been commissioned to serve and had

119 See Annual Report 2011, 2.2.3

120 See § 19 Para. 1 No. 5 JVollzDSG

not only assign the usual abstract combination of numbers as a business reference,

but the reference number under which the client used the

driving led. However, this business reference referred to the contents of the locked

Close the letter that was to be delivered to the person concerned.

While it may be necessary to deliver documents to be served - also on the

postal envelopes or in the viewing window - to be marked separately to avoid confusion

to avoid genes, it was not necessary for the work of the bailiff to

to adopt such a "speaking" business reference of the client. A

own, encoded business reference would have been completely sufficient. Because as far as the

draw conclusions about the specific content of the document.

or the content of the document is recognizable when the envelope is closed,

there is a violation of the GDPR.121 Such data processing is for the

Task performance not required. We have this action of the court

bailiff reprimanded with a warning.

Bailiffs are not allowed to use "speaking" business

use sign.

4.5 Limitation of the right of access to

the legal profession

s

i

x

a

right

P

right

e

i.e

s

and

A

We keep getting complaints from citizens who, at a legal

walter or a lawyer, the issuance of a data protection

have applied for future. As responsible persons, lawyers are generally subject to the

Regulations of the GDPR and must therefore also take appropriate measures

to transmit the respective information and notifications to the persons concerned

media.122 The right of the persons concerned to information can be compared to the legal

However, authority may be limited. This depends on their position

121 See Article 6 Paragraph 1 Sentence 1 Letter e GDPR in conjunction with V. m. § 132 paragraph 1 BGB

122 See Art. 12 GDPR

as so-called subjects of professional secrecy or with the legal confidentiality

obligation together.123

In order to take account of the confidentiality obligations and client confidentiality,

does the DS-GVO contain exceptional circumstances that persons subject to professional secrecy: inside at the

privilege the fulfillment of certain data protection obligations.124

The national legislature is authorized to do so on the basis of so-called opening clauses

Regulations for the restriction of information and notification obligations

to issue professional secrets to ensure the protection of confidential data

chern.125 The federal legislature has hereof within the framework of the new version of the Federal

of the Data Protection Act (BDSG).126 There is a right to information

of the person concerned according to Art. 15 DS-GVO, "if the information

information would be disclosed which, by law or by its very nature,

in particular because of the overriding legitimate interests of a third party

must be kept."127 The basically comprehensive right to information is thus

limited to obviously mandatory confidential information and the

confidentiality obligations are exceptionally given priority.128

However, the wording of the corresponding regulation suggests that the information

right of a data subject vs. a lawyer

is not generally excluded, but that the person(s) subject to professional secrecy:in

must check in individual cases whether or to what extent information

would be given, which are subject to secrecy. In practice it turns out that

particular opposing parties to a procedural or non-procedural legal

dispute a right to information according to Art. 15 DS-GVO at law firms.

In these cases, the balancing of interests or identification and delimitation of

information requiring confidentiality is regularly difficult. It is to be considered

that the subject of information to the person concerned then regularly data

123 See section 203 subsection 1 no. 3 of the Criminal Code (StGB), section 43a subsection 2 sentence 1 of the Federal

Lawyers

regulation (BRAO) i. In conjunction with Section 2 Paragraph 1 Sentence 1 Professional Code for Lawyers (BORA)

124 See Article 14(5)(b) and (d) GDPR

125 See Article 23(1)(i) GDPR and Article 90(1) GDPR

126 See §§ 29, 32 to 35 BDSG

127 Section 29 (1) sentence 2 BDSG

128 Jandt in Roßnagel, The new data protection law § 8 para. 318

who are the person(s) subject to professional secrecy in this very capacity (above all

received from the own client.

According to Art. 15 DS-GVO, lawyers are not allowed to make blanket requests for information

reject, but must examine in individual cases whether and to what extent the right to information

of the applicant due to the confidentiality of the mandate or the legal

any confidentiality obligation is excluded. About the reasons for one

(Partial) exclusion of the right to information or the reasons for a refusal

The data subject must be informed of the disclosure of information.129

129 See Art. 12 (4) GDPR

Chapter 4 Justice and Lawyers 5 Youth, Education,

Science and Research

5.1 Implementation regulations for youth welfare —

Data protection considered from the outset

This year, the Senate Department for Education, Youth and Family

same implementation regulations for cooperation between schools and districts

youth welfare offices in child protection (AV JugSchul Kinderschutz)130. Simultaneously

does it have a "manual" for the binding implementation of these implementation regulations

development guidelines for child protection” on cooperation between schools and district

youth welfare office.131 We asked the Senate administration to work on

advising on the implementation of the regulations and the guidelines.

A

and

s

i.e

e

right

P

right

a

x

i

s

The cross-departmental cooperation between district youth welfare offices and

other places, especially in the field of child protection in everyday practice,

significant data protection issues.132 Implementing regulations serve this purpose

Purpose, to specify the legal regulations and task assignments and

to facilitate practical implementation. It is important here that the professionals

in the youth welfare offices and the teachers in the schools as concrete as possible

to provide training instructions for practice.

While the procedure for dealing with child endangerment at the

Youth Welfare Offices through the common implementation regulations on the implementation

tion of child protection measures in the state of Berlin (AV Kinderschutz JugGes)133,

130 See https://www.berlin.de/sen/jugend/recht/rechtsverbindungen/

av_kinderschutzjugschul.pdf

131 See https://www.berlin.de/sen/jugend/familie-und-kinder/kinderschutz/fachinfo/

action guide_child protection_school_jug.pdf

132 See on cooperation between youth, health and social welfare offices in child

protection JB 2015, 6.2; Annual Report 2016, 5.1; JB 2017, 6.1

133 See https://www.berlin.de/sen/jugend/recht/mdb-sen-jugend-rechtsverbindungen-av_

child protection.pdf

which we have reported on several times in the past,134 is regulated in detail,
corresponding regulations for dealing with children endangering
genes for the schools.
With the implementation regulations that have now been issued, in the event of a
known suspicion of endangering the welfare of a child, a Berlin-wide
drive prescribed, which must be observed by the schools and, if necessary, information
required by the responsible youth welfare office. Since child protection cases are always about
are highly sensitive issues, on the one hand a special eye
Attention should be paid to compliance with data protection regulations in order to protect
of the affected children and young people. On the other side is
it is also necessary to provide the teachers with clear guidelines that are often available
Legal uncertainty regarding the handling of this sensitive information
take. The teachers must be given security of action, which data
they are allowed to process and, if necessary, pass them on to the youth welfare office, so that the suspicion
of a child endangerment and a danger to the well-being of children
and young people can be effectively averted. The responsible Senate administration
tion has developed uniform documentation and communication forms for this purpose
are mandatory for schools to use.
Since the in connection with the suspicion of a child endangerment in the
School documents are stored and destroyed in accordance with data protection
when they are no longer required, this was also stated in the implementation
regulations to take into account. Our suggestions for specifying the regulations
the responsible Senate administration has taken up this point. We keep it
but for expedient, with the already upcoming revision of the school data processing
ordnung135 also specifying regulations on how to deal with the

related to documents arising from suspected cases of endangerment of children's welfare

create.

The Senate Department for Education, Youth and Family informed us in good time about

review of the documents and appropriate advice. Our notes on the

Implementation regulations and the guidelines for action together with documentation and

134 Annual Report 2015, 6.2; Annual Report 2016, 5.1; JB 2017, 6.1

135 See 1.2.2

Newsletters have been accepted. The missing guidelines for dealing with

Suspected cases of endangerment of children's welfare should be included in the School Data Ordinance,

which are due to be revised anyway, are supplemented accordingly.

5.2 Unencrypted sending of copies of certificates

Schools continued to be affected by the pandemic as the winter holidays began

affected by school closures. The half-year reports should therefore not - how

as usual - before, but only after the winter holidays given to the students

become. The notification from the education administration, students and educational

If desired, a copy of the certificate can also be sent by e-mail

be led to individual school administrations in view of the confidential content

data protection uncertainty.

A

and

s

i.e

e

right

P

right

a

x

i

s

In terms of data protection, it is obvious that the unencrypted transmission of

Copies of certificates, which include grades, absenteeism and information on social behavior

is problematic. The education administration apparently felt compelled to send the schools

to point out in a further letter that the transmission is preferable

should be end-to-end encrypted and password protected, but then led

further from: "If the data subject has expressly requested transmission,

although these requirements are not met, that is also permissible."

tig she submitted a text proposal for consent to the unencrypted

Sending by email.

Apart from the fact that the text proposal as such does not comply with data protection law

meets the requirements for effective consent, we were very surprised

that the educational administration as the legal basis for the consent § 36 of the Berlin

Data Protection Act (BlnDSG). This is a requirement solely for that

Data processing by law enforcement and law enforcement authorities, d. H. into the-

special police, prosecutors and courts, is applicable, but under no circumstances

for schools. Their data processing is based solely on the basic data protection

regulation (GDPR).

Since compliance with appropriate technical and organizational measures by

is to be ensured for those responsible, we see a transfer of school certificates

no space on the basis of consent. The conference of data

The Federal and State Protection Officers (DSK) recently published a

passed a resolution according to which the technical to be maintained by those responsible

and organizational measures are based on objective legal obligations that are not

are at the disposition of those involved.136 A waiver of appropriate measures

on the basis of consent is not considered permissible. Applied to the

existing super/subordinate relationship between students and schools

Consent in the school context is hardly considered anyway.137

In the matter would be in the situation - as well as by the way of the education administration

self-executed - a postal transmission is preferable under data protection law

been. Although the dispatch of certificates by means of an end-to-end encryption

selung is not objectionable in terms of data protection, but very few schools are

currently able to send their e-mails encrypted, let alone

because most parents have the option of receiving end-to-end encrypted

rarely created e-mails.

We think it is necessary for school management and teachers to find solutions

are offered that enable them to behave in a legally secure manner

can. The creation of a possibility for data protection-compliant communication

between teachers, parents and students we think is overdue. We stand

the schools and also the education administration in an advisory capacity.

5.3 Corona self-tests in schools

s

i

x

a

right

P

right

e

i.e

s

and

A

In April, the Senate introduced mandatory self-testing for infection with the

Coronavirus SARS-CoV-2 for the students under the supervision of the pedagogical

staff at all schools. We received a large number of inquiries and

severely concerned parents, but also teachers on this subject. Besides worries

Fears were expressed about health hazards, the self-tests

136 See https://www.datenschutzkonferenz-online.de/media/dskb/

20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf

137 See EG 43 GDPR

could lead to a violation of personal rights and stigma positive

tested students lead.

In the event of a positive test result, schools process health

personal data of the students concerned. This sensitive data is subject to a

special protection and may only be processed if an appropriate

legal basis exists. Such is contained in the Schools Act (SchulG). It allows

the schools the processing of health data if this is necessary for

the fulfillment of the school-related tasks regulated in the SchulG.138 In addition, the

Education administration for carrying out the tests in the schools with the school

Hygiene-Covid-19-Verordnung139 created a regulation that expressly includes the

Processing of test results allowed by schools. Data protection regulations

think against the processing of health data by schools

so far not.

However, we have recognized the problem that there is in the implementation

the testing of all students present in the classroom is hardly avoidable,

that health data of schoolchildren who tested positive are also shared with the other

to become aware of. To ensure the greatest possible protection of health data

to ensure that a procedure would certainly have been preferable with which organizational

toric it can be guaranteed that the health data is shared with third parties not open-

be laid, as z. B. would be the case with an individual test. However, it is possible

practically do not enforce such a procedure for all students. in case of a

positive test result, knowledge of the information can also be used for possible

Other contact persons may be required to take the necessary measures

can, e.g. B. ordering a quarantine.

In responding to inquiries and complaints, we pointed out that

that the situation is complex and that the schools face significant challenges

challenges. At the same time we found that the decision

about which method of conducting self-tests in a weighing

of the different legal interests affected, the smallest encroachments on fundamental rights

138 Section 64 (1) and (2) SchulG

139 At the time compulsory testing was introduced, Section 5 of the School Hygiene Covid-19 Ordinance applied

(SchoolHygCov-19-VO). A corresponding legal basis can currently be found in § 3 Second

School Hygiene Covid-19 Ordinance (2. SchulHygCoV-19-VO).

entails cannot be assessed solely in terms of data protection law. After a

initial flood of complaints on the subject decreased in number

significantly after a few weeks. We conclude that schools have a way

found how to strike a balance between the affected legal interests

in order to avoid the violation of personal rights.

5.4 Digital blackmail: What about ransomware

has to be done

We regularly receive reports of data breaches caused by ransomware

were caused. Professional criminals infiltrate the information technology of

companies and authorities to extort money. We advise affected bodies and

attach particular importance to preventive measures during technical inspections.

s

i

x

a

right

P

right

e

i.e

s

and

A

The Technical University of Berlin, the Court of Appeal, the City of Bitterfeld, the State

district of Ludwigslust-Parchim but also connects many small and medium-sized companies

a commonality. All were victims of attacks with so-called ransomware - malware

programs whose purpose is to extort money from those affected. Such

Attacks are now primarily carried out by organized criminals

and so their approach is often similar.

Once an attack has been successful and the IT systems have been compromised, it takes time

sometimes it takes months for the attacked area to restore its full ability to work

asked. Especially with complex, confusing system landscapes, such as

she z. B. prevail at universities, it is anything but trivial to ensure

that the malware is removed from all devices put back into operation

became. Otherwise, the attack may be repeated.

Ransomware is not a new problem. In recent years, however, there has been a clear pro-

professionalization of the attackers has taken place. Were IT sys-

teme largely automatically encrypted in order to extort relatively small amounts,

the procedure is now usually different. Criminal groups work

lig and specialize in different phases of an attack. The ones there

The software used is often used by other criminals as “Software-as-a-Service”

shopped Instead of automating an infected system as quickly as possible, as was previously the case

encrypt, the currently used procedure is usually a careful, manually

gliding exploration of a network in which an infected system resides. loading

before the actual blackmail begins, the attackers try to get as far as possible

to spread many systems in the network. In order to increase the pressure on the victims,

often tries to destroy or compromise backups. Besides – and here lies

the particular explosiveness for data protection - are meanwhile also being used in many cases

Data downloaded by the attackers. Because among these data are common

also data from customers. The criminals threaten to publish the data

and it is not uncommon for these to actually become public in the course of the attack.

The reasons for a successful attack are similar in many cases. After successful

Rich initial infection of a system, which often takes the form of an infected email attachment

or a link to malware, attackers connect to it

system and use it as a kind of stepping stone to others that can be reached in the network

systems. Even if most software manufacturers provide security updates

, these are often not installed on the systems or not installed in time. The

There are many reasons for this, ranging from inadequate patch management140

on the part of those responsible for IT to the knowing use of old, less secure

software, e.g. B. Because a critical application was not prepared to start with a

newer version of the operating system or other basic software together

to work. Due to the networking of the systems with each other, this is sufficient

sometimes a single insecure system to open the door to the entire attacker

to open the network of those responsible.

It is also extremely problematic that many IT systems are in the delivery state

are initially configured insecurely and only once by competent personnel in

must be brought into a state in which it is possible to safely

operate.

In many cases those responsible seek their salvation in the most comprehensive

monitoring and logging of the activities of the IT systems. In fact, over

security systems available that recognize specific attack patterns and anticipate them

can warn. So an attack should be detected early and at least its effects

140 patch management describes the process of updating installed software and e.g. B.

to provide security updates.

be limited. However, for one, the effectiveness of the systems may be lower

prove to be advertised, as the attackers develop evasion strategies. And

on the other hand, there is a tense relationship between ill-considered surveillance and

Data protection. It is only permitted if it is configured to save data, if you

It is ensured that the users of the systems are informed that and in which

Scope the systems are monitored, and if the log data exclusively

to ensure the security of the IT systems and not to control the

performance and behavior of employees. Unfortunately we are watching

regularly that data is collected prophylactically without a plan being

was made, how and under what conditions they are to be evaluated. To

every protocol that contains personal data also has an associated policy

its data protection-compliant evaluation.

Another effective measure, reducing the damage in the event of a successful

Attack can limit, is a division of the IT systems of those responsible

different subnets. These subnets are then separated from each other in such a way that only

neither can the absolutely necessary data traffic flow and be monitored between them

can. In a favorable case, such a separation can also lead to a successful

Limit attack to a small part of IT.

Companies and public authorities must ensure the security of their IT systems

invest. In particular, it must be ensured that the software used

is always up to date and known security gaps are eliminated.

At the same time, software manufacturers should ensure that their products are already

can be operated as safely as possible in their basic configuration. Where this

is not the case, those responsible have a duty to ensure a secure configuration

to manufacture. This can also include the fact that large organizations have their IT systems in

split into smaller units so that in the event of a successful attack at least

the potential for damage is reduced.

Against the background that the attackers are starting to download data

to load and to sell at a later date, it is from the point of view of the data

protection has become even more important to take effective measures

since it is no longer just a question of the availability of data, but also of the

ensuring their confidentiality.

84

Chapter 5 Youth, education, science and research 6 Health and care

6.1 Contact tracing in health authorities

To efficiently care for people infected with SARS-CoV-2, and

The health authorities are supposed to use the software to track their contacts

SORMAS141 are used. We have the Senate Department for Health,

Advice on the introduction of care and equality (SenGPG). gave at the same time

together with supervisory authorities of other countries and the federal government in a working

group Notes to the developers and operators of the system.

A

and

s

i.e

e

right

P

right

a

x

i

s

The SARS-CoV-2 pandemic has put the health authorities under particular pressure

set. In order to cope with the large volume of infection reports and the con-

The health authorities felt compelled to inform contact persons of infected

to optimize their processes. Technical solutions should make it easier to deal with

simplify and standardize the large number of infection reports.

If an infection is confirmed by a laboratory, the responsible health authority receives the information

via the German electronic reporting and information system for the infection

schutz (DEMIS) sends a message and contacts the persons concerned. These will

asked about the circumstances of the infection and about the contacts of the last few days

to be able to warn other contacts who may already be infected. About it

In addition, the health department can order that the contact persons have themselves tested

sen or even have to go into quarantine.

The health authorities process this, as with many other notifiable cases

Infectious diseases also, health data on a large scale and transmit

As part of their legal mandate, daily infection figures to the Robert Koch

Institute (RKI).

141 Surveillance, Outbreak Response Management and Analysis System

For this work, the health authorities have the software SORMAS for case

processing and contact tracing.142 This is a

open source software originally developed to deal with previous epidemics such as

Ebola was developed in Africa. Some health authorities use this software

ride in.

We intensively supported SenGPG during the comprehensive introduction of SORMAS

advise.

In addition, we have endeavored to focus on the development of the software product

to influence. Together with other supervisory authorities, we stood up for this

Exchange with the Helmholtz Center for Infection Research (HZI), which
development of the software on behalf of the Federal Ministry of Health (BMG)
ned. As a result of the development, the health authorities nationwide should
version of SORMAS will be provided by a federal institution.
This centrally operated version called SORMAS X was released in 2020
put into operation and in some federal states, but not in Berlin, in the pilot
operation used. Contrary to his promises, the project developer HZI was in the process
this year not able to eliminate the significant deficits of the software,
to which the supervisory authorities had pointed out. Deadlines were not met
and documents not submitted as requested. It remained unclear whether self-announced
measures have been implemented.
Significant points of criticism related to the extent of the data to be processed with the software
Data; the incomprehensible specifications and lack of functionality
to delete data that is no longer necessary for the further work of the health authorities
are needed; the regulation of authorizations for health authorities and their
busy working with the data; the lack of protection of interfaces
of the system to the outside and the design of the functions for the exchange of
Data between the different offices involved in the handling of a case.
Due to the HZI's lack of willingness to cooperate, we decided to
decided to withdraw from the advisory process. The competent Senate

142 In addition to SORMAS, some health authorities use other systems; see 1.5

administration, we can encourage the Berlin health authorities to participate in SORMAS X
currently do not recommend. The one already used by some health authorities
and their own version of the application is from this assessment

not affected.

Digital case processing and contact tracing in the health authorities

tern is still in its infancy. The health authorities need solutions

which enables them to work efficiently and - without additional investments in power and

Resources - the protection of the affected citizens from risks and an over-

enable on-board processing of their data.

6.2 Digital vaccination certificates: prevent counterfeiting,

check for sure

We followed up on leads on opportunities, vaccination certificates and test evidence

falsify, require citizens to prove compliance with the 2G or 3G rules

necessary that were introduced to combat the Sars-CoV-2 pandemic.

Due to a number of requests, we have also approved the use of the CovPass

Check app for examining digital COVID certificates and found that

there is no danger.

A

and

s

i.e

e

right

P

right

a

x

i

s

In order to avoid further infections in the Sars-CoV-2 pandemic, it was decided

that only people who have received a full vaccination, their recovery after an

infection or a recent negative test for infection

(2G or 3G rules), admitted to certain events or in certain

facilities are admitted. Evidence is provided via electronically generated

Documents that are machined with a so-called QR code (a square dot grid)

be made readable.

The advantages associated with one of the mentioned proofs create a

Incentive to fake these for people who meet the requirements for their legitimate

acquisition do not own.

87

We received reports of data breaches at both test centers143 and the

Operator of a portal for issuing vaccination certificates. The issuance of vaccination certificates

katen via this portal, which was intended for use by pharmacies

be suspended for several weeks after security researchers

lungs was to register an unauthorized user account for a fictitious pharmacy and

to issue any vaccination certificates.

We investigated the data breach at the Vaccination Certification Portal and

ensured that the operator of the portal draws sufficient lessons from the glitch.

The case showed again how important it is to have sufficiently reliable procedures

establish with which the identity of those involved in a procedure - here the pharmacist

- it is determined and ensured that they are authorized to

to take on the right role in the proceedings. The supervisory authorities have

repeatedly pointed out in different contexts.

However, there is no reason to worry when using the CovPassCheck app to

Checking of digital vaccination and recovery certificates. restaurants, shops and

other institutions are legally obliged to report the vaccination or

recovery of visitors based on their above to check certificates. For this has that

RKI released the CovPassCheck app.

A number of complainants have contacted us because they

use of the data contained in their digital certificates by organizers in

Feared consequences of using the CovPassCheck app. We were able to confirm

that the app only informs the organizer of the status of the respective certificate as well as

Displays the surname, first name and date of birth of the certificate holder. the latter is

required to enable the event organizer to use an ID document to

ment of the person concerned to verify the ownership of the certificate. The app

saves the data only temporarily when the certificate is checked using a scan.

The data is automatically deleted with the next scan.

Of course, this assessment only applies to the CovPassCheck app. Should events

ter:innen use another app, e.g. a photo of one presented

To create a certificate, you would be left with a copy of everything contained in the certificate

143 See 1.4

Data. We therefore advise that you familiarize yourself with the CovPassCheck app and

to ask the organizers to leave the display of the smartphone with which the

control of the digital certificate is carried out, first to assign

those who are controlled, and only then to see for yourself. pointers to specifics

We accept misconduct by event organizers for review.

Who IT systems for processing personal data for use

by a large number of parties involved, must ensure their reliable identification

ensure that only those who are authorized to do so can use them. If

If citizens are allowed to see responsible documents, this does not mean

that they are authorized to make a copy.

6.3 Maximum deadlines are not mandatory

storage obligations

A

and

s

i.e

e

right

P

right

a

x

i

s

A citizen had complained to us about the fact that the Association of Statutory Health Insurance Physicians

igung (KV) Berlin did not respond to their request for information and deletion. The

Reasoning of the KV did not completely convince us.

When we asked, the KV explained that in connection with the

sending of vaccination invitation letters in the spring144 to an increased and the normal

number of requests for information that exceeded the measure. Also set

KV uses numerous systems to fulfill its tasks, from which the requested

information would have to be gathered. This was called

th period turned out to be extremely time-consuming due to the large number of inquiries,

which is why, as in the present case, it was not able to comply with them immediately.

