

Christian Flache (Hrsg.)

Praxishandbuch Datenschutz im Notariat

NOTARPRAXIS

Praxishandbuch Datenschutz im Notariat

herausgegeben von
Notar
Dr. Christian Flache,
Leipzig



Deutscher**Notar**Verlag

Zitiervorschlag:

Flache/*Autor*, Praxishandbuch Datenschutz im Notariat, § 1 Rn 1

Hinweis

Die Ausführungen in diesem Werk wurden mit Sorgfalt und nach bestem Wissen erstellt. Sie stellen jedoch lediglich Arbeitshilfen und Anregungen für die Lösung typischer Fallgestaltungen dar. Die Eigenverantwortung für die Formulierung von Verträgen, Verfügungen und Schriftsätzen trägt der Benutzer. Herausgeber, Autoren und Verlag übernehmen keinerlei Haftung für die Richtigkeit und Vollständigkeit der in diesem Buch enthaltenen Ausführungen.

Anregungen und Kritik zu diesem Werk senden Sie bitte an

info@notarverlag.de

Autoren und Verlag freuen sich auf Ihre Rückmeldung.

Copyright 2022 by Deutscher Notarverlag, Bonn

Umschlaggestaltung: gentura, Holger Neumann, Bochum

Satz: PMGi Agentur für intelligente Medien GmbH, Hamm

Druck: Hans Soldan Druck GmbH, Essen

ISBN 978-3-95646-234-4

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronische Systeme.

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über

<http://dnb.d-nb.de> abrufbar.

Vorwort

Kaum eine Materie wird so gerne hochgehalten und dennoch allzu schnell zur Seite gelegt wie der Datenschutz. Und das ist auch kaum verwunderlich. Ist das Datenschutzrecht doch, außer für einen kleinen Kreis von „Störenfriede“, für die meisten Juristen ein Nebengebiet. Man beschäftigt sich damit nur, wenn man muss und nur soweit es wirklich sein muss. Notare sind da bislang keine Ausnahme.

Dies wird sich zukünftig ändern. Bei vielen Notarinnen und Notaren ist eine erste Befassung mit den zum Teil sehr technisch geprägten Fragen des Datenschutzes erst mit dem Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) erfolgt. Die Notwendigkeit, sich mit Fragen der Sicherung von Daten auseinanderzusetzen wird für das Notariat mit Einführung des Elektronischen Urkundenarchivs zum 1.1.2022 eine ganz neue Dimension erreichen. Zahlreichen Vorgaben aus der BNotO und der NotAktVV zwingen die Notarin und den Notar zu einem vertieften und vor allem stetigen Blick auf die technischen und organisatorischen Maßnahmen zum Schutz der Daten und der Datenverarbeitungssysteme. Damit wird der Datenschutz nun wirklich Amtspflicht.

Das vorliegende Werk hilft dem Notar und der Notarin die eigenen datenschutzrechtlichen Kenntnisse so zu erweitern, dass die Pflichten bzgl. des Datenschutzes souverän erfüllt werden können. Es ist als Nachschlagewerk für den Amtsträger konzipiert und soll einen Einstieg mit der notariellen Brille zu ermöglichen. Die Vorschläge zu Mustern und insbesondere den technisch organisatorischen Maßnahmen sind dabei stets an, vor allem technischen Änderungen anzupassen. Gerade die rasante technische Entwicklung und auch die zu erwartenden rechtlichen Änderungen bedingen, dass die im Notariat genutzten Muster etc. immer wieder überprüft und einer Revision unterzogen werden müssen.

Das Werk hat die sich abzeichnenden Änderungen der DONot bereits berücksichtigt. Da bis zur Drucklegung aber die finale Fassung noch nicht veröffentlicht wurde, können sich Abweichungen in der Nummerierung ergeben. Inhaltliche Änderungen der den folgenden Ausführungen zugrunde liegenden Normen sind dagegen nicht zu erwarten.

Leipzig, im Oktober 2021

Dr. Christian Flache

Inhaltsverzeichnis

Vorwort	5
Autorenverzeichnis	13
Abkürzungsverzeichnis	15
Literaturverzeichnis	23
§ 1 Einführung in den Datenschutz	25
A. Vorbemerkung	25
B. Datenschutz und Geheimnisschutz	26
C. Datenschutz und IT-Sicherheit	27
D. Entstehung des Datenschutzrechts	28
E. Die Datenschutzgrundverordnung	29
I. Struktur und Ziele der Verordnung	29
II. Anwendungsbereich	32
1. Personenbezogene Daten	33
2. Verarbeitung	34
a) Automatisierte Verarbeitung	35
b) Nichtautomatisierte Verarbeitung in einem Dateisystem.	35
3. Ausnahmen	36
III. Verantwortlichkeit	37
IV. Grundsätze der Verarbeitung	39
1. Grundsatz der Zweckbindung	39
2. Grundsatz der Datenminimierung	40
3. Grundsatz der Speicherbegrenzung	41
4. Grundsatz der Rechenschaftspflicht	41
§ 2 Rechtmäßigkeit der Verarbeitung	43
A. Vorbemerkung	43
B. Grundlagen einer zulässigen Verarbeitung	44
C. Rechtsgrundlagen im Notariat	44
I. Erfüllung eines Vertragsverhältnisses	44
II. Rechtliche Verpflichtung/öffentliche Aufgaben	44
III. Einwilligung	45

