

Timo Bittner

# Geeignete Rahmenbedingungen für ein Datenschutzaudit bei Auftragsverarbeitern

Eine Untersuchung von Ausgestaltung,  
Nutzen und Aussagekraft



**Nomos**

## Der Elektronische Rechtsverkehr

Herausgegeben von  
Prof. Dr. Alexander Roßnagel und  
Prof. Dr. Gerrit Hornung, LL.M.  
in Zusammenarbeit mit  
dem TeleTrusT Deutschland e.V.

Band 46

Timo Bittner

# Geeignete Rahmenbedingungen für ein Datenschutzaudit bei Auftragsverarbeitern

Eine Untersuchung von Ausgestaltung,  
Nutzen und Aussagekraft



**Nomos**



Onlineversion  
Nomos eLibrary

**Die Deutsche Nationalbibliothek** verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Zugl.: Kassel, Univ., Diss., 2020

ISBN 978-3-8487-7173-8 (Print)

ISBN 978-3-7489-1219-4 (ePDF)

1. Auflage 2021

© Nomos Verlagsgesellschaft, Baden-Baden 2021. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

## Danksagung

Ich widme diese Arbeit meinen Kindern Isabella und Magnus und danke meiner Frau Anna-Caroline dafür, dass ich die Zeit für diese Arbeit aufbringen konnte.

Für die hilfreiche Unterstützung während der Arbeit danke ich meinem Doktorvater Herrn Prof. Dr. Alexander Roßnagel.

Darüber hinaus bedanke ich mich bei allen, die mich in irgendeiner Weise dabei unterstützt haben, diese Arbeit schreiben zu können.



# Inhaltsverzeichnis

Abkürzungsverzeichnis	15
1 Einleitung	23
1.1 Problematik	23
1.2 Ziele der Arbeit	25
1.3 Methodik	31
2 Grundlagen	34
2.1 Ziele und Nutzen eines Datenschutzaudits bei Auftragsverarbeitern	37
2.1.1 Fortlaufende Verbesserung des Datenschutzes und der Datensicherheit	38
2.1.2 Datenschutz als Lernsystem	41
2.1.3 Erleichterung bei der Umsetzung von gesetzlichen Vorgaben	43
2.1.4 Steigerung der Selbstverantwortung	47
2.1.5 Senkung des Vollzugsdefizits	50
2.1.6 Senkung von Haftungsrisiken	52
2.1.7 Verringerung von Bußgeldrisiken	53
2.2 Bisherige Initiativen und Bestrebungen in der Bundesrepublik Deutschland	54
2.3 Neueste legislative Entwicklungen in Europa	68
2.4 Ausländische Entwicklungen in der Vergangenheit	71
3 Existierende Modelle als Vorbilder	78
3.1 Umweltaudit	78
3.1.1 Grundlagen	78
3.1.2 Ziele	80
3.1.3 Auditgegenstand	87
3.1.4 Ablauf	88
3.1.5 Resümee	90

*Inhaltsverzeichnis*

3.2	QM-Audit	93
3.2.1	Grundlagen	93
3.2.2	Ziele	96
3.2.3	Auditgegenstand	98
3.2.4	Ablauf	99
3.2.5	Resümee	101
3.3	Informationssicherheitsaudit	102
3.3.1	Grundlagen	104
3.3.2	Ziele	106
3.3.3	Auditgegenstand	107
3.3.4	Ablauf	108
3.3.5	Resümee	108
3.4	Analyse bisheriger Datenschutzzertifizierungen	110
3.4.1	DSZ	110
3.4.2	ULD	114
3.4.3	Gütesiegel Datenschutz M-V	120
3.4.4	EuroPriSe	125
3.4.5	Stiftung Datenschutz	129
3.4.6	Andere Anbieter	132
3.4.7	Resümee	136
4	Die Auftragsverarbeitung	138
4.1	Gegenstand	138
4.2	Rahmenbedingungen	141
4.3	Abgrenzung von der Funktionsübertragung	145
4.3.1	Kontaktaufnahme	148
4.3.2	Rechte der betroffenen Personen	149
4.3.3	Finanzielles Eigeninteresse	149
4.3.4	Eigene Geschäftszwecke	150
4.3.5	Hilfsfunktion	151
4.4	Beteiligte Stellen	152
4.4.1	Verantwortlicher	152
4.4.2	Auftragsverarbeiter	160
4.4.3	Abgrenzung	163
4.5	Technische und organisatorische Maßnahmen	165
4.5.1	Auswahl des Auftragnehmers	165
4.5.2	Überzeugung von der Geeignetheit der Maßnahmen	167