The KV even completely rejected the request for deletion. For this purpose, the KV

informed that she had not complied with the complainant's request

because they are subject to retention by a regulation in the Social Security Code (SGB).

obliges be.145

144 See 1.3.2

145 See § 304 SGB V

That the complainant's request for information due to the presented

overload are not met within the statutory period of one month

that was not surprising and was understandable for us. Nevertheless, the

chief in accordance with the requirements of the General Data Protection Regulation (GDPR)146

informed at least about the extension of the deadline and the reasons for the delay

Need to become. From a data protection perspective, however, was more interesting

Justification of the KV as to why they are involved in deleting the social data of the complaint

leader saw prevented.

It is correct that the provision in the SGB used by the KV stipulates that

agreed, in the law specified social data from the KV "at the latest after ten

years" are to be deleted. However, this is not a retention

obligation that generally prevents deletion before the end of this period. Much more

The aim of the regulation is to ensure that social data is not stored for longer than

tasks are absolutely necessary to be saved if special regulations

do not provide for a longer retention period. The wording also indicates this

("at the latest"). There are therefore no retention requirements with the regulation

stipulated that prevent deletion, but maximum storage periods

fixed. Deletion before the end of this period would therefore be legally possible,

if the further processing of the data for the fulfillment of the tasks of the person responsible

is no longer required.

We were able to determine whether these requirements were actually met in the initial case

cannot judge based on the information available to us. In addition

it is first up to the KV to check what data the complainant has

actually necessary to fulfill their tasks. That's why we have the KV

advised of our legal opinion and requested that the request for deletion of the

to check again on the basis of our statements.

There is a crucial difference between maximum periods and mandatory storage obligations.

the difference. In particular, deletion requests from data subjects

not with a blanket reference to statutory maximum storage

be rejected.

146 See Art. 12 (3) GDPR

6.4 Deleting an entry about an unconfirmed child endangerment

In a file kept by a health authority, there is an entry that the

has not confirmed the thought of endangering the welfare of the child, at the latest after the expiry of one

year to delete.

The legislation applicable to the public health service provides that

that personal data, unless other legal provisions require storage

set deadlines, to be deleted or made anonymous as soon as they are necessary for the purpose

to which they were processed are no longer required, but no later than two

Years after completion of the process that triggered the data processing. 147

A

and

s

i.e

e

right

P

right

a

x

i

s

The information that the suspicion of a child endangerment is not confirmed

is no longer required after a year has elapsed. This results from a

a comparison with the regulations applicable to the youth welfare office148. After that they are

Destroy documents no later than one year after the final decision

and to delete stored data if the responsible body is part of a

Risk assessment comes to the conclusion that there is a risk to the welfare of the child

not available.

The only result of this is that the data concerned will be deleted after one year at the latest

are no longer required for the youth welfare office under the above conditions.

But the same must also apply to the health department. Because it opens up

not why the same data should continue to be required for the health department-

when they are no longer needed for the youth welfare office. On our corresponding

Upon request, the health department concerned deleted the entry from the file.

Sensitive information on an unconfirmed suspicion of the existence of a child

endangerment may only be kept for as long as absolutely necessary.

is. Youth and health authorities should apply the same deadlines here.

147 § 4d para. 1 Health Service Act (GDG)

148 Common implementation regulations on the implementation of measures to

Protection in the State of Berlin (AV Kinderschutz JugGes), Section 7.3.3

6.5 Appointment management in medical practices —

What is to be considered?

s

i

x

a

right

P

right

e

i.e

s

and

A

This year we again received numerous inquiries and complaints

by citizens from all over Germany for data processing

a company that is often used by medical practices to manage appointments.

Increasingly, medical practices, medical care centers and

Hospitals contacted us and asked for advice on what to do when claiming

Providers of appointment management software must take into account.

Many practices have switched to specialized appointment management

Outsource appointment management companies. Such companies are for practices

attractive because these promise them the utilization with reduced waiting time for the

to improve patients. They also entice you with additional functions such as

ments for the patients.

The solutions distributed in this way are used when patients themselves

an appointment management company website set up for this purpose

book in practice149 or if patients book one by phone or in the doctor's office

Make an appointment and have this appointment entered into the online calendar by the practice staff

entered into the system of an appointment management company. In the latter case

the patients learn about the processing of their data by the appointment

ment companies often only by sending an e-mail or

Received an SMS with an appointment reminder from the company.150 Not only patients

ments, but also medical practices have asked us whether the patients are in action

from appointment management companies have to agree.

Patient consent is not required if appointment management

processing companies are so-called processors of the medical practices. order processing

Employees act on the instructions of the doctor's office. The data processing by Ter-

minverwaltungsunternehmen is then insofar - as well as with the claim

other IT service companies - completely the medical practices that use this service,

149 See 6.6

150 See Annual Report 2019, 6.3

attributable. However, the medical practices must protect the patients in their data protection

information about the use of processors.

The situation is different when medical practices send their patients by e-mail or SMS to ver-

want to remind you of scheduled doctor's appointments. Because medical practices are allowed to give patients a term

only then transmit the reminder or transmit it through processors

leave if the patients vs. the medical practice have expressly consented to

that their telephone numbers or e-mail addresses are used for appointment reminders

151 Medical practices should review their procedures in this respect and, if necessary,

adjust.

The purpose of storing the appointment data no longer applies as soon as the appointment has passed.

Since the practices document the appointments in the patient files, one

additional storage in the systems of the appointment management companies

Deadline not allowed. The time required after the deadline

imminent deletion of the data from the online calendar system should already be

processing contract to be established.

The doctors must ensure that the security of the processing by their

Processors are guaranteed because they are responsible for processing the data themselves

stay responsible. Since the assessment of the security level of appointment management

development company is a complex issue, it is recommended for most

Medical practices, obtain external advice on this, but at least on common data

to respect the protection or information security certifications of the companies. au

In addition, they must ensure that they inform the companies in the order processing

contract to maintain secrecy, in order to protect them as persons subject to professional secrecy

comply with the statutory duty of confidentiality.

Also in the event that parts of the data processing are carried out by processors

outside of Germany, in particular outside the scope of the GDPR

are to take place, it is necessary to obtain advice on data protection in this regard.

151 See Annual Report 2019, 6.3

There is often uncertainty among both patients and doctors as to what

data protection law must be observed if appointment management companies

be set. We have frequently asked questions in an information

collection that can be accessed on our website.152

6.6 With a click to the appointment — appointment booking portals and

their handling of patient data

s

i

x

a

right

P

right

e

i.e

s

and

A

It is convenient for patients to use an online appointment portal to

agree mine with medical practices. Already when looking for an appointment

However, it can happen that highly personal information such as the requested

ten specialists or treatment methods or even symptoms

become. Based on two indications, we checked with a provider whether this data

impermissibly transmitted to third parties, and whether the provider fulfills its obligation to delete

obligations after closing an account.

If appointment management companies operate websites about the patients

themselves can book appointments at doctor's offices, they must ensure that the

(health) data entered by the patient are treated confidentially.

The processing of special categories of personal data i. s.d. Article 9

GDPR, which also includes health data, requires special care.

Monitors the company to ensure the security of the

tenen services the interactions of patients with his website, may

no data not required for this purpose is collected. particularly prob-

The transmission of sensitive data such as e.g. B. the transmission of symptoms

to companies in countries with an insufficient level of data protection.

Such an approach was demonstrated to us this year by security researchers at a

App of an appointment management provider, with whom we have already been reported in the past

Genheit had complained about the same procedure in the context of his website. through the

Security researchers found that data e.g. to a US-

cal company and were thus transmitted to an insecure third country.

152 https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/terminverwaltung-

from-doctor appointments

Do patients have a user account with an appointment management company?

directed to being able to search for appointments at doctor's surgeries online, there is a

contractual relationship between the patient and the appointment management company.

If this contractual relationship is terminated, the purpose for which the appointment management

company has stored the personal data of the patients.

When the purpose no longer applies, the duty of the person responsible usually goes

for immediate data deletion153. The only exception is data for

which is subject to a statutory retention obligation. The deletion must be the responsibility

literally do it yourself. You cannot meet it by using the

Patients - as actually happened in one case - the deletion of their

give up data yourself.

In both cases, we asked the relevant provider for a statement and

asked him to rectify the deficiencies found.

A transmission of unencrypted health data by appointment management

companies to third parties in unsafe third countries in the course of looking for an appointment

or booking by the patient is not permitted, even if it is for the purposes of

usage analysis is carried out. In addition, the patients have to rely on it

can that after a contract termination their personal data without

further action on your part will be deleted.

6.7 Easily looted patient files

We officially checked the implementation of certain standards at a hospital

standard measures to ensure the security of those processed by it

Patient: internal data.

In clinics today, large amounts of sensitive health data are collected from patients

ent:innen processed in digital form. Both laboratory equipment with which physiological

Values are recorded digitally, as well as tablet computers at the patient’s bed

listen to everyday clinical practice. Of course, this has many advantages, since the

health data that are often urgently required for an action are available in a timely manner,

A

and

s

i.e

e

right

P

right

a

x

i

s

153 See Art. 17 GDPR

95

and doctors the treatment documentation, e.g. from the home office

can continue. The latter aspect gained additional attention in the pandemic

interpretation.

On the other hand, data in digitized form is exposed to new risks. So try

Attackers: inside again and again, from outside into the IT systems of the hospitals

intrude to obtain data or by encryption for use

render them unusable and thus blackmail their victims. To fight against

ers, solid security precautions are needed to prevent intrusion of attackers:in-

complicate and successful attacks on small parts of information technology

restrict.

We checked whether the hospital in question had four basic precautions

were taken: The reliable authentication of employees at their

accessed the clinic systems from the home office, the use of centrally administered

Service devices for this access, the division of information technology into

the safety-related separate areas depending on the protection requirements and purposes of the

Data processing and the immediate elimination of discovered vulnerabilities

in IT systems.

Unfortunately, our audit revealed significant deficits in all four areas. In sum

would have attackers with well-known and relatively simple attack methods

far-reaching access to the hospital's IT systems and thus insight into almost

all files of currently treated and former patients can be obtained.

Reliable authentication of employees when accessing the clinic

systems from the home office requires two things:

First, the beneficiaries must unequivocally prove their identity before they can

Obtain passwords and other information they need to log in to the systems

need. This applies both to the first allocation of an account and to

the restoration of access if e.g. B. Passwords have been forgotten.

Second, it must not be possible for third parties to access this information.

Neither by recording the network traffic nor by phishing - that is, through

the misrepresentation of a legitimate hospital website to which employees are referred

through fake e-mail messages or intrusion into network traffic

to be able to pick up passwords - nor by accessing storage locations

where the information required for dialing in is stored.

Established technologies such as virtual private networks (VPNs) and multi-factor authentication

fication (MFA/2FA) help to ensure this. keep passwords and other secrets

information that may be required for registration (e.g. secret keys)

must be deleted from the locations where they were posted,

as soon as the beneficiaries have received them. Finally, it is necessary really all of

interfaces of IT systems that are accessible outside the hospital for risks

to check.

With the use of centrally administered service devices for external access to

the clinic systems will ensure that access is from a secure basis

done. If, on the other hand, private devices are used, the security is with them

processed data is at risk. Attackers seize one of these

regularly only weakly protected systems, they can access all data,

to which the owner of the device also has access. goods to

At the beginning of the pandemic, some managers were still overwhelmed by their employees

to supply service equipment, two years after the start of the

give more compensation for this omission.

The immediate elimination of discovered vulnerabilities is one of the elementary

The toughest requirements for secure operation of information technology. In the of

In the case we examined, the failures in this area were known to the IT management

and have been tolerated for a long time. Even some safety-critical systems have been

operated with software that is no longer maintained by the manufacturer.

In hospitals, tightly networked IT systems that are interlinked are widespread

offer services. Software updates must always be checked for their effects on this

these complex systems are tested. Therefore, it is not easy to ensure

that they are entered in a sufficiently timely manner. This requires foresighted planning

tion, the cooperation with the software manufacturers, whose prompt support

must be contractually secured, and a well thought-out process for the

Test updated software for unwanted effects. But the same applies here:

The complexity of the task is no excuse for long-term deficits.

97

At our request, the hospital in question has started to report deficits

to be eliminated gradually. The process was still ongoing at the time of going to press.

Digitization in the healthcare system offers a multitude of opportunities

Treatment of patients can be made significantly easier and more efficient

to. At the same time, however, they create a large number of new dangers for the

Patient data. Those responsible must therefore guarantee

devote sufficient attention and resources to safety. methods

according to the state of the art are to be applied systematically, the effectiveness of

measures to be checked regularly - also from the point of view of external attackers:

- and to rectify any deficiencies found consistently and promptly.

98

Chapter 6 Health and care 7 Integration, social and

Work

7.1 Complaints office for refugees

About the establishment of an independent complaints office for refugees

we already have the Senate Department for Integration, Labor and Social Affairs (SenIAS).

reported several times.154 The position is intended to be easily accessible to people who have fled

Provide an opportunity to find out about grievances and problems related to their

to complain about accommodation. You should be able to take the hurdle

having to go to a government agency. As part of our consultations

We have repeatedly pointed out that it is necessary to carry out the tasks of these

Body to be anchored in law in order to create legal certainty for those affected.

A

and

s

i.e

e

right

P

right

a

x

i

s

Such a legal basis for the activities of the independent complaints

position has now been created.155 The for a transitional period with our

Support developed solution, the activity of the complaints office on the basis

legitimizing the situation of consent could thus be replaced. We have

accompanied this process intensively. In doing so, we have sensitized SenIAS to

that in the area of accommodation for homeless people, different federal

and state laws are affected. Mention should be made e.g. B. the Asylum Act (AsylG), the Asylum

Applicant Benefits Act (AsylbLG) or the General Safety and Regulatory

law Berlin (ASOG Bln).

Since in this respect the processing of personal data is also based on the respective

measured by the statutory tasks performed, it was important to

ben of the complaints office. This is with the new legal regulation

he follows. At the same time, it is made clear there that processing personal

154 Annual Report 2019, 7.1 and Annual Report 2020, 6.1

155 Accommodation Complaints Act (UBeschwG)

ner data of the people who have fled by the independent complaints office

requires written consent from the complainant.156

We welcome the fact that SenIAS has taken up our suggestion and that the tasks of the

independent complaints body has now been legally defined. With the independent

Complaints office can make an important contribution so that refugees

People low-threshold grievances in connection with their accommodation

can claim. Especially with projects like these, however, a special

whose attention to the protection of people's personal data

to judge. Violations of personal rights would be here with a special

severe loss of trust. We assume that the special

Guaranteed to comply with data protection requirements when handling complaints

become.

7.2 Housing the homeless “at the push of a button”

s

i

x

a

right

P

right

e

i.e

s

and

A

With the ambitious project "City-wide control of accommodation"

(GStU), which we reported on last year,157 SenIAS plans to

the need-based allocation of accommodation places for the homeless

across districts using a central IT process. In doing so

capacity planning and occupancy control "at the push of a button" and

be supported. Since sensitive data, e.g. B. Health data or

the sexual orientation, of very different groups of people such as

Asylum seekers or homeless people should be processed centrally, it is

particularly important to consider the data protection requirements from the outset

seek.

As a central component of the "Berlin Master's degree" presented by SenIAS in September

plans”158, the GStU project also serves the goal of reducing homelessness in Berlin by

to be overcome in total by 2030.

156 § 2 sentence 1 UBeschwG

157 JB 2020, 6.2

158 See “Berlin master plan to overcome homelessness by

Year 2030", at: https://www.berlin.de/sen/ias/_assets/aktuelles/2021_09-02-master-

plan2030.pdf

At the end of the year, SenIAS started the pilot phase of the GStU, the preliminary

riding we have supported in intensive consultations. As part of the pilot project

was able to create a data protection framework for the use of the IT specialist procedure for

the allocation of accommodation places in four district accommodations and a

of the State Office for Refugee Affairs (LAF).

become. In view of the different legal tasks that are to be carried out by the

ten authorities are perceived according to different legal provisions

it is important to identify the respective responsibility for data processing and the respective

to establish legal powers. For the use of the IT specialist procedure was

it necessary to define the access rights. Finally, we worked towards

that the necessary order processing agreements between the parties involved

actors have been completed.

SenIAS plans to further develop the project in the future by creating a

ner "Central Service Unit GStU". contract and accommodation management as well

Billing and quality assurance are to be centrally located there. Since the

Accommodation of the different groups of people, however, according to different

legal regulations, some of which are in federal law and some in state law

are located, the applicable to the processing of personal data

regulations are carefully examined. Whether to set up such a central

Be legal in view of the different legal frameworks

can be shown requires closer examination.

Overcoming homelessness is an important social state challenge

financial support. However, it must not be forgotten that the task

the accommodation of the different groups of people in different

laws is located. This means that the data protection laws

differentiate requirements. For a further development of the

project GStU beyond the pilot operation, the legal

to explore the general conditions. We will continue to consult on that

participate in the project.

8 Employee data protection

8.1 A list of information about everyone

employees during the probationary period

s

i

x

a

right

P

right

e

i.e

s

and

A

A company has hired a large number of service staff. Shortly before the

At the end of the probationary period, the management appointed the superiors of the service staff

instructed to create a list of employee information for internal

to be able to justify which employees should be dismissed during the probationary period

len. Some of the information on the list was not properly related

with their purpose.

In addition to some master data, the list contains brief assessments of the

worked and partially made recommendations for dismissals during the probationary period

ten. A good third of the employees were rated as “critical” or “very critical”.

For almost a fifth of the employees, the recommendation was made to

cancel the probationary period. In a table column entitled "Reason" were

partial work motivation, sick days, social or political attitudes, possible

interest in a – not yet existing – works council and often non-

driving reasons that stand in the way of a flexible division into work shifts

would, listed. Such reasons could be other activities, studies or a

be a hobby. Two people also noted that regular psychotherapy

dates would conflict with the desired flexibility.

The company has stated at our request that the list is for the purpose

should be able to objectively assess the performance of employees. On that basis

should be decided whether the employment relationship should be continued. The list became

by the manager of the service staff by e-mail to the management and the

sent to HR department.

Companies are allowed to consider internally whether they want employees within the

terminate the trial period. Since decisions are made here about several employees

should, nothing speaks against a tabular list.

102

8.1 A list of information about all employees on probation

However, the content of the list was sometimes extremely problematic, because of course

only personal data that is not processed

subject to a ban on trading. The information must be in a permissible

related to the employment relationship.

In the list, it was often stated that the persons responsible for duty planning were not

flexible enough, supplemented with the justification why they are at certain times

can't work. It must be given to an employer for his or her

their decision to continue an employment relationship regularly

that the employed person is not available at certain times. On this

basis, it can be decided whether the specified available time is sufficient,

to continue the employment relationship. This applies to an increased extent to information

like “going to psychotherapy”. This is a health

Date that is subject to a processing ban and for the processing of which

Employee data protection does not provide for an exception here.159

With a total of five employees, there was an interest in the works council or another

form of commitment to collective employee interests. This information

are in no way connected with the allegedly pursued by the company

purpose of conducting a performance appraisal of the employees. Because interest

in a works council, some or some employers may find it a thorn in their side

this information is not a statement on the performance of the employees. On

Demand has informed the company that these comments have also been made

to support the establishment of a works council. Evidence that this

The company was unable to provide any support for the claim. On the contrary: four

of the employees concerned were dismissed during the probationary period, with the fifth person

a termination agreement was concluded.

Much of the information contained in the list was provided by the employees of their

set self communicated. For example, if they ask for a specific classification in e-mails

asked for the duty roster and gave reasons for this. In this respect, a first

not prove the suspicion that employees have been spied on.

However, information provided by employers in this way may also

are not processed further for the stated purposes.

159 See Art. 9 Para. 1 GDPR, Section 26 Para. 3 BDSG

Since a managerial employee, on the instructions of the management,

has carried out the processing and has serious consequences during the data processing

We have started the procedure

handed over to our sanctions office to check whether a fine procedure has been initiated

shall be.

Employers may consider to what extent employees continue to

are to be employed and in this respect also process personal data.

However, the data processed in this way must be suitable for this purpose at all,

which means that they are directly related to the employment

not have to stand.

8.2 Must legal trainees dem

Court of Appeal their state of health

communicate?

s

i

x

a

right

P

right

e

i.e

s

and

A

Before legal trainees are taken to the so-called preparatory

medical service, they must submit a declaration of their health

state of health. In this they should indicate whether they are attending a physical or

mental illness for which they are being treated or which

requires treatment.

The legal basis for generally obtaining a declaration of health status

len, is located in the Berlin Lawyer Training Act (JAG). It says there that the

Admission to the preparatory service can be refused if the applicant

the applicant suffers from an illness which the proper training seriously

could affect or endanger the health of others.160

In most cases, applicants are not obliged to provide qualified information

to reveal information about their state of health. It is an exception if

Applicants know that due to their state of health, they are the target

activity cannot be carried out. In this case there is even a revelation

160 Section 10a (2) No. 2 JAG (until September 24, 2021 in Section 20 (2) No. 1 Berlin Lawyers'

training regulations - JAO - regulated)

104

Chapter 8 Employee data protection 8.3 Free access to applicant data

obligation to possible employers. Concealment can otherwise be considered malicious

deception, as a result of which the employment relationship on the part of the

can be rescinded.

Because of this clear objective of the legal requirements, we have

mergericht asked the query of the state of health to the wording of the law

adjust what the Court of Appeal did at the end of last year. future appraisals

Ber:innen now only have to state that they suffer from a disease that

is likely to seriously impair proper training or

likely to endanger the health of others. information about the disease itself

are voluntary. This voluntary additional information enables the Court of Appeal to

to make a different assessment yourself and to give a person despite these explanations

to grant access to the training.

Future employers and training positions may also work in public

Service will only collect Health Information that it is legally authorized to collect

are. This includes only such information that has a direct impact on

have the employment relationship.

8.3 Free Access to Applicant Data

At the end of August we received a notification that a security hole in a

software for scholarship portals access to a large amount of personal

Generic data from various study foundations is possible. The insecure software

was mainly used to provide scholarship application portals,

where a large amount of partly highly personal data is stored.

Due to the respective orientation of the study foundations concerned, there were also

special categories of personal data, such as religious affiliation or

Political belief and belief data affected.

A

and

s

i.e

e

right

P

right

a

x

i

s

We were informed by email about critical vulnerabilities in a software

mised, which to provide different portal solutions of different

study foundations. The software is developed by a Berlin company

and expelled. The e-mail was sent not only to us but also to the Federal Office for Security

in information technology (BSI) as well as to the software manufacturer itself

105

contained a detailed report on several different vulnerabilities in the

portal software.

By exploiting the vulnerabilities, attackers would have been able to

create a user account, query the database, uploaded documents

ments and to set up a user account with administration privileges

see.

The application portals of four different study foundations were also affected

different orientations, and in the case of a foundation, a portal that

at:innen is used for exchange. Applicants for scholarships from the foundations could

upload their documents to the portals as part of their application and so the

provide foundations. A total of around 350,000 documents were accessible,

highly personal data, such as copies of ID cards, certificates of enrollment,

Letters of recommendation and motivation included.

Due to the respective orientations and focal points of the study foundations concerned

This data also included sensitive personal information, such as e.g. B.

on religious affiliation and proximity to political parties. Because of the high

There is a risk to the rights and freedoms of data subjects with such data

regularly assume a high need for protection and appropriate measures are

to take measures that are suitable for effectively reducing these risks. That was

in this case, however, it was obviously a criminal offense.

It was easy for us to understand the documented vulnerabilities. The

Software manufacturer reacted quickly to the message and made changes to the software

ware that should prevent exploitation of the vulnerabilities. After

another report by security researchers, who pointed to remaining vulnerabilities

bodies pointed out, these were also closed.