IV. Berechtigtes Interesse	47
V. Zweckänderung	48
D. Besondere Kategorien von Daten	49
I. Rechtmäßigkeit der Verarbeitung	50
II. Besondere Kategorien von Daten im Notarbüro	51

§ 3 Rechte des von einer Datenverarbeitung Betroffenen .. 55

A. Vorbemerkung	55
B. Auskunftsrecht	56
I. Sinn und Zweck	56
II. Inhalt	57
III. Verfahren	58
C. Recht auf Berichtigung	60
I. Sinn und Zweck	61
II. Inhalt	61
III. Verfahren	61
D. „Recht auf Vergessenwerden“	63
I. Sinn und Zweck	63
II. Inhalt	64
III. Verfahren	65
E. Widerspruchsrecht	66
F. Beschwerderecht	66
I. Sinn und Zweck	67
II. Inhalt	67
III. Verfahren	68

§ 4 Informationspflichten im Rahmen der Datenverarbeitung 69

A. Vorbemerkung	69
B. Information bei der Datenerhebung	70
I. Information der Rechtssuchenden über die notariellen Tätigkeit	70
II. Inhalt	71
III. Verfahren	77

IV. Information der Besucher des Internetauftritts	78
C. Information bei Datenerhebung durch Dritte	84
§ 5 Dokumentationspflichten	87
A. Vorbemerkung	87
B. Umfang der Pflichten	87
C. Folgen der Dokumentationspflichten	88
D. Verzeichnis der Verarbeitungstätigkeiten (VVT)	90
I. Anwendungsbereich	90
II. Inhalt des Verzeichnisses	92
1. Kontaktdaten	93
2. Verarbeitungszweck	94
3. Kategorien von Daten und Personen	99
4. Kategorien von Empfängern	100
5. Übermittlung ins Ausland	101
6. Löschfristen	102
7. TOMS	108
III. Gestaltung des Verzeichnisses	110
IV. Muster	113
V. Aktualisierung	115
E. Datenschutzmanagement	116
I. Aufgabenverteilung	120
II. Technikgestaltung/Voreinstellung	120
III. Auskunftspflichten	122
IV. Mitarbeiterschulungen	125
V. Kontrolle	125
VI. Muster/Richtlinien	126
§ 6 Auftragsverarbeitung (Art. 28 DS-GVO)	129
A. Allgemeines	129
B. Wer ist Auftragsverarbeiter im Sinne der DS-GVO?	129
C. Was gehört zum Inhalt eines Auftragsverarbeitungsvertrages?	130
D. Form der Auftragsverarbeitungsverträge	131
E. Welche Vorteile bieten Auftragsverarbeitungsverträge?	132
F. Was sind typische Auftragsverarbeitungen im Notarbüro?	132

§ 7 Datenschutzbeauftragter	135
A. Einleitung	135
B. Welche Qualifikation muss ein Datenschutzbeauftragter haben?	135
C. Stellung des Datenschutzbeauftragten	143
D. Aufgaben des Datenschutzbeauftragten	144
E. Haftung des Datenschutzbeauftragten	152
F. Wann muss ein Datenschutzbeauftragter benannt werden?	154
G. Wann muss ein stellvertretender Datenschutzbeauftragten wo benannt werden?	156
H. Kündigungsschutz	156
I. Rechtsfolgen fehlerhafter oder unterlassener Bestellung	157
§ 8 Definition des Datenschutzvorfalls	159
A. Vorbemerkung	159
B. Was ist eine Datenschutzverletzung?	159
C. Wann ist diese der Aufsichtsbehörde zu melden?	161
D. Wie schnell muss die Meldung erfolgen?	164
E. Wie muss die Meldung erfolgen?	164
F. Dokumentation der Datenpanne	172
G. Meldepflicht gegenüber Betroffenen	174
§ 9 Besonderheiten im Anwaltsnotariat	177
A. Vorbemerkung	177
B. Kollisionsprüfung	179
C. Aufbewahrungsfristen	182
D. Privacy by Default	184
E. Geldwäschedokumentation	185
§ 10 Technisch-Organisatorische Maßnahmen	187
A. Grundlagen	187
I. Risikobasierter Ansatz	188
II. Risikoanalyse	190
1. Durchführung einer Risikoanalyse	191
a) Schutzgut	191