4.5.3	Dokumentationspflicht	175
5	Gegenstand des Audits	177
5.1	Regelungen der DS-GVO	177
5.2	Objektiver Gegenstand	178
5.2.1	Auftragsverarbeiter	178
5.2.2	Dateien und Datenbanken	181
5.2.3	Verarbeitungszwecke	182
5.2.4	Produkte	183
5.2.5	Dienstleistungen	185
5.3	Subjektiver Gegenstand	190
5.4	Grenzen des Audits	196
6	Pflicht oder Freiwilligkeit	202
6.1	Regelungen der DS-GVO	202
6.2	Pflicht	202
6.3	Freiwilligkeit	205
6.4	Abwägung	206
7	Inhalt und Ablauf des Audits	212
7.1	Regelungen der DS-GVO	212
7.2	Allgemeine Voraussetzungen	213
7.2.1	Festlegung der Dienstleistung	213
7.2.2	Vertragsabschlüsse	214
7.2.2.1	Verträge mit Unterauftragnehmern	214
7.2.2.2	Vertrag mit dem Auditor	217
7.2.2.2.1	Vertragsart	217
7.2.2.2.1.1	Werkvertrag	217
7.2.2.2.1.2	Dienstvertrag	219
7.3	Auditvorbereitung	221
7.3.1	Festlegung des Auditgegenstandes	222
7.3.2	Grundlagen für die Vorbereitung	224

*Inhaltsverzeichnis*

7.4	Auditverfahren	227
7.4.1	Internes Auditverfahren	227
7.4.1.1	Datenschutzprüfung	227
7.4.1.1.1	Bestimmung der einschlägigen Vorschriften	228
7.4.1.1.2	Prüfung der Einhaltung der Vorschriften	229
7.4.1.1.2.1	Datenminimierung	231
7.4.1.1.2.2	Anonymisierung	241
7.4.1.1.2.3	Moderne Instrumente des Datenschutzes	246
7.4.1.1.2.4	Sicherheit der Verarbeitung	254
7.4.1.2	Datenschutzmanagementsystem	325
7.4.1.3	Datenschutzpolitik	328
7.4.1.4	Datenschutzprogramm	329
7.4.1.5	Wirksamkeitsprüfung und Datenschutzerklärung	331
7.5	Externes Auditverfahren	335
7.5.1	Prüfung und Bewertung der Unterlagen	336
7.5.2	Kontrolle und Stichproben	338
7.6	Fehlerquellen der Praxis	339
7.7	Nachbereitung	341
7.7.1	Zertifizierung	341
7.7.2	Folgeaudits und Rezertifizierungen	347
7.8	Anforderungen der Praxis	349
8	Auswirkungen der Auditergebnisse	352
8.1	Regelungen der DS-GVO	352
8.2	Fortlaufende Verbesserung von Datenschutz und Datensicherheit	353
8.3	Datenschutz als Lernsystem	353
8.4	Erleichterung bei der Umsetzung von gesetzlichen Vorgaben	354
8.5	Steigerung der Selbstverantwortung	356
8.6	Senkung des Vollzugsdefizits	356
8.7	Senkung von Haftungsrisiken	357
8.8	Verringerung von Bußgeldrisiken	357