The cause of the problem was the incorrect use of a software framework161, which

che caused the authorization check not to work as intended and

161 A software framework is a kind of construction kit that software developers use in different ways

provides reusable basic functions that can then be used when creating

can use more complex programs.

that more information than necessary is given to the users of the website

were delivered.

The manufacturing company informed us that the vulnerabilities found as a reason

were taken, an outside company with a security check of the product

to commission.

Providers of service portals must ensure that the data stored there

data is protected against unauthorized access. Is it a matter of

Providers should ders sensitive data on a large scale, but also the

Persons responsible for using the software should take special care

and actively check whether the systems used and their configuration

have the necessary safety features.

107

9 housing, urban development,

Services of general interest and the environment

9.1 Online broker publishes tenant data

on the Internet

A company focused on the online marketing of housing offers

on his website the possibility of documents on the planned sale of a

to discard property. For the anonymization of the documents stored there

not sufficiently taken care of by the online broker.

s

i

x

a

right

P

right

e

i.e

s

and

A

The company offers several services in combination. Next to the

Valuation of real estate by own or with the company cooperating

Brokers: the services also include the creation and support of

purchase notices and the procurement and provision of documents required for the

real estate business are needed. These documents regularly include

mente with very personal data, since it involves assets, liabilities and

often also the living space. In addition, third-party data is affected if the

the property in question is rented. Also documents of entire apartment owners

Community groups are sometimes filed in the company's online offering.

We have received several complaints in recent years about the fact that the

Provision of the documents by the company concerned the necessary

anonymisation of the documents is not carried out sufficiently. Also reported

the company itself regularly reports data leaks that lead to unauthorized

calling for personal documents.

Confronted with the complaints, the company referred to a

Subcontractor used to prepare the documents. It is still in individual cases

not ruled out that insufficiently redacted documents will be published

would. A task force will be deployed to deal with the reported data leaks.

After the next data leak was reported, the company said it would

The work of the "Task Force" will be intensified. On the occasion of the notification of another

9.2 Data processing by smoke detectors?

new data leak, the company announced a step-by-step principle, so now only

qualified prospective buyers were given access to the documents.

The various complaints and company reports become

evident that the company's will or ability to comply with data protection

forms handling of the personal data of third parties is lacking. It would have in the

better control subcontractors acting on their own behalf or redacting

have to check the personal data in their online offer themselves

senior After the company received a warning last year,

was spoken, our sanctioning body is now running a fine procedure because of the

named violations of the rights of the publication of their documents

affected persons.

Documents required for the processing of contracts for residential rent and real estate

lien purchase required can also be done digitally through secure online platforms

be replaced. Personal data that is not required must then be

however, blackened out and the companies commissioned for this activity, if any

are adequately controlled by the portal operators.

9.2 Data processing by smoke detectors?

Since January 1, 2021, smoke alarm devices have been installed in private homes

mandatory by law. The devices used for this are now so

ensures that their functionality is checked and serviced by radio

can.

A

and

s

i.e

e

right

P

right

a

x

i

s

In previous years, we have repeatedly received requests for advice from Bürger:in-

with regard to possible monitoring by means of smoke alarms to be newly installed

reporting devices.

Although smoke detectors must have sensors to fulfill their purpose,

which can, for example, measure distances to prevent the alarms from being covered by furniture

etc. to recognize. However, these sensors are not suitable for detecting the presence

to capture people for motion profiles or to make sound recordings.

109

In addition, the low-power radio transmitters built into the devices would also be

unable to transmit large amounts of data to the outside world.

However, a smoke alarm device cannot do without personal reference. every

devices must be able to be assigned to a specific housing unit if the devices

provide information about their functionality by radio. Usually the

device number as well as the corresponding maintenance logs are sent to the outside. The

The responsible body must then be able to allocate where a possibly reported function

fault is to be remedied. Indications of unauthorized processing of these

However, we could not determine any data.

The protection of personal

Son-related data a role if device number and functionality

be transmitted to the responsible departments during maintenance work. Data about

Presence and behavior of people within the sensor range of the devices

are not collected and processed according to our knowledge.

9.3 Misuse Prohibition Act

In September, the House of Representatives amended the misappropriation agreement

bot law (ZwVbG). The ZwVbG regulates i.a. the rental of holiday

Apartments in Berlin and the Consequences of Unauthorized Renting. through the novel

should the authorities be given the opportunity to fight illegal rental

In the event of suspicion, certain information can be obtained directly from

Query online mediation platforms, for example to punish administrative offences

to be able to

A data query on digital mediation platforms for providers of

agreed apartments or after concluded contracts for a specific

Apartment, is referred to as inventory data query. The stock data is

to be distinguished from the usage data: Usage data is data that e.g. B. for the

Connection establishment to a website are necessary, such as IP addresses.

According to the so-called "double-door case law" of the Federal Constitutional Court (BVerfG)

All data queries need two legal bases: On the one hand, the requesting

authorities have the right to collect the data. On the other hand, they also have to

companies may be entitled to release the requested data.

In this respect, the ZwVbG can only create the legal basis for the authority that

Request data from mediation platforms. The legal basis for the data

publication by the operators of these platforms is regulated by federal law. Of-

half the ZwVbG refers to the Federal Telemedia Act (TMG).

At the same time, therein lay the difficulty of the legislative process: the relevant

gigantic provisions in the TMG were last changed in April because the BVerfG

found out last year that the regulations on inventory data disclosure in

TMG were unconstitutional.162 The decision of the Federal Constitutional Court was particularly

also about the requirements for inventory data information in the pursuit of order

violations. So the judgment concerned the kind of data queries that the goal of the

Berlin law amendment were. The Federal Constitutional Court has, with a view to the federal law

Regulations expressly require that it must be "about - also in individual cases - particularly

serious administrative offenses, which the legislature also expressly

must name". In the judgement, the BVerfG also considered the relevance of the usage data

reconfirmed for personal rights.

It is neither the task of our authorities nor of the state legislation to

constitutionally reviewed in the TMG. Nevertheless, it is striking that the

Publication of usage data in the current version of the TMG no limitation

was made for particularly serious administrative offences. Therefore has

our authority noted in its statement on the amendment to the ZwVbG that the

Constitutionality of the federal legal basis in the case of usage

data is unfortunately again doubtful.

Due to an amendment to the ZwVbG decided in September, the possibility

created the possibility that, in the event of suspicion, authorities can directly provide certain data

Companies can query the platforms for vacation rental brokerage

operate. As a result, there are doubts as to whether the new federal regulations

ments, in particular with regard to the (technical) usage data, the specifications

162 BVerfG, decision of May 27, 2020 - 1 BvR 1873/13, 1 BvR 2618/13

correspond to the BVerfG. The state of Berlin has no influence on this circumstance,

However, the state authorities should take this into account if they decide in individual cases

decide to also collect (technical) usage data.

9.4 Data protection consequences of the burst

rent cover

Last year, the House of Representatives passed the so-called rent cap. In the

On April 1st of this year, the BVerfG published a decision163 in which this

Mietendeckel was declared void because the state of Berlin was required to

Legislative competence was lacking.

This decision also had consequences under data protection law, because the law

to regulate the rent cap also contained a legal basis for the

expedient data processing, which is now eliminated. The Senate Department for Urban Development

ment and housing (SenSW), as one of the main people responsible in this

rich, turned to our authority. She asked for help with the transaction

of the failed law. The accumulated data had to be deleted immediately

s. At the same time, the question arose as to which documents the SenSW should use in future

Legal proceedings are still required and whether there are legal bases for further

storage are given.

For us, the creation of an overall extinguishing concept for all due to the rental

deckels collected data priority vs. the immediate implementation of individual deletion

long. Nevertheless, the maximum period of three months for the implementation of

to comply with the right to meet. The SenSW succeeded under pandemic conditions and

with inter-agency coordination, the review of further storage

reasons for all documents to be completed by the end of July. As a result,

there are no reasons for a further one beyond the state budgetary regulations (LHO).

Storage of the files in the responsible Senate administration. So the files became

as provided for in the archive law of the state of Berlin (ArchGB), the state archive

required. At the beginning of September, the state archives of SenSW issued the deletion permit.

163 BVerfG, decision of March 25, 2021 – 2 BvF 1/20, 2 BvL 5/20, 2 BvL 4/20

As a result, all of the data collected on the basis of the rent cover, which the Land

desarchiv were offered were deleted at SenSW.

The state archive now checks the archival value of the processes under its own responsibility

ability. This review was still ongoing at the time of going to press. After completing the archive

The documents that are not worthy of being archived are checked for their worth by the State Archives

also deleted.

9.5 Radio-based heating cost meters

On January 1, 2022, new regulations for recording heating costs will come into effect

Kraft,164 which also concern the transfer of personal data. The then

Mandatory electronic recording of heating and

costs replaces the annual visit to a billing company because the

usage data from e.g. B. radiators are transmitted electronically to the outside.

However, the consumption data can sometimes be very detailed and therefore

there is a risk to data protection.

A

and

s

i.e

e

right

P

right

a

x

i

s

With the radio-controlled recording of consumption data, the respective consumption

values are recorded using electronically operated devices and transmitted by radio or other network

factory technology to the cost-accounting departments. This happens in

in most cases via a station - e.g. in the hallway or basement - that receives the data

of the individual consumption meters in the house and initially stores them temporarily.

The values in this collection station are then transmitted by radio at certain time intervals

queried electronically by employees of the respective billing company.

The introduction of this digital form of consumption billing has for consumers:

many advantages in terms of transparency. Billing companies need to post about

the new rules also indicate comparative values from previous periods

and generally also provide consumption information on a monthly basis. This is how the

analyze consumption better, for example to be able to heat in a more climate-friendly way.

164 See Sections 6 – 6b of the Ordinance on Billing for Heating Costs (HeizkostenV)

However, the detailed recording of consumption data also creates risks

for the informational self-determination of data subjects. The electronically generated

The values recorded can partly provide information about the number of residents

of a dwelling, its presence, its consumption and usage habits.

The rules of the General Data Protection Regulation (GDPR) counteract these dangers

ments in that only the data required for the creation may be collected

of the legally owed billing are required. The survey and further

processing of data that goes beyond this purpose is only possible with an

informed and transparent consent by those affected. have to

Devices must be set from the outset so that only the billing-relevant data

be collected.

When converting to radio-based consumption recording, the people concerned should

always expect comprehensive information about the associated data traffic

work and do not hesitate, e.g. B. Information rights vs. billing company

men to assert.

Radio-based heating bills offer advantages in terms of transparency

and at the same time pose risks to privacy when data processing

goes beyond billing purposes. Those affected should responsible

authorities and companies insist on full transparency.

9.6 Disputes among allotment gardeners —

Does the GDPR apply?

s

i

x

a

right

P

right

e

i.e

s

and

A

The GDPR applies to the processing of personal data by private

persons in the exclusively personal or family sphere not applicable

(so-called household exception).165 With this household exception, the free development

of the personality of private individuals are protected from regulation. Typical

personal or family activities are i. i.e. R. in the areas of leisure, sport

or holiday taken.

165 Article 2(2)(c) GDPR

in the association

In private life, in friendships or in the family, this often occurs

Ask whether cases from these areas fall within the scope of the GDPR

fall. One of the complaints we dealt with concerned an allotment garden association

A dispute between a leaseholder of an allotment plot and her neighbor. Thieves-

chief objected to the fact that the neighbor had sent her a letter to her

private address and not to the parcel in the allotment garden association. Our

Investigations revealed that the neighbor gave the complainant's home address

rin from a time when the participants were friends. The then

The collection of the address data was therefore purely private, i. H. without any relation to one

professional or economic activity.166 spoke in favor of the so-called household exception

also that the said letter is a written exchange between

between two private individuals who focused exclusively on their leisure activities

ten within the framework of the neighborhood in the allotment garden association. The processing of

personal data found accordingly in the context of a neighborly and

exclusively private arguments. The complainant could

therefore not assert any data subject rights under the GDPR.

The scope of the GDPR is not open if it is a data

processing of a private individual in the context of a personal or family

activity.

9.7 Publication of membership lists in the association for

assertion of minority rights

A member of the association and the corresponding association contacted each with the

Consultation request to us, whether the list of members of the association to the association member

and two other members to convene an extraordinary membership association

collection could be published. The association initially had the publication

and transmission of the list of members to carry out an extraordinary meeting

members' meeting refused because the applying group according to the statutes

of the association for calling an extraordinary general meeting

A

and

s

i.e

e

right

P

right

a

x

i

s

166 See EG 18 GDPR

required number of votes167 by at least 25% of the members of the association

fulfilled.

Under association law, a right to inspect a list of members is often granted

Enforcement of minority requests, such as the convening of an extraordinary

formal general meeting, accepted. The

Publication and transmission of the list of members in individual cases due to the obligation of the

association, the exercise of statutory rights and/or minority requests

to enable necessary due to legitimate interests of the applicant

be livable without compromising the interests of the members of the association in the protection of their personal

data outweigh.168 The legitimate interest here lies in the right to cooperation

effect on the formation of will in the association, in particular through the perception of

minority rights are exercised and that the applicant club members

limbs must be proven.169

The members can assert their minority rights on the member

list to have enough members for the sub-

supporting an application to convene an extraordinary general meeting

lung to win.

When asserting minority requests, the size and type of the

to differentiate one. Although it seems disproportionate for larger clubs,

to require the members to enforce minority rights, first all members

to get to know the members personally and to ask them about the topic in order to

to achieve the required quorum of votes. However, at the same time it is not very

fair, e.g. B. in nationwide clubs with several million members,

issue a list of members to the applicants.

167 According to Section 37, Paragraph 1 of the German Civil Code, the general meeting of an association must be convened

if

neither the proportion of votes specified in the Articles of Association or, in the absence of a provision

Ten percent of the members of the meeting in writing, stating the purpose and reason

required.

168 See Article 6 Paragraph 1 Sentence 1 Letter f. GDPR

169 See AG Hannover, judgment of February 13, 2019 - 435 C 10856/18

in the association

In this respect, the board of directors must examine how a minority request for data

economical170 can be met. This can be done either by submitting the

member list to a trustee or lawyer or by forwarding the

Minority requests are implemented by the board of directors to the members

the, without the list of members being issued directly to the applicants or

must be transmitted. However, if the list is issued to the applicant

is given, an assurance must be demanded from them that the personal

to process data in the member list exclusively for specified purposes

and then to be deleted.

The personal data of the members of an association in the form of a

derliste may not be passed on to other members by the association without a legal basis

be published or transmitted. If individual members are minorities

rights, such as B. the calling of an extraordinary general meeting

ment, want to assert is the legitimate interest, e.g. the right to

Participation in decision-making in the association by the applying members

to prove. Before releasing the data, the association is obliged to check

whether milder means can be considered that are equally suitable for reducing the

eat the recipient:in to suffice.

170 See Article 5(1)(c) GDPR

117

10 economy

10.1 "Responsible data processing"

through banks

s

i

x

a

right

P

right

e

i.e

s

and

A

A bank informed all customers that they intend to

to advertise with services and products in the future that exactly match the respective

living and financial situation would correspond. For this purpose, almost all data, about

that the bank has can be evaluated. Among other things, the letter kept the

Bank under the heading "The data processed includes" the following

gifts:

• “Payment transaction data, such as e.g. B. Details of payees and payers

as well as information from purposes of use;

• Data that we collect when you use our online offering (such as websites, online

line banking and apps). These include e.g. B. Information about the of

Your chosen access path/communication channel (such as IP address, type of

device), date and time of use, information about your service history

and information about the online products you have accessed."

The letter had the subject "Responsible data processing" and contained

the indication that there is a right of withdrawal against the advertising.171 Several affected

fene have complained to us about the bank's approach.

The bank belongs to the Federal Association of German Volksbanken and Raiffeisenbanken

ken e. V. (BVR). This had its member banks the described procedure

recommended and a corresponding text made available. Since this

kens from different federal states was used, we have the result of our own

coordinated nationwide with the other supervisory authorities.

171 See Article 21(2) of the General Data Protection Regulation (GDPR)

10.1 "Responsible Data Processing" by Banks

The BVR assumed that the data analysis carried out here for advertising

purposes is lawful without the existence of consent. The basic data protection

ordinance (DS-GVO), data processing would also take place without the existence of a

allow the consent of those affected. 172 Direct mail represents a legitimate interest

173 Interests of those affected that are worthy of protection are also not affected, since they are

were informed in good time about the planned advertising and the right to object.

The legal opinion of the banking association is incorrect. In the recital

Based on the DS-GVO, it is determined that in particular if an affected

the person concerned cannot reasonably expect further processing,

their interests and fundamental rights outweigh the interests of the person responsible

can.174

Those affected will generally not expect banks to collect payment transaction data

and evaluate their customers' internet behavior in order to be able to advertise them better.

Notifying those affected does not change this. The expectations of

affected persons cannot be affected by the data provided for in the GDPR

Mandatory information175 to be expanded.176 During non-performance or poor performance

the information obligation, the result of the assessment, i.e. from the point of view of the person responsible

negatively influenced, the proper fulfillment of the information obligations has none

Impact on the balancing of interests.177 The bank's information letter

does not lead to the legality of data processing.

The legitimate interests of those affected are therefore also higher than the economic

to assess the bank’s interests, as the payment transaction data

precise profiles can be created for those affected. Also the usage data

172 See Article 6(1) sentence 1 lit. f GDPR

173 See EG 47 last sentence DS-GVO

174 EG 47 sentence 4 GDPR

175 See Art. 13, 14 GDPR

176 See Conference of Independent Federal and State Data Protection Authorities

der (DSK), guidance of the supervisory authorities for providers of telemedia, p. 16; on-demand

cash at https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

177 So also the European Data Protection Board (EDPB), Guidelines 8/2020 on the targeting

of social media users, version 1.0, par. 60, p. 18; available at https://edpb.europa.eu/

our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-

media-users_en

of the online offer are very worthy of protection, because they contain information about

lifestyle of those affected.

Negotiations with the banking association have not yet been completed,

However, the affected bank must expect that we will object to their advertising campaign

- as long as the procedure is not changed - a prohibition order can be issued.

Payment transaction data and data about the use of the online offer

Bank may only be used for advertising purposes with the consent of the person concerned.

the.

10.2 Transparency in Scoring Procedures

A customer applied for a credit card from his bank. The request was made by the

Bank rejected on the grounds that they had based on probability values

ten carried out a credit assessment (so-called scoring), this showed that

he does not have sufficient creditworthiness.

s

i

x

a

right

P

right

e

i.e

s

and

A

Because the bank customer has a good SCHUFA score and is a successful lawyer

is, he doubted the correctness of the score value calculated by the bank. He be-

carried information about the data on the basis of which the bank made negative credit

dit assessment has come. The bank then informed him about the to his

person stored data and gave general information about their credit

but refused to tell him why, in his case, she

ten credit rating. The right to information178 would not go that far, moreover

the bank can invoke a trade secret.

The bank customer also asked the bank to check his creditworthiness again. The

Bank then informed him that the second test had again shown that his

creditworthiness is not sufficient for a credit card. The person concerned complained

about the lack of transparency in credit scoring.

178 See Art. 15 GDPR

The bank violated the transparency requirements for scoring procedures. At

automated individual decisions such as credit scoring leading to rejection

leads to the conclusion of a contract, the data subjects have the right to

to argue and present their own point of view.179 To perceive these

Effective rights must at least also include the essential reasons for the persons concerned

notified of the relevant automated individual decision and its impact

and explained in more detail, otherwise there is an objection to the decision

not possible. In the case of credit scoring, there is a so-called “right to explanation”, i.e

an obligation to justify and explain with regard to automated

ter decisions.180 The bank is therefore obliged to support customers

Automated credit decisions about the main reasons for a credit refusal

to teach. This includes information on the database and the use of

certain factors or parameters on which the specific decision is based

became. The information only has to be detailed insofar as this is necessary for

the traceability, but not for the recalculability of the automated

decision making is required. “The core concern of any transparency is that

to let the data subject understand processing processes and the possibility of

intervention.”181

Since the bank refused to make the credit decision transparent, the

Process submitted to our sanctions office.

Is affected by an automated credit decision due to a

Credit scoring does not provide a service, the decision is up to those concerned

vs. to make transparent.

10.3 Consent to Telephone Call Advertising

A bank informed its customers by telephone about how to use the

Credit card paid on the Internet (service call). At the end of the conversation, the

Those affected asked whether they agreed to this, also by telephone in the future

179 See Art. 22 (3) GDPR

180 See Gola, DS-GVO, Franck, Art. 15, paragraph 19 with further references.

181 Gola, DS-GVO, Franck, Art. 15, para. 19

A

and

s

i.e

e

right

P

right

a

x

i

s

to be advertised. The consent to the telephone advertising was subsequently

confirmed in writing. Some of those addressed denied that they had asked for consent by telephone

and filed a complaint with us.

The question of whether the bank inadvertently gave no consent at all in the complaint cases

had obtained, can remain open, since the bank's approach is independent of

of was unlawful. The processing of the telephone number for the purpose of collection

A consent to future advertising measures was due to a lack of legal basis un-

permissible, in particular it was not about lawful processing

Safeguarding the legitimate interests of the person responsible.182 Due to legal

According to the OVG Berlin-Brandenburg, it can be assumed that the collection

to classify the consent for future advertising measures as (direct) advertising

ist.183 Direct advertising can in principle be a legitimate interest of those responsible

body for the processing of personal data.184 The German law

However, in implementing European law, geber has decided that advertising

a phone call vs. a consumer without prior

express consent of the persons concerned is not lawful.185

The Bank has the option of obtaining consent to telephone advertising using other

means of communication than by telephone. A phone call with two

For different purposes (service call, consent to advertising) lives a certain

“Surprise Effect” inside. Because the person concerned will not regularly

wait that you:e contractual partners:in a call for the purpose of contract

pursue another, self-interested purpose.

We warned the bank for their behavior. The bank informed us

that in future it will no longer obtain consent to advertising by telephone. The previous

In addition, previous consents are no longer used by the bank.

Service calls may not be used to obtain consent to telephone

to give advertising.

182 See Article 6(1) sentence 1 lit. f GDPR

183 See OVG Berlin-Brandenburg, decision of July 31, 2015 – OVG 12 N 71.14

184 See EG 47 last sentence GDPR

185 See § 7 Para. 2 No. 2 Act Against Unfair Competition (UWG) i. in conjunction with Art. 13

Para. 3 Directive 2002/58/EG (Privacy Directive for Electronic Communications)

10.4 Unsolicited advertising after alleged Participation in a competition — Evidence of the declaration of consent

Again and again we receive complaints from the persons concerned, the advertising

received from companies unknown to them. In response to

Requests for information then often refer advertising companies to one of the

affected persons vs. a third party as part of a sweepstakes

submitted declaration of consent.

A

and

s

i.e

e

right

P

right

a

x

i

s

According to the DS-GVO, the responsible body must be able to prove that the

data subject has consented to the processing of their personal data186.

In this respect, the previous case law of the Federal Court of Justice (BGH) on the

law against unfair competition (UWG)187 continues to apply, according to which

it is not sufficient if it is merely stated in abstract terms that consent has been

was shared. "If, for example, in the context of a data protection dispute, the

effective consent is disputed and the responsible body cannot

provide unequivocal proof of this, it can be assumed in case of doubt that

there is no legally effective consent.”188

Can not give consent or not in the form and under the conditions that

resulting from the DS-GVO189, can be proven, the processing of personal

personal data for the purpose for which a declaration of consent was

nes other permission would have to exist, inadmissible. Recital 42

DS-GVO states that the responsible body should be able to prove “that the

data subject has given their consent to the processing operation". The

The responsible body must therefore prove how and on the basis of which

declaration or active action made before the start of processing

affected person has given their consent. It must be demonstrable that the

Declaration made in advance.190 It must also be proven what the content of the consent was

186 See Article 7(1) GDPR

187 See BGH, judgment of February 10, 2011 – I ZR164/09

188 Ehmann/Selmayr/Heckmann/Paschke GDPR, Article 7, para. 68

189 See Art. 4 No. 11 GDPR and Art. 7 GDPR

190 See Article 6(1) sentence 1 lit. a GDPR ("has ... existed")

has consented, in particular to which processing of which data for which purpose

became. Furthermore, proof must be provided that the person concerned

Granting their consent all the necessary information has been given so that

this the decision on the basis of sufficient information about risks and

Consequences of consent recognized. To be logged and documented

hence not only the content of the declaration, but also the procedure, such as the declaration

came about, including specifying what information about the scope and

the purpose of the data processing and the right of withdrawal of the data subject

submission of the declaration of decision-making.191

In numerous complaints procedures, a company was able to

men of a competition vs. consent given by a third party

Regularly failing to provide unequivocal proof of people receiving advertising. Our

The fine office will now examine appropriate sanctions.