b) Mögliche Datenschutzverletzung	191
aa) Auswirkungen der Datenschutzverletzung für den Betroffene	191
bb) Aufwand um die Folgen der Datenschutzverletzung überwinden	192
c) Prüfungsfaktoren	192
d) Strukturanalyse	193
e) Risikoabstufung	195
2. Auswahl und Umsetzung	197
a) Stand der Technik	199
b) Implementierungskosten	199
B. Die Besonderheiten des § 6 NotAktVV	200
C. ToMs unter besonderer Berücksichtigung des Urkundenarchivs	202
I. Pseudonymisierung	203
II. Verschlüsselung	203
III. Vertraulichkeit	205
1. Zutrittssicherung	206
2. Zugangssicherung	208
3. Zugriffssicherung	211
IV. Gewährleistung der Integrität	213
V. Exkurs: Cyberangriffe	215
VI. Gewährleistung der Verfügbarkeit	219
VII. Gewährleistung Belastbarkeit der Systeme	221
VIII. Gewährleistung der zeitnahen Wiederherstellung der Verfüg- barkeit	222
IX. Kontrolle der Maßnahmen/Schulung	222
X. Datenschutzfreundliche Voreinstellung	223
§ 11 Anhang: Musterverarbeitungsverzeichnisse der BNotK	225
A. Vorbemerkung	225
B. Datenschutzhinweise für Mandanten	226
C. Urkundenverzeichnis	228
D. Verwahrungsverzeichnis	230
E. Vermerke über Wechsel- und Scheckproteste	232
F. Geldwäschegesetz	234

G. Amtsprüfung	237
H. Grundstücksgeschäfte	239
I. Gesellschaftsrecht	244
J. Erbrecht	249
K. Familienrecht	254
L. Vorsorgevollmacht und Patientenverfügung	259
M. Sonstige Niederschriften	263
N. Protokollierung des Grundbuchinhalts durch den Notar	267
O. Einhaltung von Mitwirkungsverboten	269
P. Übersicht über die Verwahrungsgeschäfte	271
Q. Zahlungsverkehr, Rechnungswesen und Mahnwesen, Finanzbuchhaltung	273
R. Videoüberwachung	275
S. Protokollierung der Internetzugriffe	277
T. Mitarbeiterverwaltung und Lohnbuchhaltung	279
U. Arbeitszeiterfassung	281
V. Sonstige Bürokommunikation	283
Stichwortverzeichnis	285

Autorenverzeichnis

Ingo Drube

Rechtsanwalt, Syndikusrechtsanwalt, Geschäftsführer GNotDs Gesellschaft für notariellen Datenschutz mbH, Leipzig

Dr. Christian Flache

Notar, Leipzig

Stephan Hansen-Oest

Rechtsanwalt, Fachanwalt für IT-Recht, Certified Information Privacy Professional Europe (CIPP/E), Flensburg

Dr. Andreas Salzmann

Notar, Hof

Drx. Frank Tykwer

Rechtsanwalt und Notar, Datenschutzbeauftragter, Geschäftsführer der DSB für Notare und Ärzte GmbH, Recklinghausen

Abkürzungsverzeichnis

A

a.A.	andere Ansicht
a.a.O.	am angegebenen Ort
Abs.	Absatz
Abschn.	Abschnitt
A.d.ö.R.	Anstalt des öffentlichen Rechts
a.E.	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AG	Aktiengesellschaft/Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
Alt.	Alternative
Anh.	Anhang
Anm.	Anmerkung
ArbGG	Arbeitsgerichtsgesetz
ArchivNotBek	Gemeinsame Bekanntmachung des Bayerischen Staatsministeriums der Justiz und des Bayerischen Staatsministeriums für Wissenschaft, Forschung und Kunst über die Aufbewahrung, Abgabe und Vernichtung von Notariatsakten
Art.	Artikel
Aufl.	Auflage
Az.	Aktenzeichen

B

BAnz	Bundesanzeiger
BauGB	Baugesetzbuch
bay.	bayerisch(e)
BayDSG	Bayerisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
beA	Besonderes Elektronisches Anwaltspostfach
BeckOK	Beck'scher Onlinekommentar
beN	Besonderes Elektronisches Notarpostfach
Beschl.	Beschluss

Abkürzungsverzeichnis

BeurkG	Beurkundungsgesetz
BeurkG-2022	Beurkundungsgesetz in der ab dem 1.1.2022 gültigen Fassung
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des BGH in Zivilsachen
BNotK	Bundesnotarkammer
BNotO	Bundesnotarordnung
BNotO-E	Bundesnotarordnung in der Entwurfsfassung
BRAO	Bundesrechtsanwaltsordnung
BRD	Bundesrepublik Deutschland
BR-Drucks.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drucks.	Bundestagsdrucksache
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des BVerfG
bzw.	beziehungsweise

C

CD	Compact Disc
CERT	Computer Emergency Response Team
COD	Ordinary legislative procedure

D

DDR	Deutsche Demokratische Republik
ders.	derselbe
d.h.	das heißt
dies.	dieselbe/dieselben
DMS	Dokumenten Management System
DNotI	Deutsches Notarinstitut
DNotI-Report	Informationsdienst des Deutschen Notarinstituts (Zs.)