9	Rollen und Aufgaben der unterschiedlichen Akteure	359
9.1	Regelungen der DS-GVO	359
9.2	Rollen- und Aufgabendarstellung	359
9.2.1	Verantwortliche	360
9.2.2	Auftragsverarbeiter	361
9.2.3	Auditoren	361
9.2.4	Betriebliche und behördliche Datenschutzbeauftragte	362
9.2.5	Aufsichtsbehörden für den Datenschutz	365
9.2.6	Öffentlichkeit	368
9.2.7	Betroffene Personen	370
9.2.8	Zertifizierungsstelle	371
9.3	Interessenkonflikte	372
9.3.1	Konflikte zwischen den Interessen	372
9.3.2	Folgen von Interessenkonflikten	375
10	Auditoren	377
10.1	Regelungen der DS-GVO	377
10.2	Persönliche Anforderungen an Auditoren	378
10.2.1	Unabhängigkeit	378
10.2.2	Zuverlässigkeit	383
10.2.3	Fachkunde	388
10.2.3.1	Datenschutzfachkunde	389
10.2.3.2	Auditkunde	391
10.3	Rahmenbedingungen	392
10.4	Ausbildung und Zulassung des Auditors	394
11	Branchenspezifische Besonderheiten	398
11.1	Regelungen der DS-GVO	398
11.2	Personaldienstleistungen	399
11.2.1	Zeiterfassung	399
11.2.2	Entgeltabrechnung	401
11.2.3	Personalaktenführung	403
11.2.4	Bewerbungsmanagement	405
11.3	IT-Dienstleistungen	407
11.3.1	Cloud-Computing	407

*Inhaltsverzeichnis*

11.3.2	Prüfung und Wartung	414
11.3.2.1	Vor Ort	416
11.3.2.2	Fernwartung	416
11.4	Hosting von E-Shops	418
11.5	Marketingdienstleistungen	419
11.5.1	Direktmarketing	419
11.5.2	Preisausschreibung	421
11.5.3	Kundenbefragungen	422
11.5.4	Webanalyse	423
11.6	Kundenbetreuung	424
11.7	Datenentsorgung	425
11.7.1	Vernichtung von elektronischen Datenträgern	426
11.7.2	Vernichtung von Papierdokumenten	427
11.8	Telearbeit	427
11.9	Werkschutz	428
11.10	Akteneinlagerung	429
12	Regelungsrahmen	431
12.1	Grundbedingungen für die Aussagekraft des Audits	433
12.1.1.1	Transparenz	435
12.1.1.2	Vergleichbarkeit	436
12.1.1.3	Qualität	437
12.2	Regelung durch den Markt	438
12.2.1	Angebote durch Interessenvertretungen	438
12.2.2	Initiativen durch Aufsichtsbehörden	439
12.2.3	Audits auf Grundlage von technischen Normen	440
12.3	Legislative Regelung	442
12.3.1	Europäische Vorgabe	451
12.3.2	Nationales Gesetz	456
12.3.3	Supranationale und nationale Kombination	460
13	Empfehlung für legislative Maßnahmen	481
14	Vertragsinhalt	489
14.1	Vertragsparteien	490

14.2	Vertragsabschluss und Vertragsbeginn	490
14.3	Grundlage und Ziel des Audits	490
14.4	Gegenstand des Audits	491
14.5	Leistungen des Auditors	491
14.6	Unabhängigkeit, Qualifikation und Zulassung des Auditors	491
14.7	Mitwirkungspflicht des Auftraggebers	492
14.8	Auditplan	493
14.9	Abschlussbesprechung	494
14.10	Abnahme und Mängel	494
14.11	Leistungen des Auftragsverarbeiters	495
14.12	Vertraulichkeit	495
14.13	Datenschutz	496
14.14	Gewährleistung und Verzug	496
14.15	Haftungsbeschränkung	496
14.16	Versicherung	497
14.17	Vertragsdauer und Kündigung	497
14.18	Schlussbestimmungen	498
15	Fazit	499
15.1	Regelungsrahmen	499
15.2	Aussagekraft	501
15.3	Nutzen	501
15.4	Bisherige Modelle	502
15.5	Empfehlung	503
	Literaturverzeichnis	507



## Abkürzungsverzeichnis

a. F.	alte Fassung
AaaS	Anything as a Service
ABL.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AiB	Arbeitsrecht im Betrieb (Zeitschrift)
AktG	Aktiengesetz
Alt.	Alternative
AnwBl	Anwaltsblatt (Zeitschrift)
AO	Abgabenordnung
AöR	Archiv des öffentlichen Rechts (Zeitschrift)
APPI	Act on the Protection of Personal Information
Art.	Artikel
AVV-EnEff	Allgemeine Verwaltungsvorschrift zur Beschaffung energieeffizienter Produkte und Dienstleistungen
AZRG	Ausländerzentralregistergesetz
B2C	Business-to-Consumer
BAG	Bundesarbeitsgericht
BauR	Baurecht (Zeitschrift)
BB	Betriebs-Berater (Zeitschrift)
BBB	Council of Better Business Bureaus
BbgDSG	Brandenburgisches Datenschutzgesetz
BC	Zeitschrift für Bilanzierung, Rechnungswesen und Controlling (Zeitschrift)
BDSG	Bundesdatenschutzgesetz
BeckRS	Beck-Rechtsprechung (Online Rechtsprechungssammlung)
BetrVG	Betriebsverfassungsgesetz