Responsible bodies are obliged to provide unequivocal proof that the affected

interested persons in the processing of their personal data for advertising

purposes have consented.

10.5 Applicability of the GDPR in favor of

legal entities?

s

i

x

a

right

P

right

e

i.e

s

and

A

The subject of numerous inquiries that we receive is the applicability of the

DS-GVO in favor of legal entities. For example, we received complaints

to promotional e-mails sent to general functional e-mail addresses of legal entities

were directed to, but addressed the management by name in the text section.

The GDPR applies insofar as personal data is concerned.192

“Personal Data” means any information relating to an identified

or identifiable natural person.193 Recital 14 DS-GVO

clarifies the regulation on "personal data of legal entities

191 See Taeger/Gabel/Taeger DS-GVO, Art. 7, paragraphs 37-40

192 See Art. 2 Para. 1 GDPR

193 See Art. 4 No. 1 GDPR

companies and in particular companies established as legal entities” as non-

reversible. Individual members of a legal entity or one or more behind

However, natural persons belonging to the legal person are protected if

the information about the community of persons also relates to them. In this way,

via a GmbH to shareholders or managing directors of this GmbH

related, if between the GmbH and the people standing behind it

there are close financial, personal or economic ties. With such

Links between a natural person and a legal person, often at

of the "one-person GmbH" can generally be assumed

that a reference to the natural person behind the legal person

stands and thus the scope of the DS-GVO is opened.194

In the complaints we have received, in which managing directors of a

GmbH from the advertising company, with which you have never previously been in contact

were in contact, were addressed by name in advertising letters, we

because a warning was issued.

The principle remains that the GDPR applies to legal entities as such

does not apply. However, this does not apply when it comes to protecting the

natural persons standing behind the legal entity.

10.6 The – limited – powers of

Group data protection officer

Data protection law provides that companies have a data protection officer: n

have to call if u. at least twenty people constantly with the automatic

tized processing of personal data.195 companies

in a group of companies196 it is possible to have a common group

to appoint a data protection officer,197 who will carry out the tasks for each legal

A

and

s

i.e

e

right

P

right

a

x

i

s

194 See Gola, DS-GVO, Gola, Art. 4, para. 25 and ECJ, judgment of November 9, 2010 -

C-92/09, C-93/09

195 See § 38 BDSG

196 Art. 4 No. 19 GDPR defines a group of companies as: “[A] group consisting of a

the controlling company and the companies dependent on it”.

197 See Art. 37 (2) GDPR

table independent companies of the group of companies. In this

In this case, every company no longer has to have its own data protection officer

to name.

We have received inquiries from companies and works councils about the role of corporate

data protection officer. In doing so, companies primarily have to comply with the

inquired about the duties and obligations of the group data protection officer. The works councils in

were particularly interested in the rights of employees. Since the beginning

the pandemic, there were also more questions about the accessibility of corporate data

protection officer.

Group data protection officers may not be hindered in their work by the company

be changed. The group of companies must access the data protection officer

grant to all personal data and processing operations whose

Knowledge required to perform the function. The necessary resources198
must be present to the extent that the data protection officers of their work
can pursue unhindered. Although the employer may:
gent to perform the function. However, it must be dimensioned in such a way that
the person can perform the task properly.199 Because of the size
of the tasks that arise within a group, the data protection officers
carried here often flanked by a larger team. In this case, not only applies to
the group data protection officer, but also for the employees
the team's obligation of confidentiality200.
Corporate Data Protection Officers should be from each branch of the company
be easy to reach from. Employees should receive this within one business day
can reach personally. Employees should deal with any issues related
to the processing of their data and with the exercise of their rights to the person
can contact.201 The specifications are particularly
pen is often difficult to fulfill. To support the work, the respective individual

198 E.g. employees, premises, IT infrastructure and financial resources

199 See Art. 38 (2) GDPR

200 See Art. 38 (5) GDPR; Employees must confidentially contact the
Group data protection officer. The group data protection
commissioner may report a data protection violation to the supervisory authority.

201 See Art. 38 (4) GDPR

companies have therefore appointed additional data protection coordinators. This sub-
support the group data protection officers in the implementation of their tasks
at their location or in their department. They are also contact persons

for inquiries from employees on site.

127

11 Transport, Tourism and credit bureaus

11.1 “Jelbi” – the BVG mobility app — An interim conclusion

The BVG operates the "Jelbi" app, which combines various mobility offers.

be ned. With the app, driving information can be obtained and bookings from both

Bus and train as well as e.g. by scooter, bicycle, taxi or car, also in combination

tion, be made.

s

i

x

a

right

P

right

e

i.e

s

and

A

The app was developed and put into operation in 2019 without us being involved

became. We only found out about it from the press. Already during cursory examination

of the app, we have identified numerous data protection violations. About this we have

reported in detail in our 2019 Annual Report.202

Ever since the app became known to us, we have been in constant exchange

with the BVG. In the course of this we have made some improvements to the data protection

veaus can achieve at "Jelbi". The BVG has contradictions and ambiguities in

the declarations of consent and data protection notices. She now points

e.g. that she assigns her claims to a company, which then transfers them

claims in its own name. Unlike before, new customers who use

want to pay by credit card, no more SCHUFA inquiries were carried out. With these

an assessment of the creditworthiness is not necessary due to the lack of default risk. In addition, the

BVG no longer provides information about the respective gender of the users to the

company to which it assigns any claims. Be within the app

Furthermore, no cookies are set by third parties. The US company that

previously verified the telephone numbers of the users for the BVG is also not

used more. 203 This list does not claim to be complete.

202 JB 2019, 4.1

203 For the general problem see 1.1

Nevertheless, there are still points, because of which we "Jelbi" for two years

cannot confirm data protection compliance after starting the app. This concerns before

above all the use of other US services, in particular a cloud pro-

vids.

"Jelbi" is currently in a re-tendering process. In 2022 a new

edition of the app. As part of the tender, the BVG has various

Data protection and IT security requirements established. A firm assurance

towards the use of the problematic service providers we have addressed

However, we did not receive this from the BVG. are in need of clarification

Furthermore, about the duration of the storage of the driving license data, the transmission

Distribution of e-mail addresses to the receivables buyers or the currently existing one

Obligation to provide the cell phone number when registering with the app.

We consider a concept like "Jelbi" to be generally implementable in compliance with data protection. here

However, certain legal and technical requirements must be observed. The

BVG assumes that it will be able to meet these in the new version of the app at the latest.

to. We will accompany the implementation attentively from the beginning, so that not

Another app that is incomplete in terms of data protection comes onto the market.

11.2 Check-In/Check-Out via smartphone in public transport

Transport companies throughout Germany have recently been offering so-called check-in/check-

out systems on a digital basis. Passengers enter start and end times in an app

a ride. The app records the distance traveled and then calculates on the basis

location of the cheapest possible fare. In comparable check-in/

Out or Be-In/Be-Out systems, the app records the start and/or end of a journey

independent. Also comparable, but more extensive, are based on such

cher systems so-called airline tariffs introduced. Billing no longer takes place here

based on tariff zones, but based on the distance between the start and destination

tion. The BVG also gave us a project to test a corresponding check-in/

Check-out system introduced to a limited extent.

A

and

s

i.e

e

right

P

right

a

x

i

s

129

When using such systems, compared to buying traditional tickets

processes a multiple of the personal data of the passengers. this concerns

in particular the comprehensive collection and storage of movement data.

In the BVG system, for example, all the stations that are used should not only be recorded,

but also stored for one year. In addition to the

th stations, in particular location data of the passengers are processed. Should

the passengers do not log out accidentally or due to technical problems,

their location data will also be processed beyond the journey.

This data can be used to create comprehensive movement profiles. So can

conclusions about the place of residence and work as well as the leisure time behavior of the passengers

to be pulled. In particular, it is also possible to draw conclusions about sensitive data

such as visiting a doctor's office or place of worship. Such systems are

therefore not unproblematic.

In addition, there are transport companies that want to introduce such systems

agreed pitfalls in the concrete implementation, especially when based on existing ones

Third-party apps are used. In other states are such

Some apps are used more extensively than before in Germany. are natural

the providers of these apps make little effort to adapt their products to the local

ben to adapt, as this is associated with additional effort and costs. In addition

Would such third-party providers want to use the app of the respective

The data collected by the transport company is often also used for further development

use their own app. This is problematic for public transport companies,

since supporting the further development of an app from a private company

is not part of its task of "implementing local public transport".

The service provider commissioned by the BVG in connection with the project is planning

In addition, numerous data of the passengers, e.g. their contact and locomotion data

ten to transmit to US companies, such as cloud services. The

The use of such service providers involves considerable risks for the persons concerned

connected, as the transmitted data is also accessible to US authorities

are subject to, and only permissible under very narrow conditions.204 These

Requirements are currently not met by the BVG.

204 See 1.1

We have these objections to of the BVG and are in an internal

active exchange with the BVG about the project. There have already been some successes

be achieved. For example, the BVG has comprehensively adapted documents in which

the passengers have so far only been insufficiently informed about the risks of the system

the. In addition, no subcontractor was used. Whether the app

it remains to be seen whether the BVG can ultimately be implemented in compliance with data protection regulations.

App-based check-in/check-out or comparable systems contain considerable

risks for users. This is particularly the case when transport companies

men on existing third-party apps and on service providers in the

resort to the United States. In addition, certain technical specifications must be observed.

In addition, such systems are subject to the fundamental problem that means

movement profiles of the passengers based on the numerous data, some of which are sensitive

can become. They are therefore already conceptually problematic. Should a

transport companies nevertheless stick to the introduction of such a system

want, there should be a great deal of data protection right from the start of the planning phase

pay attention, e.g. through narrow earmarking and short storage periods

necessary data to be processed.

11.3 Processing of data on energy supplier

contract through credit agencies

Some credit bureaus were considering a "pool" of data records

Electricity and gas contracts between private individuals and energy supply companies

take (so-called energy supplier pool) to create. In these should also data about

Contracts are transmitted in which there were no payment defaults (so-called

positive data).

A

and

s

i.e

e

right

P

right

a

x

i

s

Credit bureaus are generally not allowed to collect positive data on private individuals due to predominantly

of legitimate interests205. The legitimate interest regularly predominates

interest of the data subjects to determine for themselves how their data is used.

The conference of the independent data protection supervisory authorities of the federal government

205 See Article 6(1) sentence 1 lit. f GDPR

and the federal states (DSK) as early as 2018.206 After the considerations on the

Creation of the energy supplier pool became known, the DSK made this decision

for the energy supplier pool again confirmed.207 The template for the recent

The decision was essentially made by our authority together with the state

North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information.

Energy supply companies regularly offer new customer discounts. means

some positive data on energy supplier contracts (number and duration of the respective

contracts) it would be possible to determine whether consumers regularly use their energy

change power supply companies in order to obtain permanently favorable conditions.

The persons concerned could then be excluded from new customer discounts

become. However, excluding "bargain hunters" does not constitute a justified interest

esse dar. The data subjects have the right to suppress competition between the

to use energy supply companies, especially since these are the incentives to

to change companies, have created themselves.

Even if there were a legitimate interest, according to the general

my principles for the processing of positive data by credit agencies, the Internet

eat of the persons who behave in accordance with the contract. These may expect their

Data not, insofar as going beyond the purpose of the contract, to credit bureaus

be told.

The processing of positive data on energy supplier contracts through information

on the basis of a legitimate overriding interest is not permitted.

The interest of data subjects in sovereignty over their own data

prevails. In particular, they are entitled to prevent competition between energy

to use utility companies and to switch between them several times.

Otherwise they would (further) become transparent consumers without that

they would have given cause for this through their behavior.

206 DSK resolution of June 11, 2018: “Processing of positive data on private individuals

by credit bureaus”; available at https://www.datenschutz-berlin.de/infothek-und-service/

publications/decisions-dsk

207 Decision of the DSK of March 15, 2021: "'Energy supplier pool' must not lead to transparent

lead users”; available at https://www.datenschutz-berlin.de/infothek-und-ser-

vice/publications/decisions-dsk

Chapter 11 Traffic, Tourism and Credit Bureaus 12 CCTV

12.1 Body cams at Deutsche Bahn

In 2016 and 2017, Deutsche Bahn Sicherheit GmbH (DB)

ment of a pilot project to equip their security forces with bodycams

Self-protection and tested as a de-escalation measure.208 Since 2018,

set of bodycams at selected train stations209 now in regular operation. a first

DB now has an evaluation report on regular operations for the years 2019/2020

submitted.

A

and

s

i.e

e

right

P

right

a

x

i

s

The following principles for regular operation were derived from the experience of the test phase

fixed:

• Bodycams are only used in areas and during business hours

those with a view to the registered attacks on the security forces as critical

be rated. These so-called "crime rooms" are subject to an annual

new assessment and thus review.

• Bodycams are switched on when switched off and not in stand-by mode.

set. Pre-recording is excluded. There is no sound recording.

• In the event of an emerging critical situation, the security

security forces to a possible recording by the bodycam. Should

ease the situation significantly due to this notice, there is no recording

drawing. However, if the situation remains unchanged, the security force,

as announced, the device. A live camera image is then displayed on the display

visible. However, this is not recorded yet. Only when the situation

is estimated to be more escalating, the actual

208 See 2016 Annual Report, 3.8.2 and 2017 Annual Report, 3.5

209

In Berlin: Ostbahnhof, Alexanderplatz, Zoologischer Garten and on trains between

Westkreuz and Ostkreuz train stations

nal recording after appropriate further announcement (level de-escal

tion model).

• In order to implement the transparency obligation210, the security forces keep a

card for data collection with you and hand it over in the case of a

tuation out done record. Furthermore, the clothing of the security

forces on the front with a camera pictogram and on the back with the imprint

Marked "Video".

• The camera's focus is set by default so that bystanders in the background can

are usually hardly noticeable.

• Recorded data are immediately after the end of service, but no later than

24 hours after the end of the recording, insofar as a handover to the

Security authorities is not required, deleted by the system.

• Access to the video data through the DB is not possible. The footage

can only be viewed by the federal police.

In accordance with our demands, DB has in the following years 2019 and 2020

after the introduction of regular operations, the overall situation of attacks on employees

in relation to the effectiveness of the technology and the perception of the employees

further observed and evaluated on the effect of the bodycams on patrols.

In total, DB employees worked 350,000 hours during the evaluation period

wearing a body cam. During this period, the bodycam was only 23

times activated. Of these, the recorded material appeared in only 14 cases

suitable for handing over this to the Federal Police for evidence purposes. In how many cases

It is not known whether the police used the material. These numbers leave for

taken, the benefits of bodycams appear and justify as very small

Doubts about the necessity of this measure.

However, the DB said in its evaluation a preventive effect of visible

worn bodycams, even if they are not switched on.

210 See Art. 13 General Data Protection Regulation (GDPR)

Because in the evaluation period, only 116 of the 2,196 attacks on
Railway workers committed on staff who wore a body cam. That equals one
rate of approx. 5.3%. Nevertheless, when we asked DB, DB had to concede that
that a bodycam was only worn in 7.9% of the total working hours, what
the numbers mentioned are clearly put into perspective.

According to the subjective impressions of the railway employees, on the other hand, there was a clearer one
to record success. Due to wearing a bodycam z. B. the duration of a
Measure or escalation in dangerous situations significantly reduced or
even prevented. This shows that wearing the bodycams as preventive
Security and de-escalation measures represent a suitable means.

However, since video surveillance involves encroachments on fundamental rights, the
the effectiveness of this measure cannot be significantly measured by subjective impressions
but is to be assessed on the basis of the objective necessity of the measure.

Since the figures determined here do not allow any clear conclusions, we will
Continue to monitor use of the bodycam by DB. However, in the 23rd
mentioned cases, no complaints from those affected or other indications
received a data breach in an individual case.

Since bodycams were rarely used, it is difficult to verify the extent to which they are used
Technology has contributed to safety at train stations. Came for the same reason
however, there are hardly any interventions in the informational self-determination
right. We will continue to monitor the use of this technique.

12.2 Information rights in the case of video surveillance

For several years, not only the BVG, but also the S-Bahn Berlin GmbH

video surveillance in certain trains on individual sections. As

The S-Bahn Berlin GmbH gives the following purposes for video surveillance, among other things. "Perception

regulation of domiciliary rights", "Protection of life, health and freedom of customers and

Employees” and “Securing evidence in the event of an incident”. The video data will be in

stored in a black box procedure and deleted after 48 hours if not

are required due to corresponding incidents.

A

and

s

i.e

e

right

P

right

a

x

i

s

135

A passenger had asked the S-Bahn Berlin GmbH to tell them which data to

ner person during an S-Bahn journey using the video camera installed in the train

were saved to him. To specify his request and for identification

of his person, the passenger has the train number and the time of admission

divided. In addition, he described his appearance and the clothes he wears

of the train journey and supplemented, shown on the information sign attached to the train

have. His request for information (with the request to send a copy of the relevant

corresponding video recordings) the passenger promptly, i. H. within the storage period,
submitted to the S-Bahn Berlin GmbH.
The passenger relied on his right to information under Art. 15 of the General Data Protection
regulation (GDPR). Accordingly, the data subject has the right from the
to request confirmation from those responsible as to whether they
data are processed. If this is the case, she has a right to information
about this personal data.
The S-Bahn Berlin GmbH then informed the passenger that the release of a
Copy of video recordings was not possible and also referred to the data
protection. To protect the personal rights of other passengers, a challenge
only on police request and not to private individuals. Even the subway
himself have no access to the video data. information to law enforcement agencies
would only be based on a time stamp, but not by viewing the contents of the
video material. According to the S-Bahn Berlin GmbH, it is
The video data does not include personal data, as this is from the S-Bahn Berlin
GmbH would not be viewed.
We have informed S-Bahn Berlin GmbH that the video data is
personal data. The video recordings made are just for use
In addition, in the case of certain events such as damage or assaults, the perpetrators
to identify. In addition, it is not important whether the data of S-Bahn employees
be viewed or not. Since the video material is personal
Genetic data is concerned, those affected have the right to request information about it.
This information can also be requested in the form of a copy.
Information in the form of a copy cannot be refused across the board for
because the personal rights of other passengers may be affected. That is

the DS-GVO provides that the right to a data copy protects the rights and freedoms
must not affect other people. However, this would have been taken into account here
Can be carried out by taking pictures of other passengers before transmission
be blackened or pixelated. Even a high level of effort is no reason for the information
to refuse. In this case, the regular data transmission to the police
authorities that it is entirely possible to provide information.

We asked the S-Bahn Berlin GmbH to develop a process like this
video data will be correctly reported in the future. The S-Bahn Berlin GmbH rejects this
so far and would now like to clarify the matter with us in court.

Anyone who processes personal data must expect that data subjects
assert their right to information.211 This also applies to personal data
Data collected via a video surveillance system.212 Information
can only be refused in a few exceptional cases. Too much effort
is not regularly included.

211 See Art. 15 GDPR

212 So also the European Data Protection Board (EDPB), Guidelines 3/2019 on processing
personal data through video devices, Version 2.0, Section 6.1, p. 24 f.; available at
https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien

13 sanctions

13.1 Corona cases

Especially in the early days of the pandemic, many contact details forms were open
in restaurants, cafés or bars where several people are independently
gig had to enter from each other. So that health authorities effectively break down chains of infection
can track saw the respective versions of the SARS-CoV-2 infection

protective measures regulation regulations for the collection of contact data such as name,

telephone number, address or e-mail address.

Such data collections harbor the risk of misuse. In three of us with

In each of the cases subject to a fine, the contact details were checked by two employees

misused.

For example, an employee of a fast-food restaurant and an employee of a

hofs first names, surnames and telephone numbers of women from the

taken from contact lists in order to write to the women privately and e.g.

asking about their relationship status.

The use of personal data from contact lists for infectious

property rights documentation of presence outside of contact tracing

is illegal and will be sanctioned by our authorities.

13.2 Penalties for Unauthorized Use of

Police database POLIKS

The sanctioning body regularly conducts proceedings against police officers who

unauthorized, d. H. for non-service purposes, personal data from third parties

from the internal police databases.

13.2 Fines for unauthorized use of the police database POLIKS

POLIKS is one of the most important electronic information systems of the police and

accordingly contains a lot of personal data, some of which is very sensitive. In

POLIKS, in particular, data from suspects, criminals, suspects

genes, those affected as well as data from victims and witnesses are recorded and stored; there-

down, for example, names, dates of birth, addresses and marital status, but also previous

fen and testimonies of witnesses. The police use POLIKS as an information system for

their statutory duties in the field of criminal prosecution and security.

Police officers are informed at regular intervals about data protection

legal regulations and instructed that they are expressly prohibited from doing so

is, data from POLIKS and other police information systems for private purposes

to use.

However, access to POLIKS is repeatedly misused to

ask family members, neighbors or third parties and their living conditions.

A police officer asked everyone around his ex-partner

who might have been familiar with the fact of the separation.

In another case, a police officer wrote to a witness after questioning her

via her private cell phone number to ask her for a date, after-

from which he had retrieved the telephone number from POLIKS.

In another case, a police officer questioned his step-

son in order to prepare him for his testimony and to inform the responsible

gen clerk to convince of a different course of events.

In addition, a police officer had stolen the new partner of a friend's ex-wife

asks because he feared that their child would be endangered by the new partner.

det be. Queries in POLIKS are only permitted for official purposes, which presupposes

that the police investigations into the matter concerned the enquirer

were officially transferred. This was not the case here. The cop acted up

own initiative without reporting the suspicion to the responsible department.

In another case, a police officer accused in a criminal

ter use the information from POLIKS to base his testimony in court

to prepare.

139

This year we have fifteen cases against police officers

initiated and already a total of eleven fine notices with a total of 42 fines

issued against police officers.

13.3 Unauthorized Database Queries By Job center employees

Again and again we sanction employees of the job center if they made queries in the online civil register or the social database systems men without there being a legal basis for the data processing.

In a procedure we initiated, employees wanted to prove that two of their colleagues have a relationship with each other and checked the reports for this deadresses of the two.

In another case, an employee asked for the registration data of the ex-wife of hers brother who had broken off contact with the ex-husband.

This year we have a total of four procedures against employees of the job center and a fine has already been imposed.

13.4 Orders and Fines for Inadmissible video surveillance

Our sanction practice shows that video surveillance is often too careless and without well-founded justification from a prevention point of view is used, without ignoring the adequately respect the rights of the data subjects.