DNotZ	Deutsche Notar-Zeitschrift
DONot	Dienstordnung für Notarinnen und Notare
DSB	Datenschutzbeauftragte
DSG	Datenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DSRL	Datenschutzrichtlinie
DuD	Datenschutz und Datensicherheit (Zs.)

E

Ed.	Edition
EDSA	Europäischer Datenschutzausschuss
EDV	Elektronische Datenverarbeitung
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	EG-Vertrag
EGZPO	Einführungsgesetz zur Zivilprozessordnung
Einl.	Einleitung
einschl.	einschließlich
ENA	Elektronische Notaranderkontenführung
ErwG	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRCh	Charta der Grundrechte der Europäischen Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht

F

f.	folgende
FAQ	Frequently asked questions
ff.	fort folgende
FIU	Financial Intelligence Unit
Fn.	Fußnote

G

GBO	Grundbuchordnung
GbR	Gesellschaft bürgerlichen Rechts
GBV	Verordnung zur Durchführung der Grundbuchordnung
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
ggü.	Gegenüber
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GnotDS	Gesellschaft für notariellen Datenschutz mit beschränkter Haftung
GNotKG	Gesetz über Kosten der freiwilligen Gerichtsbarkeit für Gerichte und Notare
GRCh	Charta der Grundrechte der Europäischen Union
grds.	grundsätzlich
GVBl.	Gesetz- und Verordnungsblatt
GwG	Geldwäschegesetz
Gz.	Geschäftszeichen

H

HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HdB	Handbuch
HGB	Handelsgesetzbuch
h.M.	herrschende Meinung
HmbBfDI	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit
Hs.	Halbsatz

I

i.d.F.	in der Fassung
i.d.R.	in der Regel
i.H.v.	in Höhe von
insb.	insbesondere
IP-Adresse	Internet Protokoll Adresse

i.S.d.	im Sinne des
i.S.e.	im Sinne einer/eines
IT	Informationstechnik
i.Ü.	im Übrigen
i.V.m.	in Verbindung mit

J

jM	juris – Die Monatszeitschrift
juris	juris (Datenbank)
JuS	Juristische Schulung (Zs.)

K

Kap.	Kapitel
KMU	Kleine und mittelständische Unternehmen
KOM	Dokumente der Kommission der Europäischen Gemeinschaft
KostO	Kostenordnung
krit.	kritisch
KV	Kostenverzeichnis

L

LfD	Landesbeauftragter für Datenschutz
LG	Landgericht
lit.	litera (Buchstabe)
LPartG	Lebenspartnerschaftsgesetz

M

m. abl. Anm.	mit ablehnender Anmerkung
m. Anm.	mit Anmerkung
M.E.	Meines Erachtens
Mio.	Million
MIRT	Mobile Incident Response Team
MittRhNotK	Mitteilungen der Rheinischen Notarkammer (Zs.)
MMR	Zeitschrift für IT-Recht und Recht der Digitalisierung (Zs.)
m.w.N.	mit weiteren Nachweisen

Abkürzungsverzeichnis

N

n.F.	neue Fassung
NJ	Neue Justiz (Zs.)
NJW	Neue Juristische Wochenschrift (Zs.)
NotAktVV	Verordnung über die Führung notarieller Akten und Verzeichnisse
notar	notar – Monatsschrift für die gesamte notarielle Praxis
NotBZ	Zeitschrift für die notarielle Beratungs- und Beurkundungspraxis
NotK	Notarkammer
Nr.	Nummer
n.v.	nicht veröffentlicht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht Rechtsprechungs-Report
NZA	Neue Zeitschrift für Arbeitsrecht

O

o.g.	oben genannt
OLG	Oberlandesgericht
OLG-Präsident	Präsident des Oberlandesgerichts
OLGZ	Entscheidungssammlung der Oberlandesgerichte in Zivilsachen
OVG	Oberverwaltungsgericht
OWi	Ordnungswidrigkeiten
OWiG	Gesetz über Ordnungswidrigkeiten