*Abkürzungsverzeichnis*

BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen (Entscheidungssammlung)
BImSchG	Bundes-Immissionsschutzgesetz
BImSchV	Bundes-Immissionsschutzverordnung
Biokraft-NachV	Biokraftstoff-Nachhaltigkeitsverordnung
BioSt-NachV	Biomassestrom-Nachhaltigkeitsverordnung
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BPersVG	Bundespersönlichkeitsvertretungsgesetz
BremDSAuditV	Bremische Datenschutzauditverordnung
BremDSG	Bremisches Datenschutzgesetz
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BT-Sten. Ber.	Stenografische Berichte über die Sitzungen des Deutschen Bundestages
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (Entscheidungssammlung)
BYOD	Bring your own device
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
CF	Computer-Fachwissen (Zeitschrift)
ChemKlimaschutzV	Chemikalien-Klimaschutzverordnung



COBIT	Control Objectives for Information and Related Technology
CR	Computer und Recht (Zeitschrift)
CuA	Computer und Arbeit (Zeitschrift)
DAkkS	Deutsche Akkreditierungsstelle
DANA	Datenschutznachrichten (Zeitschrift)
DB	Der Betrieb (Zeitschrift)
De-MailG	De-Mail-Gesetz
DepV	Deponieverordnung
DEV	Datenerhebungsverordnung
DIHK	Deutscher Industrie- und Handelskammertag
DIIR	Deutsches Institut für Interne Revision e. V.
DIN	Deutsches Institut für Normung
DJT	Deutscher Juristentag
DoS	Denial of Service
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSB	Datenschutz-Berater (Zeitschrift)
DSBK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DSK	Datenschutzkonferenz
DS-GVO	EU Datenschutz-Grundverordnung
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DSG-EKD	Datenschutzgesetz der Evangelischen Kirche in Deutschland
DSGSVO	Datenschutzgütesiegelverordnung
DSRITB	Deutsche Stiftung für Recht und Informatik (Zeitschrift)
DStR	Deutsches Steuerrecht (Zeitschrift)
DSZ	DSZ Datenschutz Zertifizierungsgesellschaft mbH
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl	Deutsches Verwaltungsblatt
e. G.	eingetragene Genossenschaft

*Abkürzungsverzeichnis*

e. K.	eingetragener Kaufmann
e. V.	eingetragener Verein
EaaS	Everything as a Service
EDPS	European Data Protection Supervisor
EEG	Erneuerbare-Energien-Gesetz
EfbV	Entsorgungsfachbetriebsverordnung
EG	Europäische Gemeinschaft
EG-UAVO	Europäische Verordnung über die freiwillige Beteiligung gewerblicher Unternehmen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung
Einf v	Einführung vor
EMAS	Eco Management and Audit Scheme
EMASPrivilegV	EMAS-Privilegierungs-Verordnung
EN	Europäische Norm
EnergieStG	Energiesteuergesetz
ERFA-Kreise	Erfahrungsaustauschkreise
ErwGr	Erwägungsgrund
EU	Europäische Union
EU-UAVO	Europäische Umwelt-Audit-Verordnung
EuGH	Europäischer Gerichtshof
EuroPriSe	European Privacy Seal
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
EVPG	Energieverbrauchsrelevante-Produkte-Gesetz
EWGV	Vertrag über die Europäische Wirtschaftsgemeinschaft
f.	folgend
ff.	folgende
GABl.	Gemeinsames Amtsblatt des Innenministeriums, des Finanzministeriums, des Wirtschaftsministeriums, des Ministeriums Ländlicher Raum, des Sozialministeriums, des Ministeriums für Umwelt und Verkehr sowie der Regierungspräsidien des Landes Baden-Württemberg
GDD	Gesellschaft für Datenschutz und Datensicherheit (GDD) e. V.