In one case, we therefore instructed property owners to ban the processing of personal ment-related data by those installed in a mixed-use building

Video cameras prohibited. 213 The video surveillance served the purpose of prevention and clarification of criminal offenses in the form of damage to property by "smear

213 See Article 58(2)(f) GDPR

break-ins, or drug abuse as the building is in a crime

center of gravity is located. However, no case could be proven in which the
video surveillance actually led to the detection of criminal offences. The three cameras
made possible by their positioning in the entrance area, in the inner courtyard and in front of the
Cellar access, the tenants around the clock without cause, especially to that effect
to observe when and how often they enter and leave the house and the basement
(including attendance and absence) and whether they dispose of their rubbish properly. In addition
nor that the patients of the medical practices also located in the building
were filmed entering the building. In the specific case, the video surveillance
tion is not necessary, because of well-positioned motion detectors
and agreements with the doctor's offices, who is granted admission to the building, it was
possible to make access to the building more difficult for uninvited third parties. She was too
not proportionate in the narrower sense, because constant video surveillance
A residential building to protect against damage to property is generally not permitted. It
requires concrete facts that demonstrate the existence of an actual risk situation
justify to the extent that video surveillance as a last resort214
necessary is.
One fine case concerned the video surveillance of a specialist clinic by
including 21 cameras in the rooms of the clinic. Around the clock, the patients were
and employees filmed because the clinic management was afraid of criminal offenses and property
wanted to protect against damage in the clinic. An alleged consent of the employees
in the employment contract already failed because of the voluntary nature of the consent
Pressure situation in the employment relationship. Also clearly visible notices on
the video surveillance does not justify the conclusion that the patients through
entering the monitored premises is legally your consent to the
express observation. The specialist clinic could not provide any other clues either.
present points that justify this extensive video surveillance of the clinic.

In another case we have a fine against a drinks retail company

imposed, which filmed the public road next to the company building.

214 Ultima ratio

141

The video surveillance of buildings and public roads should

In terms of intellectual property law, it is basically the last resort to protect property and prevent crime

be considered. For the admissibility of such video surveillance requires

there are concrete facts for the existence of an actual risk situation that

goes beyond the general risk of life and not by other means

can be encountered.

13.5 Data protection is a matter of management, but not like this

A fine case is an example of the importance of selecting the operational ones

data protection officer. A specialist clinic had the clinic manager, who at the same time

shareholder of the clinic, was appointed data protection officer.

A data protection officer can perform other tasks and duties,

However, the company has to ensure that other duties and responsibilities

of the data protection officer does not lead to a conflict of interest.215 The

The data protection officer has, as part of his/her duties216

especially when there is a conflict between economic or technical targets and

Interests with data protection issues (e.g. of employees or customers

nen) to advise the management without being exposed to this conflict.

If data protection officers decide on data processing themselves,

This basically leads to a conflict of interest, since they do not control themselves in this respect

can. An impermissible conflict of interest can therefore initially arise from the

position of the person in the company, in particular a:e data protection

commissioned: r not owner: in the respective company or member of the business

to be a leading body.

The head of the clinic was subject to such a conflict of interest because, on the one hand, he

Management position strategic and operational decisions on the purposes and

To meet the means of processing employee and patient data and as

shareholder has an economic interest in the success of the clinic, he on the other hand

215 See Art. 38 (6) GDPR

216 See Art. 39 GDPR

as data protection officer, the compliance with data protection law by the clinic

must control.

From such a dual role, there is also the risk of significant psychological damage

There is a barrier for patients and employees, with critical questions about the

processing of personal data to the data protection officer, who at the same time

nikleiter is to walk.

It is true that company management should always ensure compliance with data protection law

keep an eye on the decision-making authority of the executives over the

processing of personal data ensures, however, that they do not identify themselves

can appoint as data protection officer. If there are no employees

those in the company who have knowledge of data protection law can do so

be hired or existing employees for this position at the expense of the

be trained by the company. Otherwise it is possible to use external data

to hire protection officers.

13.6 Release of data to enforce a settlement of claims

We fined a lawyer who had been dealing with a for years

former client is arguing about a money claim. He published his

and surnames, the home addresses of the client and their family members

as well as various unredacted file components for two years on his blog - and

referred to the privilege of the press.

In this case, however, it was not a question of an exclusively journalistic publication

public, since the overall assessment of the facts showed that the legal

walt had no journalistic interest in the publication. He was very-

more about the payment of what he believes to be his due

to obtain. However, data will only be processed for journalistic purposes if

143

if “their sole purpose is to convey information, opinions or ideas in the

to disseminate to the public…”217.

The data processing did not take place on the basis of a legitimate interest. On-

Due to the dubious intentions of the publication, the result was that the

legitimate interests of the injured party. Precisely because of the already pending

In court proceedings it would have been reasonable for the lawyer to

Waiting for the outcome of the proceedings without giving any prior notice on its website

to report.

The lawyer paid the contribution after the initiation of our fine proceedings

deletes and cooperates in the regulatory procedure and the fine procedure

conduct, which we have taken into account to reduce the fine.

217 CJEU, judgment of 16 December 2008 – C-73/07, Tietosuojavaltuutettu v Satakunnan

Markkinaporssi Oy

144

Chapter 13 Sanctions 14 Telecommunications and

media

14.1 Deficiencies at all levels: We confront

Website operators with illegal

tracking

In view of the ongoing deficits in the use of tracking techniques and third-party

services on websites, we launched a focus campaign in August. Around

Fifty companies received a postal request to start tracking on their

to bring our websites into line with the applicable data protection regulations. In the

In the letter we have both explained the legal provisions in general and

also pointed out particularly critical points that we found in individual cases

have. Most of the companies contacted have our tips

taken as an opportunity to make visual and functional changes to their websites

to do. In many cases, however, only a few of the identified defects were

cleared, so that there is still a need for action.

A

and

s

i.e

e

right

P

right

a

x

i

s

In addition to individual complaints, we also deal with large numbers of general

suggestions for tracking processes on websites. The mass of clues shows
not only the concerns of the citizens, but is also an indicator of how many
Website operators are still struggling to understand the legal framework
to meet requirements.
With the use of tracking techniques such as B. so-called cookies, the processing
personal data, at least the IP address of the visitor. This
usually serves not only to track the behavior of users, but
also to create and adapt personality profiles over the entire internet use
rich. This data is regularly sent to a variety of actors from advertising
networks all over the world, e.g. B. personalized to those affected
apply.
145
When operators of websites monitor the behavior of their users with the help of
If you want to track cookies and other technologies, you need a
legal basis. In most cases, only consent is required for this
tion into consideration. Even if many website operators have now differentiated
Display cookie banners on their websites, these are often not suitable at all
obtain valid consent. It is particularly striking that the
Refusal of tracking is usually much more complicated and expensive
as the consent. This is often embedded in incomplete or incorrect
understandable information or labels. Like the website operators at a
want to prove such a design that the users are voluntary and informed
agreed is unclear.
In order to ensure that when using tracking techniques and third-party services on web
large-scale defects are to be eliminated, we have organized a campaign this year
starts, which should reach a particularly large number of website operators.

For this we have optical design features, technical processes and concrete
Data streams documented on almost fifty websites, for which we previously
have received suggestions. We have contacted the operators of the websites with specific
ten deficits in data protection law that we noticed. We
have the documented facts in relation to the legal provisions
genes and pointed out particularly critical points in individual cases. Next to the
The lack of an equivalent possibility of rejection at the first level also proves to be the case
the other levels of the consent dialogues are often considered to be inadequate. So match
the information contained in the cookie banners often does not match the information
in the data protection declarations. The data processing processes in the
In a number of cases, the context of the tracking is not based on consent, but on one
other legal basis without the legal requirements for this
are fulfilled.
The notices were sent to companies whose cookie banners are marked as
have been noticed particularly poorly, which have a comparatively large number of users
or which may process particularly sensitive data. Affected are
from various sectors, in particular online trading, real estate, finance,
Social networks, software, health, education and comparison portals. The responsible
verbal were requested to process the data immediately in accordance with

to comply with data protection regulations. Our campaign complements that already
ongoing test procedures, which are based on personal complaints and also serves
as a signal to website operators.
A renewed inspection of the websites showed that the cookie ban
ner on most websites changed visually and functionally, or at least the

amount of cookies set and data streams to third parties have been reduced. total

together with this, deficits were reduced on many websites. Mostly enough

however, the measures taken fail to eliminate all identified deficiencies.

On some websites we could even see that the situation is still changing

has deteriorated by now z. B. even more cookies that require consent without

prior valid consent. In individual cases, rejections

additional options on the first banner level, but these seem to have no effect

are. Finally, during our review, it struck us that most website

according to the Telecommunications Telemedia Data Protection Act (TTDSG).

whose entry into force in December218 have not yet been taken into account. Therefore exists

On the part of the website operators, there is still a need for action in many cases in order to

bring about a legally compliant situation.

If persistent violations of data protection law are determined during the

are made, the companies must expect regulatory measures.

Against those responsible who continue to monitor usage behavior on their

our website, we will monitor the initiation of orders and fines

check procedure.

14.2 The Telecommunications Telemedia Data

schutz-Gesetz — More legal clarity for cookies

December 1, 2021 is the Telecommunications Telemedia Data Protection Act

(TTDSG) came into force. The TTDSG regulates i.a. the protection of confidentiality

and privacy when using technical devices connected to the Internet

can be connected. By law, with years of delay

A

and

s

i.e

e

right

P

right

a

x

i

s

218 See 14.2

147

Finally, the European requirements of the ePrivacy Directive into German law

set. This also changes the legal framework for the

Use of cookies. Among other things, operators of websites and apps should

check their processes accordingly. For support, the German authorities

regulatory authorities published a new guide.

When operating so-called telemedia, such as e.g. B. websites or apps, are regularly

Technologies are used that make it possible to track the behavior of users

gen. In practice, this is often – but not exclusively – done through cookies. Independent

of the technical design or the purposes pursued, the technical

Collection and further processing of this information usually as a uniform

life situation perceived. From a legal point of view, however, there are two steps to be taken:

separate: The use of cookies and similar technologies initially serves to

Collection of user data in order to then collect this personal data in a

second step to further processing for various purposes, e.g. for the personalization of

advertising and content, for the security of a website, for research into

of the offer and much more m.

The lawfulness of this (follow-up) processing is based in principle on the

General Data Protection Regulation (GDPR) requirements. The upstream tech

nical processes - in particular the setting of cookies and reading of information

from these - but also affect the integrity of the end devices and the privacy

sphere of the users. There is a special legal framework for this

European level – the ePrivacy Directive.219

According to the assessment of the supervisory authorities, the one that has been in force for telemedia since 2009

Art. 5 Para. 3 ePrivacy Directive by § 15 Telemedia Act (TMG) not yet

been sufficiently transposed into national law.220

219 Directive 2009/136/EC of the European Parliament and of the Council of 25 November

2009 amending Directive 2002/22/EC on universal service and users' rights

for electronic communications networks and services, Directive 2002/58/EC on the

Processing of personal data and protection of privacy in electronic

communication and Regulation (EC) No. 2006/2004 on cooperation in

consumer protection

220 See guidance from the Conference of Independent Data Protection Authorities

Federal and state authorities (DSK) for providers of telemedia dated March 29, 2019; available at

https://www.datenschutzkonferenz-online.de/orientation aids.html

The regulation was finally implemented into German law on December 1, 2021.221

This regulation must be observed in the future when using any technology, by means of

whose information is stored on end devices or read from them.

The standard regulates the principle that the storage of information in

technical end devices or access to information already stored there

is only permitted with the consent of the end user. The same applies to consent

n conditions as they already apply to consent under the GDPR.222

Consent is not required if the storage of and access to

Information in the end devices is absolutely necessary so that a user:in-

an expressly requested telemedia service can be made available.

With a view to the new legal situation, the supervisory authorities have the guidance

from 2019223 completely revised and the new version released in December

licht.224 In it, the supervisory authorities give practical advice on which cookies

and similar technologies under the strict requirements of the TTDSG in general

can still be used without consent. In addition, in the orientation

information on the requirements for effective consent

contain. Here we have in the past when checking the cookie or

approval banner on various websites found major deficits.

14.3 Need for improvement in the online guide

to test centers

Deficiencies in data protection law are particularly evident on such websites

from the content of which citizens depend without alternative. Such a con-

stellation existed on an online information platform of the Senate Department for

Health, care and equality (SenGPG), which as the central state start-up

place for corona tests has been set up. Have when reviewing the website

we found various violations. Our hearing was responded to in a timely manner.

Various measures were taken to rectify the deficiencies as far as possible.

A

and

s

i.e

e

right

P

right

a

x

i

s

221 See § 25 TTDSG

222 Section 25 (1) sentence 2 TTDSG

223 See footnote 2

224 See https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

In March we received a large number of complaints about possible violations of the law
Website test-to-go.berlin received. The website operated by SenGPG
was used at the time as a central information platform for corona tests. under
a daily updated overview of all test centers and test
made available, in some cases directly with the option of booking an appointment.
On the one hand, the complainants have concerns about the use of Tra-
cking techniques of international corporations. On the other hand, the data
property rights information on the website is incomplete, incorrect and confusing
been ren. In particular, it was not possible to understand which data
to which third parties were disclosed when using the functions of the website.
We then opened an examination procedure in which the concerns of the citizens
ger:innen have confirmed. A banner was displayed when the website was first called up
displayed at the bottom, with the information about the use of techniques for analysis

purposes and consent to this was requested. However we could

determine that processes requiring consent already took place before the button

"Accept" was clicked in the banner. Among other things, was called immediately after

the site displays an interactive city map, which provides personal information

a US-based third-party service. In addition, the banner

accessed the imprint and the data protection declaration, so that users

had no opportunity to find out about the background and responsibilities of the

data processing processes. Ultimately, it would even have the user

not helped to be able to call up the data protection declaration unhindered, because this

contained insufficient information. It wasn't just that a lot of information was missing

to the data processing processes that actually took place on the website.

Instead, the data protection declaration contained various information on pro-

eat that didn't exist at all. The impression was gained that the explanations

tion was a duplicate of another website or a sample that was not sufficient

adjusted to the individual case.

Due to the lack of information, the people affected could not form an image

about which other actors are involved in which step of the integrated

supervisory function involved and how the responsibilities were regulated in each case. clarification

information was urgently required here, since the design of the subpages,

into which the booking function was integrated contained enormous potential for confusion.

It was also noteworthy that we no longer had any addresses in the list of test centers

were displayed when we activated a program when visiting the website with which

chem browser connections to third-party service providers are blocked. Users who

have set their browsers to be particularly data-efficient, not a single one was able to do so

View information on the government offer.

At our hearing, the technical service provider who used the SenGPG at the time

assisted in the operation of the website responds. Various measures were taken promptly

taken to rectify the deficiencies. Among other things, a new cookie

Banner solution implemented, which technically ensured that those requiring consent

Processes only activated after approval and no content was lost through the banner

were covered. Tracking techniques from third-party service providers have also been used by local

replaced hosted solutions. The address list was created independently of any browser

made retrievable and the city map was only loaded when

Users activated these. Finally, the privacy notice and the

The design of the appointment booking has been completely revised so that those responsible

relationships became more comprehensible. However, it also became apparent that the

necessary formalities for any contractual relationships are not completed in good time

were.

A follow-up check of the website in September revealed that

with regard to potential third-country transfers and the role of some service providers

there was still a need for clarification. However, the offer on test-to-go.berlin was

above set. Since then, the website has only served as a guide to a new

information offer, in the design of which our instructions appear to be fully comprehensive

were taken into account. Because of the serious and diverse shortcomings,

the SenGPG issued a warning.

151

14.4 Processing of personal data in Internet offer of the Wikimedia Foundation Inc. - Wikipedia

The US-based Wikimedia Foundation Inc. offers – as joint responsibility

Verbatim together with the authors of the articles225 - on the Internet e.g. the German-

language version of the online encyclopedia Wikipedia. For individual articles in

We received complaints from people affected by this offer.

s

i

x

a

right

P

right

e

i.e

s

and

A

The complaints concerned i.a. the refusal of those responsible to

to correct gene data of data subjects or individual information from the

tick to delete. In addition, other affected persons had the complete

Deletion of your data or the entire article concerning you from the offer

required. Some of the complainants assumed that our authority

for checking compliance with data protection regulations in the German language

Wikipedia is responsible because the national country organization (chapter)

of the Wikimedia Foundation, the “Wikimedia Germany – Society for the Promotion

free knowledge e. V.” (Wikimedia Germany e. V.), has its registered office in Berlin.

With the question of whether and, if so, to what extent the national or European data

protection right to the publication of personal data in the German language

Gen Wikipedia applies, we had already agreed before the GDPR came into force

occupied. We came to the conclusion that a data protection law

Liability of the Berlin-based Wikimedia Deutschland e. V. not

give was. Already at this time responsible for data protection was the

USA-based Wikimedia Foundation Inc. as the operator of the Internet offering, the

was not under our control.226 This was again after the GDPR came into effect

to be checked because, in contrast to the previously applicable federal data

Protection Act (BDSG) also for those responsible in third countries outside the European

European Union (like the USA here).227

225 See Art. 26 GDPR

226 See Annual Report 2016, 12.5

227 See Art. 3 (2) GDPR

The GDPR is basically also for publications in the German-language Wikipedia

apply, since it is also vs. the publication of personal

Data subjects located in the European Union to a

service that (at least also) is offered to these people.228

The Wikipedia Foundation Inc. initially had this in its statement with the

founding disputed, the publications offered there were straightened out

not to, and would not be encouraged to, the individuals affected

to write articles with personal data in Wikipedia. This

Statement was not true: Some of the items that were the subject of complaints

were, according to the information provided by the persons concerned, originally came from

this itself. There was also no evidence to be found that the person responsible

prohibits the creation and publication of such articles by data subjects

or even effectively prevented. In addition, affected persons are also

users of the articles published about them are not excluded from their use.

men. It is therefore about the offer of a service, which is in any case

at least also to persons affected by the publication.

At the same time, the processing of personal data in Wikipedia is in the result

largely excluded from the scope of the GDPR. In particular, one

The data protection authorities do not have control competence: When publishing

gene of personal data in Wikipedia is basically a processing

processing of personal data for literary purposes.229 Literature does not count

only works of fiction, but also those of non-fiction. To

literature is the online encyclopedia Wikipedia. prerequisite for this

is a certain minimum of literary processing in the respective article

kel. However, the term "processing of personal data for literary

purposes" to be interpreted broadly to mean the right to freedom of expression

in a democratic society.230

According to the regulations of the Berlin state law, the processing of personal

ment-related data for literary purposes only a few provisions of the

228 See Article 3(2)(a) GDPR

229 See Art. 85 (2) GDPR, Section 19 (1) BlnDSG

230 See EG 153 sentence 7 GDPR

DS-GVO, which in particular includes the obligations of those responsible for technical and

organizational measures and any compensation to be paid for this

related violations. To the applicable provisions

Although the right of data subjects to lodge a complaint with a supervisory

authority for data protection231. At the same time, however, the entire chapter of the DS

GVO, which regulates the powers of the supervisory authorities to restrict the processing of personal

personal data for literary purposes does not apply, so a control

by our authority cannot take place in these cases.

The currently applicable provisions of state law extend the

attended non-public bodies without further restrictions232. You will find too

to those responsible who have their registered office in a third country outside the

have European Union.

The processing of personal data of data subjects who are in the

European Union, in articles on Wikipedia basically represents processing

for literary purposes and is therefore under the control of the supervisory authorities

withdrawn.

231 See Art. 77 (1) GDPR

232 See Section 2 (7) sentence 1 BlnDSG

Chapter 14 Telecommunications and Media 15 Political parties and

Company

15.1 Electronic Doorstep Campaigning

The CDU has been using an app for the doorstep election campaign since 2017. supporters

should document home visits to potential voters there and

age group and gender of the person spoken to, their attitude

to the CDU and whether the door was even opened. There were times too

a free text field for comments. The app automatically documents the street and place,

i.e. the approximate location of the election campaign. voluntarily could and can

citizens require further personal data for information and

specify clock purposes. In May, we were informed by a security researcher

known that this data was insufficiently protected. In addition, the data was

of home visits does not appear to be as anonymous as planned.

A

and

s

i.e

e

right

P

right

a

x

i

s

The CDU used the “Connect17” app for the penultimate federal election

doorstep campaign. The supporters should use playful elements, so-called

Gamification, encouraged to participate as actively as possible in the election campaign. So

there were points for every documented home visit. The 15 best supporters

zer:innen on the various levels (regional and nationwide) could use the app

show.233

Even then there was a data breach: the background system delivered

don't just ask the top fifteen supporters, but if you wish, up to a thousand

send. To do this, only the Internet link, which the app also calls up, had to set the value for

to change the desired number of data on supporters.

For people interested in computer science, it was therefore no problem to use the app

to determine the links called up and with other programs, in the simplest case with

a web browser. We were already talking to the CDU back then. she said

to ensure adequate protection of the data.

233 See Annual Report 2017, 10.1

Now, again, a data breach has occurred at what is now called “CDU.Connect”.

App discovered.234 This was much more problematic: The background system delivered

due to the insecure use of a software component, practically any in-

keep the entire database. By observing the app's communication with

the background system, it was easy to recognize with which requests this

is enough. In the article by the security researcher who discovered this vulnerability

impressive examples of the retrievable entries were published.

Immediately after learning of the data breach, the CDU

bare background system temporarily shut down and informed us about the facts.

We have made extensive inquiries as to how such a data breach happened

could come. In addition, our colleagues from the Thuringian State Commissioner

for data protection and freedom of information for us in administrative assistance with the then

gen order processing and development company carry out an on-site

conducted and documents secured. We also have the database contents to

secured for wise purposes.

According to its own statement, the CDU had at the time of disclosure of the data

already transferred the processing of the data to its own company. The

However, previous processors still have a copy of the data without the knowledge of the CDU

Data saved.

A total of almost 20,000 supporters with names, email

addresses and photos as well as approx. 100,000 records of home visits. The

Data records of the 20,000 supporters are clearly particularly sensitive

personal data, as information on political beliefs is disclosed here

beard

In the case of home visits, the situation is not so clear from the outset: the data may

data can only be collected on the condition that this is done while maintaining anonymity

happens with the persons concerned. Therefore, the exact status

place or the address is saved, but only the place and street. During the talks in

In 2017, it was also agreed that streets with few home visits would not

234 blog articles from May 12, 2021; see https://lilithwittmann.medium.com/wenn-die-cdu-ih-

ren-election-campaign-digitized-a3e9a0398b4d

 There are also rules for e-mail advertising for non-profit organizations

stored for more than a few days and not processed for statistical purposes

the. In addition, we were promised at the time that the times of the home visits would not

would be saved, since otherwise one would be able to trace the route taken by the supporter

could. This would lead to the house number possibly being used for a visit

can be determined or even the person concerned can be identified.

The evaluation of the secured data now showed that contrary to the assurance

the entries for the home visits even several points in time and also consecutive

contained numbers. For some data records, the free text fields also contained names,

which can presumably be assigned to the visitors. As a result, must be expected of it

it can be assumed that the data of the home visits are also classified as personal

gene data can be viewed. In this case, they would also be particularly sensitive

classified, since information on consent to the CDU or the entries in the free text feedback

enable conclusions to be drawn about political attitudes. Collection and storage

of this data over the years was not permitted because it was not (reliably) anonymised

and there was no legal basis for the personal storage.

Parties can certainly use up-to-date digital techniques for party work and

Use election campaigns if this is done in accordance with data protection. It's in Germany

However, it is not permitted to create profiles about the voters, as is the case, for example, in

is common in the USA. By and large, the parties agree. But

also need less comprehensive data on supporters and voters

Protection. Therefore, political parties must exercise due diligence

and consistently implement data minimization and anonymization.

15.2 There are also for non-profit organizations

Email Promotion Rules

We regularly receive complaints about non-profit organizations that

Personal e-mail addresses of public officials or entrepreneurs on the Internet

research or collect, and then invitations to their events or

to send information about their work.

When we speak to them, these organizations often reply that it is not

about advertising, but about the fulfillment of their statutory purpose. As a nonprofit

A

and

s

i.e

e

right

P

right

a

x

i

s

157

Organizations are not subject to the Unfair Competition Act

(UWG). There is the admissibility of e-mail advertising by suppliers of goods

and services are regulated.235 In addition, according to the organi-

sations, have been made public on the internet.