P

PC	Personal Computer
PDF	Portable Document Format

R

Rdn	Randnummer (intern)
RdSchr	Rundschreiben
RdVfg.	Rundverfügung
RegE	Regierungsentwurf
Rn	Randnummer (extern)

RNotZ	Rheinische Notar-Zeitung
RPfleger	Der deutsche Rechtspfleger (Zs.)
RS-BNotK	Rundschreiben der Bundesnotarkammer
Rspr.	Rechtsprechung

S

S.	Seite/Satz
s.a.	siehe auch
SächsDSG	Sächsisches Datenschutzgesetz
SächsJustizG	Sächsisches Justizgesetz
SächsVerm-KatG	Sächsisches Vermessungs- und Katastergesetz
s.o.	siehe oben
sog.	sogenannt
SSO	single sign on
st. Rspr.	ständige Rechtsprechung
Std.	Stand
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
str.	streitig
s.u.	siehe unten

T

TLS	Transport Layer Security
ToM	Technisch organisatorische Maßnahmen

U

u.a.	unter anderem
Urt.	Urteil
USB	Universal Serial Bus
USV	Unterbrechungsfreie Stromversorgung
usw.	und so weiter
u.U.	unter Umständen

V

v.	vom/von
vgl.	vergleiche
VO	Verordnung
Vorbem.	Vorbemerkung
VPN-Client	Virtual Private Network Client
VVT	Verzeichnis aller Verarbeitungstätigkeiten

Z

z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz (Zs.)
Ziff.	Ziffer
ZPO	Zivilprozessordnung
Zs.	Zeitschrift
z.T.	zum Teil
ZTR	Zentrales Testamentregister
ZTRV	Verordnung zur Einrichtung und Führung des Zentralen Testamentregisters
zust.	zustimmend
ZVertriebsR	Zeitschrift für Vertriebsrecht
z.Zt.	zur Zeit

Literaturverzeichnis

- Blaeschke*, Praxishandbuch Notarprüfung, 3. Auflage 2021
- Ehmann/Selmayr*, Datenschutz-Grundverordnung: DS-GVO, 2. Auflage 2018
- Franzen/Gallner/Oetker*, Kommentar zum europäischen Arbeitsrecht, 3. Auflage 2020
- Frenz/Miermeister*, BNotO – Bundesnotarordnung, 5. Auflage 2020
- Gierschmann/Schlender/Stentzel/Veil*, Kommentar Datenschutz-Grundverordnung, 2017
- Geißen/Bannasch/Naumann*, SächsDSG, 2011
- Gola*, Datenschutz-Grundverordnung: DS-GVO, 2. Auflage 2018
- Görk*, BeckOK BNotO
- Hansen-Oest*, Datenschutzbeauftragte, 2. Auflage 2020
- Heckschen/Herrler/Münch*, Beck'sches Notar-Handbuch, 7. Auflage 2019
- Heselhaus/Nowak*, Handbuch der Europäischen Grundrechte, 2. Auflage 2020
- Kühling/Buchner*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG, 3. Auflage 2020
- Maurer/Waldhoff*, Allgemeines Verwaltungsrecht, 20. Auflage 2020
- Meikel*, Grundbuchordnung: GBO, 12. Auflage 2020
- Moos/Schefzig/Arning*, Praxishandbuch DSGVO, 2. Auflage 2021
- Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG DS-GVO 3. Auflage 2021
- Paschke/Berlit/Meyer/Kröner*, Hamburger Kommentar Gesamtes Medienrecht, 4. Auflage 2020
- Plath*, DSGVO/BDSG, 3. Auflage 2018
- Schippel/Görk*, Bundesnotarordnung: BNotO, 10. Auflage 2021
- Schmidt/Weichert*, Datenschutz, 2012
- Simitis/Hornung*, Datenschutzrecht, DSGVO, 2019
- Sydow*, Europäische Datenschutzverordnung, 2. Auflage 2018
- Taeger/Gabel*, DSGVO – BDSG – TTDSG, 4. Auflage 2021

Wolff/Bachof/Stober/Kluth, Verwaltungsrecht I, 13. Auflage 2017

Wolff/Brinck, BeckOK DatenschutzR

§ 1 Einführung in den Datenschutz

A. Vorbemerkung

Die Wurzeln des Datenschutzrechts reichen weiter in die Vergangenheit, als man dies mit Blick auf die Literatur und die Rechtsprechung vermuten mag. Zwar hat dieses Rechtsgebiet erst in jüngerer Zeit eine eigenständige Bedeutung erfahren. Die Sorge vor dem Missbrauch von Daten ist in der Rechtswissenschaft aber nicht erst seit der globalen Verarbeitung einiger weniger, vor allem US.-amerikanischer, Digitalkonzerne, Gegenstand von Regelungen und Entscheidungen.