GeschGehG	Geschäftsgeheimnissegesetz
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
GRC	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
HansOLG	Hanseatisches Oberlandesgericht
HDSA-SH	Ausführungsbestimmungen für das Datenschutz-Audit-Verfahren Schleswig Holstein
HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
i. V. m.	in Verbindung mit
IaaS	Infrastructure as a Service
IEC	Internationale Elektrotechnische Kommission
IMI	Internal Market Information System
INPOL	Informationssystem der Polizei
ISO	Internationale Organisation für Normung
IuKDG	Informations- und Kommunikationsdienste-Gesetz
IZÜV	Industriekläranlagen-Zulassungs- und Überwachungsverordnung
JDCA	Japan Data Communication Association
JIPDEC	Japanese Information Processing Development Center
JZ	Juristen Zeitung (Zeitschrift)
K&R	Kommunikation & Recht (Zeitschrift)
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern
KDO	Kirchliche Datenschutzordnung
KG	Kommanditgesellschaft
KMU	Kleines oder mittleres Unternehmen

*Abkürzungsverzeichnis*

KunstUrhG	Kunsturhebergesetz
KrWG	Kreislaufwirtschaftsgesetz
KWG	Kreditwesengesetz
LDSG	Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen
LG	Landgericht
lit.	Buchstabe
MedR	Medizinrecht (Zeitschrift)
MDStV	Mediendienste-Staatsvertrag
MITI	Japanisches Ministerium für Handel und Industrie
MMR	Multimedia und Recht (Zeitschrift)
MPT	Myanma Posts and Telecommunications
NachwV	Nachweisverordnung
NDSG	Niedersächsisches Datenschutzgesetz
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	NJW-Rechtsprechungs-Report Zivilrecht (Zeitschrift)
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NuR	Natur und Recht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
o. Ä.	oder Ähnliches
OHG	Offene Handelsgesellschaft
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PaaS	Platform as a Service
PAuswG	Personalausweisgesetz
PDA	Personal Digital Assistant
QM	Qualitätsmanagement
QZ	Qualität und Zuverlässigkeit (Zeitschrift)
RAID	Redundant Array of Independent DisksRdA Recht der Arbeit (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RFID	Radio Frequency Identification

Rn.	Randnummer
S.	Seite
SaaS	Software as a Service
SDM	Standard-Datenschutzmodell
SGB X	Sozialgesetzbuch Zehn
SIS	Schengener Informationssystem
StGB	Strafgesetzbuch
StromStG	Stromsteuergesetz
TCDP	Trusted Cloud-Datenschutzprofil für Cloud-Dienste
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TÜV	Technischer Überwachungsverein
u. a.	unter anderen
u. U.	unter Umständen
UAG	Umweltauditgesetz
UAGZVV	Umweltauditgesetz- Zulassungsverfahrensverordnung
udis	Ulmer Akademie für Datenschutz und IT-Sicherheit
UGA	Umweltgutachterausschuss
UGB-KomE	Entwurf der Unabhängigen Sachverständigenkommission zum Umweltgesetzbuch beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
UPR	Umwelt- und Planungsrecht (Zeitschrift)
USA	Vereinigte Staaten von Amerika
UWF	UmweltWirtschaftsForum (Zeitschrift)
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vor
VerwArch	Verwaltungsarchiv (Zeitschrift)
VDSZ	Verordnung über die Datenschutzzertifizierungen
VG	Verwaltungsgericht
vgl.	vergleiche
VIS	Visa-Informationssystem
VMI	Verband der Metallindustrie Baden-Württemberg
Vorb.	Vorbemerkungen

*Abkürzungsverzeichnis*

VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
vzbv	Verbraucherzentrale Bundesverband
WHG	Wasserhaushaltsgesetz
WP	Working Paper
XaaS	Anything as a Service / Everything as a Service
z. B.	zum Beispiel
ZAU	Zeitschrift für angewandte Umweltforschung (Zeitschrift)
ZD	Zeitschrift für Datenschutz (Zeitschrift)
Ziff.	Ziffer
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)
ZUM	Zeitschrift für Urheber- und Medienrecht (Zeitschrift)
ZUR	Zeitschrift für Umweltrecht (Zeitschrift)