The term advertising within the meaning of the General Data Protection Regulation (GDPR)

includes not only commercial advertising aimed at selling goods and

Services, rather it also includes contact by parties,

Associations and clubs or charitable and social organizations with affected persons

to make their goals known or to promote them.236 Also the invitation to

Public events usually serve to publicize the goals of a

Organization.

Even if personal e-mail addresses are published on the Internet,

these are only processed if this is based on a legal permission

stand can be supported. For the situation described above, there is only one

Processing according to Art. 6 Para. 1 Sentence 1 lit. f GDPR into consideration. After that there is

Data processing is permissible insofar as it is used to protect the legitimate interests of the

responsible is necessary, unless the interests or fundamental rights and fundamental

freedoms of the data subject, which require the protection of personal data,

predominate.

Nonprofit organizations have a legitimate interest in making their work known

close. However, the sending of advertising e-mails for this purpose is

moderately contrary to the overriding interests of the data subjects.

People publish their email addresses for different reasons. This

happens, for example, due to the legal imprint obligation237 or, in order for customers

to be reachable. Persons who, for professional reasons, have given their contact details in the

235 See Section 7 UWG

236 See guidance from supervisory authorities on the processing of personal data

Data for direct marketing purposes under the General Data Protection Regulation

(GDPR); available at https://www.datenschutz-berlin.de/infothek-und-service/veroef-

public/decisions-dsk

237 See Section 5 (1) TMG

(must) publish on the Internet, but have an interest in this data

used only for purposes for which they were published.

Sending e-mails with unsolicited advertising, which the recipients respectively

individually and where an objection is required to obtain another

To prevent sending leads to a not inconsiderable nuisance. For the

annoyance, it makes no difference whether this is a commercial one

Company to be sent or by a non-profit organization, so

the principles of the UWG can also be transferred to other situations

nen.238 According to this, promotional e-mails i. i.e. R. at least then an unreasonable

annoyance if there has been no prior contact between the advertiser and the person concerned

person has passed.239

As a result, the collection of e-mail addresses put on the Internet for advertising purposes

as well as the subsequent use for advertising e-mails without the consent of the

ven persons regularly an inadmissible data processing. We have against

several organizations issued a warning for this practice.

Even non-profit organizations are generally not allowed to use advertising

and information e-mails to personal e-mail addresses that they

net have collected, send.

238 See also BGH, judgment of March 14, 2017 – VI ZR 721/15 with further references.

239 See Section 7 Paragraph 2 No. 3, Paragraph 3 UWG

16 Europe, certification

16.1 New guidelines of the European Data Protection Board

s

i

x

a

right

P

right

e

i.e

s

and

A

The European Data Protection Board (EDPB) is the body of supervisory authorities of the member states of the EU. Germany will be on the committee and its Sub-working groups by representatives of the federal supervisory authorities and of countries represented. The committee decides in disputed individual cases and provides general guidelines, recommendations and best practices to to ensure legal clarity. Our authority is represented in several sub-working groups the country regulators preparing the Committee's documents.

Over the past year, the EDPB has adopted several important guidelines. Since the
General Data Protection Regulation (GDPR) was formulated in a technology-neutral way in order to
There is a constant need to provide a legal framework for new forms of processing
Need, the relatively general regulations of the DS-GVO for certain applications
gene to specify. In particular, the guidelines on virtual ones fall into this category
Language assistants240, the guidelines for the targeted addressing of users as well
social media241 and the guidelines on the processing of personal data in
related to connected vehicles and mobility-related applications.242
Other guidelines related to fundamental data protection issues, such as B. the guideline
on the concepts of controller and processor.243 These contain
important statements on the legal form of joint responsibility, which are
GDPR and the case law of the European Court of Justice (ECJ).
has gained importance. The guidelines also belong to the basic questions

240 See https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_
v2.0_adopted_en.pdf (English version)

241 See https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_tar-
geting_of_social_media_users_de_0.pdf

242 See https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_
vehicles_v2.0_adopted_en.pdf

243 See https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controller-
processor_final_en.pdf (English version)

16.1 New guidelines from the European Data Protection Board

Art. 23 DS-GVO, which deals with the question under which circumstances the data subjects
rights of the GDPR may be restricted.244 Also of great importance
is the recommendation of the EDPB on measures to be taken when data is transferred to third countries

are observed. The EDPB is thus reacting to the judgment of the ECJ of July 16, 2020

("Schrems II").245

The guidelines on the concept of relevant and justified were highly controversial

Objection246 in which our authority was involved as rapporteur. Included

is an important part of the coherence procedure. This procedure will

solved if the European supervisory authorities in certain cross-border

tending individual cases and serves to find a solution for these cases

to find. Unfortunately, the procedure is often misinterpreted by many European regulators

understood as the very last resort in dispute resolution, which must be avoided at all costs

is applicable. Therefore, the formal hurdles for such a procedure in the guidelines were very

put up. When creating the guidelines, we worked to ensure that more

Cases come into the consistency mechanism in order to – i. s.d. GDPR – ensure that

the supervisory authorities in the EU will have as uniform a ruling practice as possible. We

but we were only partially able to assert ourselves.

This year, too, the EDPB issued numerous important guidelines. So far

a German translation is available, these and other guidelines can generally be found on

available on our website.247 Other language versions of guidelines

of the EDPB can be accessed directly on its website.248

244 See https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_ad-

opted_after_consultation_en.pdf (English version)

245 See 1.1

246 Available at https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/

guidelines

247 See https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien

248 See https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommenda-

tion-best-practices_en

16.2 Developments in the service point

European affairs

s

i

x

a

right

P

right

e

i.e

s

and

A

The GDPR provides for close cooperation between the European supervisory

authorities before. In particular, this involves cases involving a cross-border

involve the processing of personal data. Our authority processes the

responsible for those cases in which this is necessary for a specific data processing

responsible company has its headquarters in Berlin. Is the headquarters

of the company in another member state of the EU or the EEA

we send the cases we receive to the responsible supervisory authorities

the. Our internal service center for European affairs acts as a hinge

between the European supervisory authorities and our experts.

After the GDPR came into effect in 2018, one focus of activities was

first of all in determining the lead responsibility for specific persons responsible. To-

In the first few years, fundamental questions of cooperation and

The design of the technical systems249 used for this must be clarified. After

the most basic structures were in place, more cases could be voted on

ment to be given in the cooperation procedure250.251

In the period under review, our authority has returned to a large number of between

the European supervisory authorities on issues requiring coordination

taken. We have the draft decisions of other lead regulators

reviewed and objections lodged in the case of deviating positions. On this way

we have introduced substantive aspects into the procedures, some of which subsequently

in the revised draft decisions and in the final decisions

were taken into account. Of course, we also have our own draft resolutions

put up for discussion in the cooperation process. In fourteen cases we were able to

sens will issue final decisions with the supervisory authorities concerned and thus

Create clarity for data subjects and those responsible.

249 See Art. 60 (12) GDPR

250 See Art. 60 GDPR

251 See also JB 2020, 17.2

May be between the authorities concerned and the lead supervisory authority

If no agreement can be reached, a dispute settlement procedure252 is to be carried out before the

EDSA provided. The EDPB consists of the leaders of all European

supervisory authorities and the European Data Protection Supervisor.253 The German

Supervisory authorities are appointed by the Federal Commissioner for Data Protection

and freedom of information and a deputy

represented in the countries.254 This construction requires an EDPB decision

upstream Germany-internal coordination.255

The GDPR provides that the EDPB at the end of a dispute settlement procedure

makes binding decisions. However, practice has shown that the

EDPB does not make its own decisions on complaints. Rather, he checks the

Decision of the lead supervisory authority solely on the basis of the received

genes relevant and justified objections, insofar as the lead

Authority has not joined the objections.

During the reporting period, our authority had a dispute settlement procedure before the EDPB

self-operated and thus done pioneering work. It was one of the first disputes

procedure with which the EDPB was confronted in the first place. The occasion was an in

Berlin filed a complaint against an online shop based in Spain. Because of

the branch of the person responsible in Spain was the case in charge

Submit processing to the Spanish supervisory authority. The cooperation

ren was performed. The Spanish supervisory authority imposed us as the affected

authority to revise a draft decision and as a result of our objections

submitted draft resolutions on the complaint.

Regarding multiple data protection violations and the appropriate legal consequences

however, despite strong efforts, e.g. B. in the context of mediation talks,

no agreement can be reached with the Spanish supervisory authority. We laid each

252 See Art. 65 GDPR; For the application of Art. 65 (1) lit. a GDPR, the EDPB has

guidelines issued: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_032021_

article65-1-a_en.pdf (English version).

253 Art. 68 (3) GDPR

254 Section 17 (1) sentences 1 and 2 of the Federal Data Protection Act (BDSG)

255 See § 18 BDSG

Objections to the draft resolutions, which Spain mostly does not agree with

connected. The dispute settlement procedure was then initiated.

In a working group of the EDPB, the case was discussed in a larger one

Group of European supervisory authorities. There was an informal dispute settlement

achieved. Thereafter, the Spanish supervisory authority imposed instead of the originally

seen warning a fine against the online shop. Because of the informal

Agreement on essential points of criticism, there was no formal decision by the

EDSA. As a result, through the discussion and the informal settlement of disputes,

created and data protection for data subjects strengthened.

We have intensively evaluated our first dispute settlement procedure. in a

Working Group of the Conference of Independent Data Protection Authorities of the Federal

of and of the countries (DSK) we also have an evaluation together with others

German supervisory authorities. Until now, only individual supervisory

Authorities gain experience with dispute resolution procedures as actively involved parties. To-

in the future, these procedures will play a greater role in the practice of supervisory authorities

play. This is gdrs. to be welcomed, since the dispute settlement procedure is a building block of the

coherence mechanism of the GDPR. This mechanism intends a

Europe-wide uniform, proper application of the GDPR.

16.3 Accreditation and Certification Updates

s

i

x

a

right

P

right

e

i.e

s

and

A

In order to increase transparency and to facilitate compliance with the GDPR,

introduced with the DS-GVO certification procedures, which the persons concerned

provide a quick overview of the data protection level of relevant products

and services should enable. As part of certification procedures

the so-called object of certification is based on compliance with previously specified

Certification criteria checked. These criteria are an essential part of certification

cation programs and must be approved by the competent authority before they can be used in practice

be checked and approved by the supervisory authority. The German supervisory authorities

have common requirements for data protection certification pro-

programs worked out. The document256 created in the process forms the basis for the approval

Approval of the certification criteria by the responsible supervisory authority.

To prepare for an accreditation, the certification body or the pro-

grammeigner:innen257 create a certification program and through the Deutsche

Have the suitability checked by the accreditation body (DAkkS). Essential part of a sol-

chen certification program are the certification criteria for the implementation of

data protection requirements. These criteria will be checked and approved if necessary

competent supervisory authority.258

In its spring meeting, the DSK has "Requirements for data protection

tification programs". The document is intended to

authorities when evaluating certification programs as a uniform evaluation
serve as a basis. It is available to program owners and certification bodies at the
preparation of their documents as a guide.
Our authority has worked intensively on the development of the "Requirements for data
protection law certification programs". She currently has two applications
for approval of certification criteria. Both deal with
contract processing. Certifications are particularly important for processors
relevant to the guarantees required by the GDPR with regard to data protection
to provide conformity. We review those embedded in certification programs
Certification criteria based on the uniform requirements.
There is a detailed paper from the supervisory authorities that outlines the basic
describes the requirements for certification programs. Aspiring certi-
Registration bodies and program owners can use this document
check whether their programs and in particular the certification criteria for
suitable for approval by the supervisory authority. That is our job

256 See https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/themen-a-z/a/2021-
DSK Application Note_Certification Criteria.pdf

257 A body that does not wish to certify itself but has a certification scheme and criteria
created, e.g. B. due to special data protection expertise in a specific area

258 See Article 57(1)(n) GDPR in conjunction with In conjunction with Art. 42 (5) sentence 1 GDPR. Will the criteria
approved by the EDPB, this can lead to a joint certification, the European
Data protection seal (Art. 42 para. 5 sentence 2 DS-GVO).

not completed in the certification area. Lying checked for suitability
certification programs and approved criteria, we will
carry out accreditation procedures together with the DAkkS.

Prospective certification bodies are selected based on specified criteria

put through its paces.259 The accreditation phase and the authorization

ment by the supervisory authorities, a monitoring phase closes both

with regard to the accreditations as well as with regard to the certifications.260

259 See 2020 Annual Report, 1.5

260 For the accreditation process see https://www.datenschutz-berlin.de/fileadmin/user_

upload/pdf/themen-a-z/a/2020-DSK-graphic-accreditation-process.pdf

Chapter 16 Europe, Certification 17 Freedom of Information

17.1 Developments in Germany

17.1.1 Results of the Conference of Information

freedom commissioners in Germany

This year, the Conference of Freedom of Information Officers met in Germany

state (IFK) chaired by the state commissioner for data protection

and Saxony-Anhalt twice for freedom of information. Both sessions were

tragic: A total of six resolutions were passed, the demands for

include more transparency in a wide variety of areas. This is what the IFK demands

federal and state legislators to include access to information

to ensure the constitutional protection authorities and exceptions to the

protection of specific security concerns.261 In a further resolution

is advocated for the introduction of official freedom of information officers,

so that a competent contact person is available in the respective authority,

coordinates information access requests, provides legal advice and support

offers.262 A twelve-point paper is addressed to the new federal legislature,

with which the IFK made proposals for the further development of the Freedom of Information Act

into a transparency law with a transparency register, but also to more

power.263 The demand is also addressed to the new federal legislator that
EU Directive on the protection of persons who report violations of Union law, see above
to be implemented as quickly as possible while also extending the protection to whistleblowers

261 More transparency in the protection of the Constitution – strengthening trust and legitimacy!, available cash at https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/decisions-freedom of information

262 More transparency through official freedom of information officers!, available at https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-freedom of information

263 Demands for the new federal legislative period: A transparency law with exemplary create a function!, available at https://www.datenschutz-berlin.de/infothek-und-service/publications/decisions-freedom of information

that report violations of national law.264 Finally, the
IFK also ensure that in Germany there is finally a uniform minimum standard for
access to information is created, which is achieved through the ratification of the so-called
Tromsø Convention, a Council of Europe convention on access to official
documents from 2009, should be achieved.265 An additional standardization
in Germany would be achieved by all state officers for domestic
freedom of information, the advisory and control competence for the respective state authorities
also in relation to environmental information law,266 as it has been since March
already for the Federal Commissioner for Data Protection and Freedom of Information in
Reference to the federal authorities is standardized.267

17.1.2 New federal legislation

With the law amending the e-government law and introducing the

Public Sector Data Use Act (Data Use Act –

DNG)268 became Directive (EU) 2019/1024 of the European Parliament and of the

Council of 20 June 2019 on open data and the re-use of information

implemented by the public sector.269

The Amending Act, also known as the Second Open Data Act, re-

the obligation to provide unprocessed machine-readable data applies to everyone

Federal authorities, i.e. also through the indirect federal administration with the exception of

Self-Governing Bodies and Entrusted Entities, and also provides for the establishment of

Open data coordinators. The DNG has the information reuse

Act (IWG) of 2006 and applies not only to the federal government, but also to the

264 EU Whistleblower Protection Directive to be implemented promptly! whistleblowers

protect donors comprehensively and effectively!, available at https://www.datenschutz-berlin.de/

infothek-and-service/publications/decisions-freedom-of-information

265 Ratify Tromsø Convention and uniform minimum standard for access to information

create information all over Germany!, available at https://www.datenschutz-berlin.de/

infothek-and-service/publications/decisions-freedom-of-information

266 Environmental information: Advisory and control competence also on state representatives for

Transferring freedom of information!, available at https://www.datenschutz-berlin.de/info-

thek-und-service/publications/decisions-freedom-of-information

267 See Section 7a of the Environmental Information Act (UIG)

268 See law of July 16, 2021, Federal Law Gazette I, p. 2941 et seq.

269 OJ L 172 of 26 June 2019, p. 56 et seq.

Countries. It determines that provided data for private or commercial purposes

cken can be used, but does not itself justify any obligation to provide and

no claim to access to data.

Under the impression of the so-called mask affair, in which several Bundestag

MPs had been accused of arranging the purchase of

Corona protective masks by the federal government from selected companies

Receive commissions, passed the Bundestag in favor of more transparency

the law introducing a lobby register270. Here are the interest groups

against the German Bundestag and of the federal government from January 1st

2022 to be entered and publicly available.

17.2 Developments in the State of Berlin

17.2.1 New State Legislation —

successes and failures

A lobby register law was also passed in Berlin.271 It sees the institution

a public register at the House of Representatives, in which the content

participation of external parties in legislative procedures should be entered. in the

In view of the resulting increased transparency in the political arena, we welcome this

Law. However, we regret that contrary to our recommendation and unlike

no regulations on fines were included in the new federal law272, with

omitted reports can be sanctioned. But only then is a

mandatory lobby register promising.

A proposed law to strengthen consumer information, about which we

had reported last year,273 has fortunately been implemented: The Law on

270 Law introducing a lobby register for lobbying vs. the German

Bundestag and vs. of the Federal Government (Lobby Register Act – LobbyRG)

271 Law on the introduction of the lobby register at the Chamber of Deputies (Lobbyregisterge-

set – BerlLG)

272 See § 7 LobbyRG

Transparency of the results of official controls in food

wachung274 has been passed and will come into force on January 1, 2023. With that is

it is possible for all consumers to find out about the hygiene status of a food

inform the company before entering it.

Last year we discussed in detail the draft of a Berlin Transparency

set (BlnTranspG) reported, to which the "antiquated" Berlin information freedom

Act (IFG) of 1999 according to the coalition agreement of 2016

should.275 Our massive criticism of the draft law, which in particular

chen, sprawling area exceptions, has unfortunately not "fruited", because the

The draft bill was introduced into the House of Representatives almost unchanged.276

A committee hearing with external experts took place in this regard

which they brought up further criticisms of the draft law.277 Unfortunately

however, this hearing was not evaluated; the deputies have the law

Draft content not discussed in committee. The reason for this was reportedly

that the three government factions do not agree on the deletion of area exemptions

men could communicate. That is why this legislative project is ultimately the same

failed like an earlier draft by the opposition FDP parliamentary group for a

Berlin Transparency Act (BlnTG).278

Regarding the request from civil society organizations such as Mehr Demokratie

e. V. and the Open Knowledge Foundation Germany e. V. at the initiation of the Volks-

The Joint Committee has requested the “Introduction of a Berlin Transparency Act” 279

at the beginning of the new legislative period in autumn, the statutory increase

ment of the persons of trust.280 After deliberation in the plenary session, this was

Procedures provided for by the Berlin Constitution and the Voting Act

274 Food Monitoring Transparency Act (LMÜTranspG)

275 JB 2020, 19.2.2

276 See Abghs.-Drs. 18/3458 of March 3, 2021

277 See item 2 of the agenda in the minutes of the Committee on

Communication Technology and Data Protection (KTDat), session of May 17, 2021,

https://www.parlament-berlin.de/ados/18/KTDat/protokoll/ktd18-040-wp.pdf

278 See Abghs.-Drs. 18/1595 of January 16, 2019

279 Application of December 3, 2019, Abghs.-Drs. 18/4044 (old), Abghs.-Drs. 19/0003 (new)

280 Section 17a(1) Act on Popular Initiatives, Referendums and Referendums (Voting

law - AbstG)

completed in a timely manner.281 A decision to accept or express

The House of Representatives did not accept the rejection of the referendum. The new

However, the coalition agreement between the SPD, Bündnis 90/Die Grünen and Die Linke provides for

to introduce a transparency law based on the Hamburg model in 2022 and at the same time

to maintain the high standards of the Berlin Freedom of Information Act.

The creation of a Berlin transparency law that lives up to its name,

remains the most pressing issue in the area of freedom of information. We hope,

that this is from the new state government and the new governing factions

also seen as such.

17.2.2 Increased number of complaints —

Also because of massive structural deficits in

some administrations

We received increasing numbers of complaints, which in our function as arbitration

pursue stelle282. The number of new cases was 132 vs. 57 last year what a

meant an increase of 132 percent. A negative image in editing – also:

Non-processing - of IFG applications in particular two administrations have behind-

leave: 27 submissions related to the business area of the police due to failure to

late or insufficient response to application items such as the attachment

specific business instructions, training and information materials, application

reports or numbers of participants in demonstrations, the number of

appointments/dismissals and cooperation with foreign police authorities.

Eight cases alone concerned the Senate Department responsible for health

IFG applications in connection with combating the corona pandemic were received; so

regarding the contract and the costs for using the Luca App, documents for

Allocation of the vaccination appointment booking portal to Doctolib, allocation of “test to go Berlin”,

data protection and data security at “test to go Berlin” and any quality

lack of activity in test centers.

281 Art. 62 para. 3, Art. 63 VvB, Section 17a AbstG

282 See § 18 IFG

Here, as in other mediation cases in which we - despite numerous reminders -

ments – no answer was obtained that was satisfactory for the applicants

have, due to a lack of authority to issue orders or sanctions, we were able to the petitioners

unfortunately give no other recommendation than to enforce their decision

to raise a so-called action for failure to act at the administrative court in Berlin.283

To avoid this unsatisfactory situation, we will advocate that

our authority will in future be given the legal authority to remove statutory

to order violations and to be able to demand disclosure of the information.

This increase in competence would underline the importance of transparency of knowledge and

Additionally strengthen the actions of public authorities and our authority if necessary

give more assertiveness.

Incidentally, our authority, which is responsible for freedom of information, is also rightly subject to it

occurs, the IFG. We received 55 applications for file information or file inspection (possibly

by sending copies), an increase of 72% vs. 32 applications in advance

year. The subjects of the application concerned figures on sanctions, reports of data

breakdowns, data protection complaints, test procedures and fine notices.

Access to official information will continue to be granted 22 years after the entry into force of the

IFG in the administrations often only insufficiently implemented. That has to be done urgently

change - and the realization of this should also and especially at management level

grow.

17.2.3 Individual Cases

17.2.3.1 Senate Chancellery asks for postal address too soon

A petitioner requested the Senate Chancellery to send the “Protocols

and other documents for the conference of heads of government of the countries with the

Chancellor to deal with the Covid19 pandemic in 2020".

The Senate Chancellery then informed him as follows: "Since the request is a long one

s

i

x

a

right

P

right

e

i.e

s

and

A

283 See § 75 Administrative Court Code (VwGO)

period is concerned, I calculate - without having checked whether it is the

ten documents here - roughly with fees in the three-digit euro range

...". A postal address would also be required for a fee notice; name and

E-mail addresses are not sufficient. Without the postal address his application would not

not further processed.

We have pointed out to the Senate Chancellery that the petitioner will

drawn data only to the extent necessary for the processing of his

request is required. This means that in the absence of the documents

a simple email reply will suffice. Other personal data such as

Postal addresses are not required for this short message. Therefore had to first

the (non-)existence of the documents by a short inquiry in the house determine

be told. Because according to the notification to the petitioner, this has not yet been

checked, but nevertheless submitted to the petitioner (insofar as contradictory) as a cost estimate

three-digit amount - i.e. an amount between 100.00 euros and 500.00 euros - as

Fee proposed.284

In addition, we informed the Senate Chancellery that we shared their opinion

share, according to which for the proper delivery of a (fee) notification

postal address that can be delivered must be provided. We also have before

reason that Berlin chaired the conference in question and it consequently

documentation must be provided, it is recommended that an addendum be sent to the petitioner.