Die **Grundlage des Datenschutzes** wird derzeit im Wesentlichen in der informationellen Selbstbestimmung gesehen, welche ihrerseits auf dem allgemeinen Persönlichkeitsrecht und damit auf einem Grundrecht beruht. Diese dogmatische Anknüpfung wurde zwar erst in der zweiten Hälfte des letzten Jahrhunderts herausgearbeitet. Die Ursprünge der Vertraulichkeit reichen aber noch weiter zurück. Erste Bestrebungen des Staates, die Weitergabe von Informationen zu beschränken, finden sich etwa im Post- oder Steuergeheimnis. Diese Begrenzung des Zugriffs staatlicher Stellen auf beim Staat vorhandene Daten diente jedoch nicht vorrangig dem Schutz des Einzelnen. So ist etwa die Diskretion der Postbeamten bei der Übermittlung von Nachrichten vielmehr Voraussetzung für die Akzeptanz dieser damals neuen Dienstleistung und damit letztlich auch Voraussetzung für die Möglichkeit Porti zu erheben.¹

Echte Konturen als Persönlichkeitsrecht erhielt das Datenschutzrecht erst mit dem **Aufkommen moderner Datenverarbeitung** durch den Staat. Erst als es dem Staat möglich war durch maschinelle Unterstützung, wie etwa Lochkartenautomaten oder durch Ordnersysteme, eine geordnete Aktenführung und Auswertung zu betreiben, wurde klar, welches Missbrauchspotential sich hinter einer großen Datenmenge verbergen kann. Offenbar wurde die Macht über Daten dann im Dritten Reich. Mit Hilfe der Daten, die der deutsche Beamte angesammelt hatte, war es möglich die Verfolgung von Juden, Homosexuellen und Systemkritikern in dem Maße zu betreiben, wie tatsächlich geschehen. Später setzte die DDR die Datenerhebung und -sammlung bis ins Extreme fort. Aber auch in der Bundesrepublik wurde in

1 Schmidt/Weichert/von Lewinski, Datenschutz, S. 26.

Reaktion auf die Rote Armee Fraktion die technische Überwachung einzelner Personen mittels deren verfügbarer Daten stark vorangetrieben.

B. Datenschutz und Geheimnisschutz

- 2 Der Schutz der Daten spielte im Notariat schon immer eine wesentliche Rolle. Die Geheimhaltung gehört für den Notar schließlich zu seinem berufsrechtlichen Selbstverständnis. Sie ist aber auch aus Sicht des Bürgers neben seiner fachlichen Kompetenz eine elementare Säule des Vertrauens in den Notar. Häufig erhält der Notar nur wegen seiner Verschwiegenheit die für seine Arbeit so notwendigen Angaben von den Beteiligten. Insofern sind Notare von Berufs wegen schon geborene Beschützer von Daten.

Hinweis

Der Schutz von Daten i.S.d. Datenschutzrechts ist jedoch mit dem berufsrechtlichen Geheimnisschutz nicht deckungsgleich. Dies zeigt sich zum einen an der jeweiligen Schutzrichtung und zum anderen an den zur Erreichung des Ziels notwendigen Maßnahmen. So regelt die Verschwiegenheitsverpflichtung der Notare das grundsätzliche Verbot einer Offenbarung der von den Rechtssuchenden übermittelten Daten und Informationen. Hierzu gehört auch, den Zugriff auf diese Daten zu verhindern und damit gleichsam eine passive Verschwiegenheitsverletzung zu verhindern. Dennoch ist Datenschutz etwas anderes als Geheimnisschutz. Dies wird besonders daran deutlich, dass der Datenschutz auch Bereiche einschließt, die § 18 BNotO nicht erfasst, wie etwa die Mitarbeiterdaten oder Daten von Lieferanten und Dienstleistern. Der Geheimnisschutz richtet sich zudem nicht gegen den Beteiligten selbst, während das Datenschutzrecht jegliche Daten und damit auch die des Beteiligten erfasst.² Andererseits erfasst der Geheimnisschutz auch Informationen, die dem Notar nur mündlich oder fernmündlich zugetragen wurden. Die DS-GVO greift hier nicht ein, da diese Daten nicht vom Anwendungsbereich erfasst sind.³

2 Frenz/Miermeister/Bremkamp, BNotO, § 18 Rn 156, Schippel/Bracker/Kanzleiter, BNotO, § 18 Rn 7.

3 Mit Ausnahme der Arbeitnehmerdaten. vgl. dazu auch unten unter Anwendungsbereich.

C. Datenschutz und IT-Sicherheit

Eine ähnliche Schnittmenge bildet die Sicherheit von Informationstechnik mit dem Datenschutz. Die **Sicherheit in der Informationstechnik** oder kurz IT-Sicherheit hat einen sehr technischen Fokus. Hier geht es um die Funktionsfähigkeit von IT-Systemen und Komponenten sowie die Verwendung von Prozessen, welche die Datensicherheit gewährleisten oder gar verbessern sollen. Das Ziel solcher Regelungen, wie sie sich etwa im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI-Gesetz) finden, ist also der Schutz der IT an sich. Der Schutz von Individualrechten, wie sie etwa die personenbezogenen Daten darstellen, erfolgt gleichsam als Reflex. Die technischen Vorgaben der IT-Sicherheit tragen aber zur Sicherheit der Daten bei.