Here he would have to be informed that the desired documents to the extent of e.g. At-

A DIN A4 folder or so many sheets (possibly estimated) available in the house

are, but checked for data285 to be protected under the IFG and possibly accordingly

need to be blacked out. The disclosure of the information remaining after

nen286 would probably pay a fee of - currently estimated - approx.

entail so many euros. Against this background, the petitioner should state whether

he the further processing of his application with the consequence of the fee-based

disclosure of the information remaining after blackening, and in this

284 The framework fee is between EUR 5.00 and EUR 500.00, see tariff item 1004 of the

List of fees of the administrative fee schedule (VGebO); available at

https://www.datenschutz-berlin.de/informationsfreiheit/ legal-basis/fees

285 Here primarily according to Section 10 (3) IFG

286 See § 12 IFG

If so, send a mailing address that can be served. Otherwise his request would not

be further processed.

The Senate Chancellery has taken up these indications.

The procedure outlined can be used by all public bodies that

receive electronically submitted IFG applications from persons who enter their name and/or

or do not provide their postal address.

17.2.3.2 Statements from the Senate Department for Finance

the Petitions Committee

s

i

x

a

right

P

right

e

i.e

s

and

A

A citizen had lodged a complaint with the Petitions Committee of the

house of orders turned. In accordance with the usual procedure, the petition

committee the affected administration, here the Senate Department for Finance, to the

to comment on the complaint. The petitioner then asked for copies of this

decision(s), initially by the Petitions Committee, later by the Senate Department for

finance. Both agencies refused.

We have informed the Senate Department for Finance of court decisions

s, according to which, on the basis of the right to information, a disclosure

claim of petitioners vs. that administration exists, the vs. the parliament

mentarian Petitions Committee has taken a stand.287 The Senate Department for

Finanzen then sent the petitioner the comments.

According to the latest case law of the European Court of Justice (ECJ), a

Parliamentary Petitions Committee to disclose the position addressed to him-

acceptance of the administration affected petitioners are obliged (although due to

of data protection law).288

287 See OVG Berlin, decision of October 18, 2000 – 2 M 15/00; BVerwG,

Judgment of November 3, 2011 – 7 C 4/11

288 CJEU, judgment of 9 July 2020 – case C-272/19; and hereafter VG Wiesbaden,

Judgment of August 31, 2020 - 6 K 1016/15.WI

Statements from administrations the Petitions Committee may the

petitioners are not kept secret. These can both places theirs

Claim Disclosure.

17.2.3.3 Senate administration responsible for education demands

Detours for IFG applications

A petitioner wanted to know from the Senate Department responsible for education who - if

not the department specifically designated by him - is responsible for the fact that

the video conferencing tool Webex as an eLearning tool for teaching in the virtual world

classroom can no longer be used. The Senate administration then informed him

first of all that for an application for information according to the IFG the "official channel"

is necessary. After the petitioner had insisted, the Senate administration informed him

said: "After consultation with various departments here in the company, I can

to inform you that for your request under IFG please do one of the following

portals: https://fragdenstaat.de/, https://www.parlament-berlin.de/

the-parliament/petitions/online-petition. This ensures that

You get an answer from the Secretary of State for Education … or the responsible body in the

Senate administration … received.”

A

and

s

i.e

e

right

P

right

a

x

i

s

We have informed the Senate Administration that the requirements for an admissible

Signed IFG application are standardized in § 13 para. 1 IFG. Thereafter it is not intended that

"the official channel" is necessary for this. The IFG also does not standardize that an application

can be made to third-party portals.289 Rather, the application must be made orally, in writing

to be submitted to the public body that manages the file in a physical or electronic form.290 If

another body than the one addressed should be responsible, is the forwarding of the

to initiate the application from there to the competent authority.291

289 In any case, this is u. a. recommended portal of the Petitions Committee in the House of Representatives –

as the name suggests - can only be used for petitions (complaints), but not as input

instance for IFG applications that are addressed to bodies other than the Petitions Committee.

290 Section 13 (1) sentence 1 IFG

291 Section 13 (1) sentence 4 IFG

175

Apparently, the responsible body in the Senate administration has recognized that the dem

Detours recommended by the petitioners are not adequate means of responding to the request for information

encounter, because she finally agreed to him.

The submission of an IFG application must not be made more difficult by the administration.

17.2.3.4 Complained to Senate administration responsible for education

area exception to itself

s

i

x

a

right

P

right

e

i.e

s

and

A

The Federal Labor Court (BAG)292 had compensation for a Muslim woman

Awarded Discrimination After It Was Found By The Senate Department For Education

administration had not been taken over into the school service. That was the background

in the Berlin Neutrality Act standardized ban on wearing conspicuously religious or

ideologically influenced garments within the service. The Senate

administration announced in February that the Federal Administration

appeal to the Constitutional Court (BVerfG). Against this background, one petitioner applied

at the Senate administration, the publication of documents that indicate the chances of success

assessment of a constitutional complaint, and the drafts or the final

version of the constitutional complaint itself. In addition, documents were

pray, which show when the judgment of the BAG was served on the state of Berlin

had been.

The Senate administration rejected the application outright with the following reasoning

from: "All these documents are part of a file on a court

ren, which is not yet completed. The IFG only applies to courts insofar as these

carry out administrative tasks (§ 2 Para. 1 IFG). The judiciary is thus

not subject to the IFG from the outset. Access to information about concrete
Legal disputes are exclusively entitled to the parties to the legal dispute. This one
The case file that is kept corresponds to a very large extent to the case file of the court. inso
far nothing else can apply to this file content. Regardless of that
according to § 10 para. 4 IFG no right to file inspection or file information if the
Content of the files on the process of decision-making within and between authorities

292 See BAG, judgment of August 27, 2020 - 8 AZR 62/19

relates. Instructions on legal remedies..." The petitioner asked us to support his
against directed objection.

We have informed the Senate Department responsible for education that they
itself is not the addressee of the area exception of § 2 para. 1 sentence 2 IFG,293 but
dern is subject to the IFG according to sentence 1. It therefore has to check whether a ma-
material-legal reason for exclusion294 exists in whole or in part. In the latter
In this case, access to information on the parts of the file that do not require protection is to be granted
ren.295 In addition, the reason for exclusion cited by the Senate Administration
of § 10 para. 4 IFG has not been applied correctly, because the statements in the decision
exhausted themselves in the reproduction of the legal text. Instead, this was the
permanent administrative court rulings on this provision to be taken into account
. This only protects the actual decision-making process, i.e. the
Discussion, deliberation and consideration, and therefore the actual process of the
superior. On the other hand, the factual bases, the fundamentals, are not protected
of decision-making and the result of decision-making.296 Finally, we pointed out
points out that the requested proof of the date of service of the judgment of
BAG can be provided without any problems by providing the petitioner with a copy

is sent to the page on which the receipt stamp of the administration is located.

The senate administration has only this latter request in the objection

decision, the application was otherwise rejected, but meanwhile at least

at least with a comprehensible reason.

Such an incorrect application of the IFG, as in the present case

has taken place must not happen again 22 years after the entry into force.

293 According to this, the IFG applies to the courts and the authorities of the public prosecutor's office only insofar as

they do administrative tasks.

294 See §§ 6 et seq. IFG

295 § 12 IFG

296 See already VG Berlin, judgment of May 4, 2006 – VG 2 A 121.05

177

17.2.3.5 Acts in bad faith by the BVG

s

i

x

a

right

P

right

e

i.e

s

and

A

A petitioner submitted three applications to the BVG, with which he received information on the following

the (abbreviated here) questions:

1.

Application: BVG advertising costs from 2018, 2019 and 2020 and

Expected costs for BVG advertising in 2021

2.

Application: BVG advertising concept(s) in 2018, 2019 and 2020

3.

Application: guidelines/specifications/instructions according to which it is checked whether sub-

accept/private individuals/authorities advertising on/in means of transport and on/in

Can/may switch/commission BVG bus stops.

All applications contained the applicant's express request to the BVG that

inform him in advance about the expected administrative expenses and the expected

costs for the file inspection or file information. This request was

not complied with: The BVG provided the requested information and used it

a fee of EUR 10.00 each. The request for payment

abinformation had classified them as an inadmissible condition; because procrastinating

Conditional applications are according to the case law of the Federal Administrative Court

(BVerwG) inadmissible.297 The petitioner therefore turned to us for help.

Although the IFG does not provide for an obligation to inform an applicant about the probable

to be informed of the costs. Nevertheless, an overriding of this express request

of an applicant as unlawful conduct. Because with that

the BVG violated § 242 BGB (performance in good faith), which is

public law applies accordingly. After that, the debtor is obliged to make the payment

to effect such as good faith with regard to the custom of the trade.

The determination of a small fee of 10.00 euros changed that

nothing.

The fact that the applications in the present cases are inadmissibly "restricted

dingt" had been made, was an incorrect interpretation of the clear requests

at the expense of the petitioner. The case law cited could also support the view of the BVG

297 BVG reference to BVerwG, judgment of October 25, 1988 – 9 C 18/88

not support, because it was about the return declared under one condition (!)

of a (follow-up) asylum application that was ineffective. The case constellation of the decision of

BVerwG would at best have been comparable with the present constellation

sen if the petitioner declares the withdrawal of the IFG application under the condition

would have a fee imposed on him. But that was not the case: He has

submitted a clear IFG application and clearly separated from this the request for cost

ten advance information expressed.

Since the BVG stuck to its view, we had to inform the petitioner that he

the disputed issue can only be clarified in court.

We re-evaluate failure to comply with an applicant's request

Advance cost information as breach of trust. The fixing of a (even if only small)

gen) fee is therefore illegal.

17.2.3.6 IFG application to the Pankow public order office

A

and

s

i.e

e

right

P

right

a

x

i

s

A citizen applied to the district office of Pankow for the disclosure of all documents that

for the use of the regulatory office in Bötzowkiez from March. had about this

the media reports: In connection with cyclist controls, a

ner wrangling of affected or non-affected citizens with employees

of the public order office or the police. The regulatory office rejected the

application on the grounds that the scope of application of the IFG was not open.

Because the office is for the punishment / prosecution of administrative offenses and therefore

acted on the basis of the Administrative Offenses Act (OWiG).

As a "small public prosecutor's office" it was - like the public prosecutors themselves - from

Scope of application of the IFG excluded. Nevertheless, the regulatory office in

As part of a "file information according to the IFG" details such as the numbers of the

Incident according to OWiG announced sanctions. The petitioner has because

objected to the limitation of his IFG claim and asked us for support

tongue asked.

After an area exception, the IFG applies to the courts and authorities of the state

anwaltschaft only if they carry out administrative tasks.298 The IFG therefore applies in

298 See Section 2 (1) sentence 2 IFG

Conversely, not for the judicial activities of the courts and authorities of

Public prosecutor. Since this is an exceptional regulation, it must be narrowly

place. It follows from this that only these institutions, in their tasks of administering justice

tion are excluded from the scope of the IFG.

Nevertheless, in the present case, the public order office was allowed to

reject requested documents. As can be seen from the media coverage of the

Incident, but also from the vs. file information provided to the petitioner showed that commercial

the officials of the public order office at the bike checks in question

with the aim of punishing administrative offenses due to violations of the StVO. In

Within this framework, the warnings and orders mentioned in the file information

violations ads pronounced. Legal basis for this repressive

Acting was the OWiG, possibly in connection with the Code of Criminal Procedure (StPO). Of-

The regulations of the OWiG i.

V. m. the StPO299, according to which u. there must be a legitimate interest. This

federal regulations supersede the general access to information

entitlement under the IFG, as can be seen from the IFG itself300 and ultimately from the basic

law (GG).301 Therefore, the contentious question of whether repressively acting orders

authorities as "authorities of the public prosecutor's office" within the meaning of Section 2 (1) sentence 2

IFG are to be considered and therefore within the scope of the IFG from the outset

not subject, not to be decided here.

The disclosure of information by repressive law enforcement agencies

cannot be requested on the basis of the IFG, because this is enforced by

superseded higher federal law.

299 See Section 49b OWiG i. in conjunction with § 475 StPO

300 Section 17 (4) IFG

301 Art. 31 GG: “Federal law breaks state law.”

Charlottenburg-Wilmersdorf

A citizen complained that he was asked for a two-stage file inspection in

Documents from the Charlottenburg-Wilmersdorf urban development office on the "Milieu-

schutzgebiet Schloßstraße and Amtsgerichtsplatz” each charge a fee of

had to pay 204.20 euros. However, the office only had protection for the first appointment

to separate scant documents for a fee; the documents for the second

min were submitted without restriction, but together with the documents of the

first appointment. A partial inspection of the files is not intended. About the process

To make it legally secure, the entire file should be submitted for the second appointment.

A

and

s

i.e

e

right

P

right

a

x

i

s

We have informed the office that the double fee collection in the same

amounting to EUR 204.20 was unlawful. Because the check for confidentiality

tem parts of the file was only made for the first appointment. For the follow-up appointment such

no effort was incurred, so for this simple inspection of files at most one

small fee could come into consideration.302 On closer inspection, however, here was

no fee at all. Because the unrestricted inspection of files on site

is free of charge for "environmental information".303 This term is

jurisdiction as far as possible and includes all of them, even if only indirectly

related to the environment.304 The fact that the district

lichen urban development office for the "Milieuschutz Schloßstraße and Amtsgerichtsplatz"

was in charge, already suggested that the documents were the second

Access to files was "environmental information" in the broadest sense. Because every

Urban development always has an impact on the environment. The office then

issue an amendment notice in accordance with Section 47 of the Administrative Procedures Act (VwVfG),

with which the repayment of the second fee of 204.20 euros to the petitioner

ten was pronounced.

The fee for an administrative effort cannot be charged twice,

if the administrative effort has only been incurred once.

302 Between EUR 5.00 and EUR 100.00, see tariff heading 1004 b) No. 1 of the list of fees

of the Administrative Fees Ordinance (VGebO); available at https://www.daten-

schutz-berlin.de/informationsfreiheit/ legal-bases/fees

303 Section 18a (4) sentence 3 number 1 IFG

304 See BVerwG, judgment of February 23, 2017 - 7 C 31.15

17.2.3.8 Incorrect fee decision in

Friedrichshain-Kreuzberg

s

A

i

and

x

a

s

right

i.e

P

e

right

right

e

P

i.e

right

a

s

and

x

i

s A

A citizen applied to the Friedrichshain-Kreuzberg Roads and Parks Office

the disclosure of the planning for the redesign of the east side of the Mehringdamm

and requested advance information on the expected fees. The Office

informed him that "for this written information ... and renewed electronic inquiries

to the above-mentioned problem ... a fee of €100 each"

puts would. Furthermore, “additionally, depending on the effort and organization of the

File inspection Fees of up to €500 are due. All costs [are] prior to termination

and granting access to files after receipt of a notice of fees on the

deposit district account.”

We have informed the Office that the statements on the expected fees

appear prohibitive and the announced procedure, if implemented in this way,

would be illegal. Because according to the case law of the BVerwG, an information

access application, which concerns a uniform life situation, under fee law

a uniform official act.305 The blanket demand for “advance payment”

was inadmissible, because such is at the discretion of the authority.306 If this discretion

not exercised in the notice of fees, it is illegal due to lack of discretion

right Advance payment of the intended fee can only be requested in exceptional cases

be, for example, if there are indications of inability or unwillingness to pay, such as

results from the case law of the OVG Berlin-Brandenburg.307 The petitioner has

then receive the requested information on the construction project - free of charge.

Fees must not be so high that interested citizens of

be deterred from their desire for access to information. “Payment in advance” can

only be requested in exceptional cases.

305 See BVerwG, judgment of October 20, 2016 – 7 C 6.15

306 See § 16 sentence 2 IFG i. V. m. § 17 Act on Fees and Contributions

307 See OVG Berlin-Brandenburg, decision of May 26, 2014 – 12 B 22.12

Chapter 17 Freedom of Information 18 House of Representatives

18.1 Deletion moratoriums — Now also with legal ones

basis

Committees of inquiry are an important instrument of parliamentary

Control. In order for the committees to actually carry out their investigative

can come, they are regularly dependent on the authorities and

make files accessible to other public bodies, the content of which is necessary for

tion of the respective facts is relevant. The work of the

Committees of inquiry, therefore, if the personal

nary-related data due to existing deletion regulations at the time of the

investigation no longer exists in the files or the files themselves

have been destroyed. To counter this problem from the outset, were in the

In the past, far-reaching deletion moratoria have sometimes been issued. A legal one

Regulation that specifically establishes the conditions under which such a postponement

the deletion can be ordered, but did not exist so far. That is now

changed with the recent amendment of the Berlin Data Protection Act (BInDSG).

A

and

s

i.e

e

right

P

right

a

x

i

s

As unfortunate as it is when the educational work is due to deletions that have already taken place

being aggravated, it must not be disregarded that with the arrangement of a

The deletion moratorium often involves far-reaching interventions in the personal rights of those affected

people can be connected. This applies in particular if the exposure

tion of deletion relates to a large number of data, e.g. B. from the protection of the constitution

or the police are processed. Records of a range

lei among young people, an ordinary traffic accident or - currently - over a

Violation of corona-related contact restriction measures also by a

covered by a deletion moratorium and thus stored for a period that would otherwise

only serious or even the most serious offences.

The arrangement of a deletion moratorium is therefore a double-edged sword

you have to be very careful. A new regulation in the BlnDSG308 therefore provides, among other things,

308 Section 20a (2) BlnDSG

stipulates that pending data deletion from public authorities will only be suspended

can be, insofar as this is part of the participation in the fulfillment of the tasks

a parliamentary committee of inquiry is also required. In temporal

In this regard, the order should not exceed a period of two years; ver

However, extensions of no more than one year should be permitted.

Of course, the decision as to which data may be collected in the course of the investigation

relevant and thus "necessary", certain uncertainties. this applies

especially if a committee of inquiry was still there at the time the order was issued

not used, but only requested in Parliament. On the other

side, this circumstance cannot lead to e.g. B. all in a certain time-

spatially recorded data of an authority classified by this as potentially relevant

and thus saved continuously. It must at least be comprehensible

bare criteria can be explained plausibly, for what reason from the

Deletion moratorium collected personal data to clarify the respective

object of investigation might be needed. This decision is also

at the latest with each extension of the arrangement to re-check and the circle

of the data collected in this context, if necessary, to further narrow it down.

In the legislative process, we successfully worked to ensure that the order

a deletion moratorium in writing by the respective house management of the person responsible

is carried out and justified in terms of content. This way the verifiability

of the decision and guarantees that the person responsible is involved

the necessity and the specific scope of the deletion moratorium also actually

have to deal with.

In addition, our suggestion that our authority

every order of a deletion moratorium and every extension of the responsible

to be informed. On the one hand, this notification obligation increases the

tion and the exceptional nature of the arrangement. Second, it's us

only possible to comply with our general control tasks309 if we

actually know of the existence of such an arrangement.

309 See § 11 Para. 1 Sentence 1 No. 1 BlnDSG and § 32a Para. 2 VSG Bln

It remains to be seen to what extent the new regulation on deletion moratoriums in the

Proven in practice or whether and at which points the adjusting screws are a little tighter

have to be pulled. A step in the right direction is with the creation

done on a legal basis at least for the time being. Those responsible are

in turn held, also already existing deletion moratoria to the agreed

ability to check with the new regulation.

18.2 Parliament as a legal vacuum

We already reported last year310 that the House of Representatives

has failed to implement its own data protection regulations or its own supervision

ment and thus still not remedied a well-known control deficit

has been. To our chagrin and the chagrin of the affected citizens, the topic is

three years after the entry into force of the General Data Protection Regulation

Regulation (GDPR) still up to date.

A

and

s

i.e

e

right

P

right

a

x

i

s

The BlnDSG stipulates that the House of Representatives, its members, the parliamentary groups

and their respective administrations and employees from the scope of the

BlnDSG are excluded insofar as they require personal data for perception

process parliamentary tasks.311 In certain constellations, the provision

lations, i.e. to the non-application of the BlnDSG and withdraws this data processing

thus, as it were, under the supervision of our authority.

The main problem here is not that our control authority is restricted

becomes. Rather, it is problematic that the House of Representatives still has no

implemented a control body that fills this vacuum. For this purpose, the state

legislator but obliged under European law.312 That the GDPR is no exception

for parliaments and thus basically also applies to them, as far as the specific activity

is subject to Union law, the European Court of Justice (ECJ) has in relation to the

Petitions Committee of the Hessian State Parliament already clarified in 2020.313

310 JB 2020, 17.1

311 Section 2 (3) BlnDSG

312 See Article 54(1)(a) GDPR

313 See CJEU, judgment of 9 July 2020 - C-272/19, Committee on Petitions

Even assuming that Parliament does not directly follow the regulations
subject to the DS-GVO, i.e. represents an opinion which, incidentally, also
not share the scientific services of the German Bundestag314, it is necessary with a view
on the sensitivity of the personal data processed in the parliamentary space
data of effective and reliable protective measures and control mechanisms
on the basis of understandable regulations. But also such data protection
Scriptures have not yet been issued.

We have pointed out in the past that this lack of control
also causes problems in practice. This includes that affected citizens initiate
atives such as the “Neutral School” project initiated by the AfD parliamentary group at the time
confronted with the possibility of control. But this year, too, there were difficulties
ten. This time, an affected person contacted us with the information that
that the plenary and committee service of the Chamber of Deputies in a committee
session to which she was invited to listen, uses a video conferencing system,
that cannot be used legally. Unfortunately, on this point, we found the
no hearing. Because the House of Representatives responded to our cover letter
in particular our limited authority to control.

Even if one considers the use of such a system in the concrete
constellation actually excluded from the scope of the BlnDSG
would like to see why the House of Representatives, when using video

conference systems claimed a special role. Rather, it should

set a good example when processing personal data

and thus actively contribute to the protection of fundamental rights.

Since sensitive data is also processed in the business area of the House of Representatives

should be quickly ensured a data protection level corresponding to the DS-GVO

be asked. The House of Representatives as a legislative body has no

undoubtedly a role model. It will be up to the newly elected Parliament to

function by establishing its own control mechanisms

become.

314 Opinion of the scientific services of the German Bundestag on the applicability

the General Data Protection Regulation of August 17, 2018, WD 3 – 3000 – 299/18

Chapter 18 House of Representatives 19 From the office

19.1 Developments

This year was another exceptional year for our office. under the impression

the corona pandemic and the associated challenges we had to

the work organization measures adapted to the pandemic situation

to continue. In concrete terms, this means that the majority of employees:

nen continued to work regularly in the home office. This was made possible by

the increased use of mobile devices. We work with high pressure to it,

to further optimize the technical requirements for telework. Also in this

This year there were face-to-face appointments with third parties in the office as well as on-site appointments

and external tests reduced to a minimum.

Due to the special situation, the external and internal communication

on processes changed permanently. The increased work in the home office, the

accompanying anti-cyclical presence of employees in the offices

as well as the waiver of larger group meetings with personal presence

safety made it necessary to respond to communication via technical aids (e.g.

video and telephone conferences). To improve the flow of information in

hörde, we have also relied on new formats and the

Exchange via regular internal electronic information letters and newsletters as well as the

Maintain modernization of our intranet. Recourse to technology can

however, only replace personal contact among employees to a limited extent.

There were also decisive changes in personnel in 2021. After finishing their

Term of office as Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI) on

January 27, 2021 Maja Smoltczyk has the official business until the end of the

statutory transitional period of nine months. Since her final

Retirement on October 27, 2021, the department will

representative, Volker Brozio, until the election of a successor in the office of the BlnBDI

the House of Representatives, headed provisionally. In view of the national

Given the importance of the position, it is to be hoped that the replacement will be filled in the near future.

187

Due to the gratifying, but also urgently needed increase in personnel in the

The spatial capacities of our authority at the location are sufficient for the years 2020/2021

Friedrichstrasse is no longer enough. As already mentioned, the increased need for space should

tet315, by moving to new offices in Alt-Moabit. until

final move, which is planned for summer 2022, are some temporary solutions

Employees already moved to the property in Alt-Moabit in December 2020

pulled. The associated division of the office into two locations

significant organizational and logistical challenges for our house

brought, but through the particularly committed commitment of all employees

could be managed.

Another change has occurred for the BlnBDI at the international level.

After many years, our agency has chaired the International Labor

privacy in technology group, also known as the Berlin Group, to the

Federal Commissioner for Data Protection and Freedom of Information (BfDI)

ben. This marks the end of an era: The Berlin Group was founded in 1983 on the initiative of

founded by the then Berlin data protection officer and has since then

Berlin Presidency made a large number of recommendations for improving data protection

developed and published in telecommunications.

19.2 Entries from the work of the citizen service point

— Trends and priorities

s

i

x

a

right

P

right

e

i.e

s

and

A

The service center for citizen submissions is the first point of contact within our authority

for inquiries, complaints and submissions of any kind by citizens

as data subjects are approached to us. The number from

Complaints about violations of data protection law by authorities and companies

men remained at a consistently high level this year. From the approx.

Of the 5,000 entries that reached us, almost half resulted in a formal one

Complaints Procedure. The other entries could be made by the Servicestelle Bürger-

Submissions with information, consultations or by reference to publications

ments of the data protection supervisory authorities and conference can be remedied. The

315 JB 2020, 20.1

188

Chapter 19 From the service center 19.2 From the work of the service center citizen input — trends and focal points

The focus of the input volume last year was again on the pandemic

related issues, but also companies from the field of payment

services and housing industry, the election campaign for the Bundestag elections and

Visits to the police were the focus of the complaints.

The largely digitized procedure of our authority for the receipt and

Handling privacy complaints will continue to enable us to resolve them

to be recorded promptly in almost all cases and the complainants informed about the

to inform the result or the progress of their entries. Despite the pandemic-related

difficult working conditions, the service center for citizen submissions was unable to carry out its tasks

fully meet again. In relation to the ongoing pandemic situation

most recently the scanning of vaccination certificates as part of 2G regulations to a

Increase in inquiries from citizens. We were able to act in an advisory capacity here

the persons concerned about the legal basis of the measures to

break the chain of infection. We also offer on our website

and in the associated information center there is extensive information on data protection law

aspects of the corona pandemic.

We received many complaints about a payment service provider that is with the

Response to inquiries from those affected excellent by stubborn reticence

not have. Requests for information and deletion were often not answered at all

However, data from data subjects will continue to be processed for advertising purposes. Here we are now

in Europe-wide exchange with the other supervisory authorities, since the main

of the company is not located in Germany.

In the area of the housing industry, we were able to help a large number of those affected,

by being a company that, through quick acquisitions in Berlin's housing

entered the market, convinced them to go to the survey of the newly acquired

genes through 3D laser scanning processes. According to our notice of data

the company stopped the campaign because it was inadmissible under intellectual property law.

The Bundestag elections in September and in particular the election campaign before

also the subject of an increased number of complaints. It exists though

with regard to the election campaign, a legal basis according to which parties

may process son-related data of voters for election advertising. That

however, this election advertising is then partly in the name of people who cannot be assigned to a party

189

Sender:innen was sent, caused displeasure among many Berliners:innen. the one

set of an app made available to election campaigners by the same party

was also led to a not inconsiderable number of data protection violations, since

sometimes the political views of people were recorded.316

A revenant in the focal points of complaints processing in our

Authority is also the police. In addition to a particularly striking case in which the

police through the unnecessary sending of unredacted files to the

administrative court has created the danger that e.g. T. particularly vulnerable

Data from demonstration applicants falls into the hands of unauthorized persons

317, we received several cases this year in which police officers:

unlawful personal data from the registers accessible to them

debit.[318]

19.3 Privacy and Media Literacy

We have set ourselves the goal of teaching elementary school children at an early age what personal data is what is behind the term data protection and how they can influence what happens with their data.

Just in time for the start of the 2021/22 school year in autumn, we published our worked media-pedagogical offer and offered elementary schools a new one free workshop format. The workshop "Privacy for Children" is aimed at specifically for grades 4 to 6. Distributed over five lessons he digital skills and introduces the world of data protection. The students discovered Playfully learn what data is, how it is collected and why it is worth protecting are. Another focus is information about personalized advertising: By designing fictitious advertisements, the students deepen their understanding of personalized advertising and the use of previously published data. Using practical case studies, the students discuss how they B. in

316 See 15.1

317 See 3.1

318 See 13.2

case of data theft would behave personally. At the end of the workshop, a "data protection contract" was concluded, into which the knowledge gained was incorporated.

The workshop met with great interest. By the end of the year we will have four Berliners districts held a total of eight full-day workshops (five hours each) and achieved with over 160 students. The increasing need for training and accompanying trending teaching material is also in view of the ongoing corona pandemic and the

increased use of digital media has become clear once again. through the

Work at the schools also revealed thematic priorities in which

special support for teachers and parents is required. To call

are above all the increasing spread of messenger services under

students and the associated dangers of cyberbullying.

We will be expanding our media education offerings on these and other topics

tig expand and offer extensive information and teaching material. Around

further workshops and projects at schools and in educational institutions in the area

to be able to carry out, we want to move on to also multipliers in the future

schools.

Furthermore, we are continuously expanding our digital offering at www.data-kids.de

out of. Primary school children, teachers and parents can find a wide range of materials on the website

rials for the secure handling of one's own data on the Internet. The website has been

supplemented this year with audiovisual media and interactive games. Why

Data protection is also important in homeschooling, for example in a new video

purifies. We provide supplementary information material for children, teachers and parents

still available there for free download. In addition to further development

of Data-Kids (age group 6 to 12) we have in a transnational work

Working group on the redesign of the website www.youngdata.de (age group

12+) by the Conference of Data Protection Authorities of the Federation and the

countries (DSK) is operated. The relaunch of Young-Data is scheduled for 2022

planned.

19.4 Cooperation with the Chamber of Deputies

from Berlin

The committee for communication technology and data protection (KtDat) came in this

Year together eight times and dealt with many topics from the
digitization and data protection. The BlnBDI attended all meetings
taken and comprehensively advised the committee together with their experts.
The digitization of schools,319 electronic contact tracing to pan-
demiekampf320 and the BVG321 mobility apps were some of the special
important items on the committee's agenda. A key issue was also
the data protection-compliant use of digital teaching and learning materials in schools.322 We
in this context we have emphatically advocated that the school
law (SchulG) is modernized with regard to data protection. The mission has
worth it. The reformed SchulG now contains regulations on data protection that are based on
explicit recommendations of our authorities and is therefore one of the modern
ten school laws in Germany.323 The planned new Berlin transparency
gesetz (BlnTranspG)324 was repeatedly put on the KtDat agenda.
Nevertheless, the Chamber of Deputies did not succeed in getting it by the end of the 18th legislative
tur period to say goodbye. On the one hand, this is unfortunate, on the other hand, this
circumstance for the newly composed House of Representatives at the same time the chance
to eliminate the serious shortcomings in the most recently submitted draft law and
actually approved a modern transparency law in Berlin during this legislative period
create.

319 See 1.2

320 See 1.5

321 See 11.1 and 11.2

322 See also our press release of January 22, 2021; available at https://
www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/
20210122-PM-Digitaler_Instruction_Misstaende_resolve.pdf

323 See also our press release of September 17, 2021; available at https://

www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/

20210917-PM_School Act.pdf

324 See 17.2.1

19.5 Cooperation with other entities

This year the DSK was chaired by the Saarland. It met on 27./28.

April and on 25./26. November each year virtually. In addition, three interim conferences

as video conferences on January 27th, June 16th and September 22nd. The DSK

passed numerous resolutions and resolutions on current

len data protection issues,325 u. a. for processing positive data in one

so-called "energy supplier pool",326 for the use of contact tracking systems327

and for the processing of the "vaccination status" date of employees by their work-

donors.

We also regularly attend the meetings of the working group (AK) DSK

2.0 participated. The AK deals with the strategic reorientation of the DSK

and is working on optimizing the decision-making processes of the DSK and its working methods

mix The AK DSK 2.0 took place on March 3rd and March 14th/15th. Met July — once when

Video conference and once as a face-to-face event in Berlin. The results of his

were discussed at a special meeting of the DSK on September 29th. Included

are i.a. a change in the rules of procedure and weekly meetings of the House

lines have been decided for the purpose of an even better exchange of information.

The Conference of the Freedom of Information Officers in Germany (IFK) met underground

the presidency of Saxony-Anhalt on June 2nd and November 3rd as a video conference

renz.

The Global Privacy Assembly (GPA)328 took place as a two-day video conference on 20/21

held in October. The focus of the conference was data protection and the protection of

Privacy in the digital age. The future strategic orientation of the

325 All resolutions and resolutions of the DSK are available on the DSK website at https://

www.datenschutzkonferenz-online.de/entschlussungen.html and https://www.datenschutz-

konferenz-online.de/beschluesse-dsk.html.

326 See 11.3

327 See 1.5, 6.1 and 6.5

328 Formerly the International Conference of Data Protection and Privacy Commissioners

GPA was again an important topic. The GPA adopted numerous reports and resolutions

ßungen329, e.g. on digital children's rights.

19.6 Public Relations

This year, our press office was reorganized. Also on organizational

On a technical level, there have been some changes with the aim of steadily increasing interest

in the topics and activities of our authority well-founded and reliable in the future

to use.

In total, we answered over 200 press inquiries. As in the year

previously, inquiries related to data protection in particular dominated

with the corona pandemic. While 2020 the analogue contact data collection in the pre-

the reason for this were inquiries about digital contact tracing this year

a focus. The media were particularly interested in the (intermediate)

Status of the ongoing audit in our house.330 We also received many inquiries

on data breaches at corona test centers and the country's vaccination management

Berlin.

In the super election year 2021, we also received many inquiries about the admissibility of personal

nalized election advertising by post and for doorstep election campaigns by app. Other important

Current topics were the consequences of the Schrems II judgment and data breaches in various
Operators of online shops, food delivery services and public authorities. always like-
we are also informed by media inquiries about suspected data protection violations
become noticeable and have taken this as an opportunity, the underlying
check data processing. Continued to ensure great national interest
our notes and test results on the data protection-compliant use of video con-
reference services. Paper first published in 2020, we have this one in February
year comprehensively revised and updated.331

329 All GPA resolutions and reports are available on the GPA website at
https://globalprivacyassembly.org/document-archive/adopted-resolutions/ and
https://globalprivacyassembly.org/document-archive/working-group-reports/ available.

330 See 1.5

331 See 2.2

We addressed the public with a total of fourteen press releases.
We have i.a. on the data protection deficits in digital teaching in the
State of Berlin and the disclosure of sensitive data in con-
trolls on buses and trains for beneficiaries of the “berlinpass” criticized. Besides that
we informed the public about new test procedures in the field of international data
transfers of companies and the use of tracking techniques and third party services
towards websites. At the end of her term of office, Maja Smoltczyk, as part of a
seminung, took stock of their more than five years of activity as BInBDI.
In addition, the management of the authorities and subject specialists answered in dozens
interviews and background discussions, a wide range of questions from A to processing
up to Z like certification. In a joint opinion, Prof. Dr.

Dieter Kugelmann as Rhineland-Palatinate State Commissioner for Data Protection and freedom of information and Maja Smoltczyk as BlnBDI the recurring loose attacks on data protection. They clarified that privacy does not stand in the way of social challenges such as the corona pandemic, but rather contributes to acceptance and trust in the population.332

We published the following press releases this year:

• Digital teaching – grievances must be remedied as quickly as possible (22nd of January)

• Data protection officers from Berlin and Rhineland-Palatinate point out unfounded attacks back to the right to informational self-determination – Smoltczyk and Kugelmann: Data protection is a European success story (5 February)

• More "green": Berlin's data protection officer publishes updated information on privacy-compliant video conferencing services (February 18)

• Benefit notification instead of a berlin pass: No data protection for low earners (1st March)

• Notice of fine against Deutsche Wohnen SE: Complaint against the cessation of the Proceedings filed (March 3)

• Berlin Group (IWGDPT) publishes working papers on Data Portability and Web Tracking (March 23)

332 See https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/2021-BlnBDI-LfdRLP-Standpunkt_Attack_auf_Datenschutz.pdf

• Berlin Commissioner for Data Protection and Freedom of Information publishes annual report 2020 (8 April)

• Berlin data protection officer takes part in Germany-wide audit international data transfers by companies (June 1)

• Deficiencies at all levels: Berlin supervisory authority confronts website

Operators with illegal tracking (9 August)

• Data protection for children: New workshop for primary schools in Berlin (16 August)

• Berlin school law: Reform strengthens data protection in the education sector

(17th of September)

• “Time of upheaval”: Maja Smoltczyk's tenure as BlnBDI ends

(October 19)

• Contact data collection: Corona warning app as a data-saving alternative in

Enable Berlin State Ordinance (November 19)

• TTDSG comes into force: Clear rules for cookies and similar technologies

(December 1)

All press releases are available on our website.333

With a corresponding e-mail to the address presse@datenschutz-berlin.de

Inclusion in our press mailing list possible.

19.7 Public Relations

19.7.1 Events and Lectures

Due to the ongoing corona pandemic, most of them took place again this year

Events take place online as part of video conferences. According to the experience

Planned podium discussions, congresses, workshops

and technical discussions are now also converted into online formats at short notice or as hy-

brid events are held. So it was possible to have a lively exchange

the national and international specialist committees, working groups and study groups

guarantee.

333 https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen

Some of the lecturing activities have also shifted to digital space. Some examples are mentioned here:

• Online lecture "Current developments in the practice of fines by German supervisory authorities" on June 10th at a club in Hamburg

• Lecture "The GDPR in practice from the point of view of the Berlin Commissioner for data protection and freedom of information" on September 16 at the Data Protection Day company in Berlin; Topics were important problem areas in the supervisory legal practice, e.g. B. when providing information according to Art. 15 DS-GVO obtaining consent for tracking and when using video conferencing border systems.

• Lecture "Website tracking in the regulatory procedure - legal sprees and technical pitfalls" at the data protection conference (hybrid event tion) of a company on September 20th

• Lecture "Consent management from a regulatory perspective" at Data Day of the Data Protection Foundation on November 3rd in Berlin; the event under the title: "The TTDSG and new ways of consent management" with various contributions and debates on individual aspects the new Telecommunications Telemedia Data Protection Act (TTDSG).

• Podcast broadcast of 15 December: "Cookies, banners and the new TTDSG"; Experts from the BlnBDI and the State Commissioner for Data Protection Niedersachsen explain the new regulations in the "data radio" podcast of the state Commissioner for data protection and freedom of information in Rhineland-Palatinate.

19.7.2 Publications

Another building block of our public relations work are the publications. The information-thek334 on our website contains i.a. Legislative texts, resolutions and guidelines such as in-house flyers, brochures and guides. All information materials are available

334 https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen

197

available as a download, some can also be printed free of charge

be ordered.

In addition to the activity report of the past reporting period, we supplemented ours

Print publications around a newly published guide:

• On the occasion of the Bundestag elections and the election to the Berlin House of Representatives

lin this year we published our guide “Election advertising by political

Parties”, which was first published in 2008, has been fundamentally revised and

relaunched. The guide provides information about the legal framework

in connection with unwanted election advertising - whether by post, at the front door

or by means of an election campaign app - and shows that and how the reporting

dedaten can be contradicted.

• We have also reissued our in-house edition of the data

General Protection Regulation (GDPR). After more than three years of experience with the DS

GVO we have adapted the first edition to the practical requirements

and thus more clarity. The recitals are now as

The entirety is printed before the articles and with references to the relevant standards

provided. The respective articles contain references to the

associated recitals.

On our website we offer in addition to those already mentioned above as examples

Materials including orientation aids and condensed information on priority

topics such as the corona pandemic. So you can find here u. current notices for

Berlin responsible for the use of video conferencing services, for data protection

compliant use of digital learning platforms, a sample form for contact

tracking and FAQs on vaccination certificates and test sites. In our section

"Topics A to Z" we cover from A like accreditation to Z like certification different

those topics that we are constantly expanding.

198

Chapter 19 From the office 19.7 Public Relations

19.7.3 Outlook

The "Committee, Press and Public Affairs" department created in September 2020

keitsarbeit" has increasingly consolidated in terms of personnel over the course of the year and the

created the necessary structures and foundations for the public relations work of our

authority to expand further. It is pleasing that the individual work areas

now mesh much better. Internal communication was also successful

be improved as a result, in particular through the

comprehensive relaunch of the intranet.

In the coming year, the position in the public relations department, which has been vacant since spring

occupied so that we can then work on new event

formats, print publications and, last but not least, the implementation of our digital

communication strategy can work. This includes i.a. the revision of our

our website and the expansion of our digital information offering.

The central concern is the exchange with politics and the media and in particular with

Citizens to continue to strengthen and so the general awareness of the

to promote data protection and media literacy. Therefore we will

work with civil society actors, scientific institutions, schools

and expand educational institutions. The involvement of multipliers,

new digital event formats and media as well as the introduction of various

Training courses will have a significant impact on our work in the coming year.

199

20 statistics for the

annual report

s

i

x

a

right

P

right

e

i.e

s

and

A

In the fourth year of the General Data Protection Regulation (GDPR), it is evident that

probably the number of entries as well as the reported data breaches on one

maintain a consistently high level. This is especially true when compared to the number of

Cases before the GDPR came into effect. Compared to the previous year, there is an increase

the formal complaints and consultations of those affected as well as those reported

record data breaches.

The presentation of the following chapter is based on the uniform statistical

tic criteria set by the Conference of Independent Data Protection Authorities

of the federal and state governments (DSK). In addition, we come

reporting obligations from the GDPR and the Federal Data Protection Act (BDSG)

after. However, it should be noted that due to the corona pandemic and the

the resulting difficult working conditions do not yet complete all processes

are statistically recorded. The figures given here are therefore subject to

just.

20.1 Complaints

This year, our authority received a total of 5,671 submissions from those affected,

of which 2,436 are to be treated as formal complaints within the meaning of the GDPR

ren.335 For the majority of the complaints, we opened procedures in our own

thing. All in all, there were 1,856 procedures this year. of which addressed themselves

more than 80% against private bodies (1,589), the rest against public authorities (267). At 580

cases, the complaints were not within our area of responsibility, e.g. because the

responsible had its German headquarters in another federal state. This

We have complaints to the responsible supervisory authorities in Germany

delivered.

335 See Art. 77 GDPR

20.2 Consultations

This year, too, the number of applications submitted to us since the GDPR came into force has remained the same

Complaints at a consistently high level. The graphic below shows one

Overview of the number of complaints submitted to us by data subjects

vs. public and non-public bodies as well as payments to other German

cal supervisory authorities since 2017.

complaints

public bodies

non-public bodies

duties

281

1222

195

2018

17

88

312

2017

Figure 1: Complaints 2017-2021

523

521

580

1684

1656

1589

248

2019

253

2020

267

2021

20.2 Consultations

The term consultation includes all written data protection statements

arrivals vs. Controllers, data subjects and public administration

described. The focus here was on advising those affected, i.e

Citizens, with 3,235 cases. There was a very strong increase in

increased compared to the previous year. In addition, we advised those responsible in 472 cases.

In addition, there is a large number of telephone inquiries that are not recorded statistically.

201

consultations with affected persons

3235

2079

2402

2438

655

2017

2018

2019

2020

2021

Figure 2: Consultation of affected persons

20.3 Data Breaches

This year, those responsible reported significantly more data breaches to us

than in the previous year. In the reporting period, there were a total of 1,163 reports from

literal, which is a new maximum value vs. represents the years before. Of the

1,026 reports were in the non-public area, i. H. especially on pri-

father company. Public authorities reported 137 data breaches to us.

Data breach reports

public bodies

non-public bodies

357

314

52

45

2017

7

43

2018

Figure 3: Data breach reports

1015

873

142

2019

202

1163

925

821

1026

104

2020

137

2021

Chapter 20 Statistics for Annual Report 20.4 Remedial Actions

Even if no quantified statements can be made due to the variety of data breaches

correct species can be taken, the following exemplary statements can be

say meet:

Not all data breaches can be traced back to direct human error.

be led. Safety measures not taken are often another cause.

For example, unencrypted mobile data carriers are problematic if lost.

Film and photo recordings are often made in childcare facilities

stored on non-encrypted media, so that in the event of loss of USB sticks, SD

Cards, cameras or computers, the recordings of children in the possession of unauthorized persons

reach. This problem was already addressed in the 2019 annual report336.

Software vulnerabilities are another indirect cause of data breaches.

Two resulting attack paths are also prominent in this reporting period

been.

First, these were common vulnerabilities in email server software that

were exploited by criminals to take over these servers, resulting in information

information that was stored on the servers could be accessed.

On the other hand, these were so-called ransomware attacks, which have already been mentioned elsewhere in this

activity report were dealt with in more detail.337

20.4 Remedial Actions

If we discover a breach of the GDPR by those responsible, we can

we take various remedial actions.338 This year we have two war-

ments and 212 warnings. From the possibility of certifications

to revoke no use was made in the reporting period. In one case

issue an order. In 61 cases we have fines totaling

336 JB 2019, 15.2

337 See 5.4

338 See Art. 58 (2) GDPR

133,350.00 euros imposed. At the end of the reporting period, the corresponding

However, the proceedings have not yet all been legally concluded. In addition, 36

issue fines. In 3 cases we filed a criminal complaint. Over

25 fine proceedings were discontinued throughout the year.

In addition to the cases mentioned here, a large number of other proceedings were carried out

opened in which no decision has yet been issued.

Remedial Actions 2021

warnings

warnings

Instructions and Orders

Revocation of Certifications

fines

2

212

1

0

61

20.5 Formal support for legislative

plan

According to the Berlin Data Protection Act (BlnDSG), our authority has the up

gabe, the House of Representatives, the Senate and other institutions and bodies

on legislative and administrative measures to protect rights and freedoms

to advise natural persons on data protection law.339 This includes both written

tive statements as well as discussions with parliamentary groups and members of parliament

and formal hearings in the House of Representatives and in its committees.

In the period under review, we advised on several legislative projects, such as

e.g. B. in the event of changes to the Schools Act (SchulG)340 or the BlnDSG341. The distance

we gave u. a. Statements on the amendment of the prohibition on misappropriation

Act (ZwVbG)342 and the Lobby Register Act (BerlLG) from.343

339 Section 11 (1) sentence 1 no. 3 BlnDSG

340 See 1.2.1

341 See 18.1

342 See 9.3

343 See 17.2.1

In addition, there were several consultations on legislative projects that would create and change of legal ordinances and administrative regulations has the object ten. An example here is the change in the regulation on material competences for the prosecution and punishment of administrative offenses (ZustVO-OWiG) u. a. on- due to the Telecommunications Telemedia Data Protection Act (TTDSG).344 In the case of federal legislation projects, we also took part together with the other ren supervisory authorities of the federal and state governments position.

20.6 European Procedures

The GDPR stipulates that the European supervisory authorities in the case of cross-border tend to work together.345 Within the framework of the cooperation procedure a lead supervisory authority is determined to carry out the investigations in the respective Case leads.346 Other supervisory authorities can report as affected authorities, if the controller has an establishment in your country or the processing has a significant impact on data subjects in the respective country. Included the respective supervisory authorities cooperate closely with each other.347 After completion of the investigations, the lead supervisory authority shall submitted a draft decision to the supervisory authorities for their comments.348 Overall our authority published 13 draft decisions and 14 final ones this year Decisions. For coordination and cooperation, the European supervisory authorities use own the Electronic Internal Market Information System (IMI).

344 For TTDSG see 14.2

345 See 16.2 and 2018 Annual Report, 1.1

346 See Art. 56 (1) GDPR

347 See Art. 60 (1) to (3) sentence 1 and Art. 61, 62 GDPR

348 See Art. 60 (3) sentence 2 GDPR

205

The following table gives an overview of the participation of our authority

in the most important of these European procedures.

European procedures

Art. 56Procedure (affected)

Art. 56Procedure (responsible)

Art. 60ff procedure

253

41

27

206

Chapter 20 Statistics for the annual report