Besonders hervorgehoben ist in diesem Zusammenhang die **kritische Infrastruktur**. Hierunter versteht der Gesetzgeber etwa die Sektoren

- Energie,
- Telekommunikation,
- Transport,
- Gesundheit,
- Wasser,
- Ernährung und alle
- anderen Bereiche des öffentlichen Lebens, die für das Funktionieren des Gemeinwesens von hoher Bedeutung sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.⁴

Mit dem IT-Sicherheitsgesetz wurde hierzu das CERT-Bund geschaffen. Das **Computer Emergency Response Team**, ist für Bundesbehörden die zentrale Anlaufstelle für alle Fragen rund um die Reaktion auf oder die Vorsorge vor sicherheitsrelevanten Vorfällen in IT-Systemen. Zur Angriffsabwehr wurden zudem „Mobile Incident Response Teams“ (MIRT) geschaffen. Dabei handelt es sich um eine Art „Cyber-Feuerwehr“, die vor Ort die IT-Infrastruktur nach einem Angriff wieder in Funktion setzen soll.

Notare bilden zwar einen Teil der Justiz. Allerdings hat der Gesetzgeber entschieden, dass die vorsorgende Rechtspflege nicht derart systemrelevant ist, dass eine vorübergehende Beeinträchtigung ihrer Funktionstüchtigkeit zu einer Gemeinwohlgefährdung führen würde. Ob diese Einschätzung vor

4 Vgl. § 2 Abs. 10 BSI-Gesetz.

dem Hintergrund der Einschränkungen des öffentlichen Lebens, wie sie sich pandemiebedingt im Jahr 2020/2021 ereigneten, und der faktischen Nichterreichbarkeit der Gerichte noch einmal überdacht wird, bleibt abzuwarten. Vor dem Hintergrund der damit einhergehenden Verschärfung der Anforderungen an die IT-Systeme des Notars (unabhängig von der Größe der jeweiligen Einheit) sollte man hier mit Wünschen allerdings vorsichtig sein.

D. Entstehung des Datenschutzrechts

- 4 Den Beginn des Datenschutzrechts als selbstständige Disziplin markiert ein deutsches, genauer ein hessisches Gesetz. Mit dem Hessischen Datenschutzgesetz vom 30.9.1970⁵ wurde weltweit die erste staatliche Kodifikation eines eigenständigen Datenschutzrechts vorgenommen. Diese war die Reaktion auf den **Mikrozensus-Beschluss** des BVerfG vom 16.7.1969.⁶ Das erste Bundesdatenschutzgesetz trat erst am 1.1.1978 in Kraft⁷ und wurde in den Folgejahren regelmäßig den geänderten Umständen angepasst.⁸
- 5 Auf europäischer Ebene ist die **Konvention Nr. 108 des Europarats als erster legislativer Akt zu nennen**. Dieser erste überstaatliche Rechtstext zum Schutz persönlicher Daten entstand in Europa somit nicht im Rahmen der europäischen Gemeinschaften. Vielmehr ging die Initiative vom Europarat aus, der seit 1949 die Entwicklung eines europäischen Systems des Schutzes der Menschenrechte betreut. Er hatte sich im Wesentlichen darauf beschränkt, Anforderungen an die Qualität der Daten zu formulieren.⁹ Gleichzeitig beabsichtigte die Konvention Nr. 108 den Austausch von personenbezogenen Daten zwischen den Vertragsstaaten: „eine Vertragspartei darf allein zum Zwecke des Schutzes des Persönlichkeitsbereichs den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei nicht verbieten oder von einer besonderen Genehmigung abhängig machen“ (Art. 12 Abs. 2DS-GVO).

5 GVBl. 1970 I, S. 625. Dem folgten das bayerische EDV-Organisationsgesetz, das schwedische Datenschutzgesetz 1973, der Privacy Act 1974 in den USA und das norwegische Datenschutzgesetz 1978.

6 BVerfG, Beschl. v. 16.7.1967 – 1 BvL 19/63, BVerfGE 27, 1.

7 BGBII 1977, S. 201.

8 Siehe zum Ganzen: *Held* in: Hamburger Kommentar Gesamtes Medienrecht, 76. Abschnitt.

9 *Breuer* in: Heselhaus/Nowak, EU-Grundrechte-HdB, § 25 Datenschutz Rn 15.

Der erste Rechtsakt der EU in diesem Bereich war die Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG), welche am 24.10.1995 in Kraft trat.¹⁰ Dieser war ein über fünf Jahre währender Beratungsprozess voraus gegangen. Noch länger währte die Entstehungsphase der DS-GVO. Ausgangspunkt der Verordnung war ein Entwurf der EU-Kommission aus dem Januar 2012.¹¹

E. Die Datenschutzgrundverordnung

Die Datenschutzgrundverordnung (DS-GVO) trat als zentrale Norm eines harmonisierten Datenschutzes am 25.5.2018 in Kraft. Sie beruht in weiten Teilen auf den Erkenntnissen der Datenschutzrichtlinie und hat diese ersetzt.

I. Struktur und Ziele der Verordnung

Nach eigenem Bekunden schützt die Verordnung gem. Art. 1 Abs. 2 und 3 DS-GVO „*die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten*“ sowie den freien „*Verkehr personenbezogener Daten in der Union*“. Zur Erreichung dieser Ziele bestimmt die Verordnung verschiedene Grundsätze bei der Verarbeitung von Daten. Zu nennen ist etwa die Vorgabe, dass Daten nur auf Grundlage einer Erlaubnisnorm verarbeitet werden dürfen (**Grundsatz der Rechtmäßigkeit**) oder dass stets so wenig wie möglich Daten zu verarbeiten sind (**Grundsatz der Datenminimierung**). Teilweise werden diese Grundsätze näher geregelt, teilweise dienen sie nur als Auslegungsgrundlage.

Aus der Entstehungsgeschichte heraus folgt zudem ein weniger offizielles Ziel. Die Erfahrungen mit der Vorgängerregelung zum europäischen Datenschutz, der Datenschutz-Richtlinie, zeigten, dass die **größten Gefahren für**

10 Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG) vom 24.10.1995 AB1 1995 L 281, 31.

11 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 011 endgültig, 2012/0011 (COD), 25.1.2012.

das Grundrecht auf Datenschutz¹² von wenigen Datenverarbeitern herühren. Zur echten Gefahr wird die Datenverarbeitung erst durch die Auswertung großer Mengen an Daten (sog. **Data-Mining**). Hierzu bedarf es des Zugriffs auf möglichst viele Datensätze verbunden mit der Möglichkeit, diese nach verschiedenen Parametern auswerten zu können. Dieses Vorgehen stellt das Geschäftsmodell einiger, vor allem großer US-Unternehmen, wie etwa Google, Amazon oder Facebook dar. Die DS-GVO war also ersichtlich auch konzipiert, um dem Datenhunger und damit der Marktmacht großer Unternehmen zu begegnen. Diesen Konzernen dürfte ob ihrer Schlagkraft auch eine hohe Regelungs- und Kontrolldichte ohne weiteres zuzumuten sein. Zahlreiche Kleinunternehmer oder gemeinnützige Institutionen treffen diese Regelungen zwar ebenso. Diese können den zugehörigen administrativen Aufwand aber oft nur mit Mühe stemmen.

Auch mit Blick auf das drohende Risiko erscheinen einem manche Vorgaben der DS-GVO als überzogen. Insbesondere könnte man sich auf den Standpunkt stellen, die Datenmenge bei kleineren Handwerksbetrieben oder Dienstleistern sei nicht groß genug, um damit Schaden anzurichten.

Dies ist gleich aus zwei Gründen zu kurz gesprungen:

- Zum einen hängt die Brisanz der Daten nicht allein von deren Menge ab. Dies wird gerade im Notariat deutlich. Hier werden neben sehr intimen Daten, etwa im Rahmen von Eheverträgen, auch wirtschaftlich bedeutsame Umstände, etwa im Rahmen von Unternehmertestamenten verarbeitet.
- Zum anderen können auch für sich betrachtet weniger relevante Daten zu einem Problem für die Betroffenen werden, wenn Dritte unbefugt darauf zugreifen können und dann mit weiteren Datensätzen verknüpfen. Ein grundlegendes Maß an Schutzvorkehrungen zur Sicherung der Daten ist daher bei jeder datenverarbeitenden Stelle notwendig.

- 8 Das **Korrektiv für einen überschießenden Datenschutz** ist bereits in der Verordnung selbst angelegt. Die DS-GVO ist von einem risikobasierten Ansatz getragen. Die **Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die Rechte und Freiheiten der betroffenen Person bei der Datenverarbeitung spielen eine wesentliche Rolle für die zu ergreifenden Maßnahmen.¹³ Für den Notar ist dies allerdings nicht mit einer Erleichterung im Sinne ei-

¹² Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union.

¹³ ErwG 76.