Martin Rost

Das Standard-Datenschutzmodell (SDM)

Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele

Springer Vieweg

Das Standard-Datenschutzmodell (SDM)

Martin Rost

Das Standard-Datenschutzmodell (SDM)

Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele

Springer Vieweg

Martin Rost
Langwedel, Schleswig-Holstein, Deutschland

ISBN 978-3-658-38879-9 ISBN 978-3-658-38880-5 (eBook)
https://doi.org/10.1007/978-3-658-38880-5

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

Planung/Lektorat: David Imgrund
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Inhaltsverzeichnis

1 Vorwort 1

2 Einleitung, oder: Wozu Datenschutz? 7
Literatur 15

3 Überblick zu den Inhalten dieses Buches 17

4 Verarbeitung 25
4.1 Was ist eine Verarbeitung? 27
4.2 Zweck 28
4.3 Ebenen der Verarbeitung 30
4.4 Komponenten einer Verarbeitung 38
4.5 Vertiefende Erläuterungen 40
4.5.1 Verarbeitungsvorgänge 40
4.5.2 Typen personenbeziehbarer Daten 44
4.6 Zwischenstand: Verarbeitung 45
Literatur 46

5 Recht 47
5.1 Anforderungen der DSGVO an die Praxis 49
5.2 Essentials 51
5.3 Vertiefende Erläuterungen 65
5.3.1 EU-Grundrechtecharta und Grundrechte 66
5.3.2 Artikel und Erwägungsgründe 70
5.3.3 Verhältnismäßigkeitsprüfung 71
5.3.4 Formen des Entscheidens 73
5.4 Zwischenstand: Recht 75
Literatur 76

6 Gewährleistungsziele 79
6.1 Normatives Gravitätszentrum 80
6.2 Grundsätze und Gewährleistungsziele 85

6.3 Vertiefende Erläuterungen . . . 87
6.3.1 Eine kurze Geschichte des SDM . . . 87
6.3.2 Gewährleistungsziele sichten . . . 94
6.3.3 Systematik der Gewährleistungsziele . . . 101
6.4 Zwischenstand: Gewährleistungsziele . . . 105
Literatur . . . 105

7 Datenschutzrisiken . . . 107
7.1 Risiken identifizieren . . . 108
7.2 Schwellwertanalyse . . . 110
7.3 Risikotypen . . . 113
7.4 Risikostufe, Schutzbedarf, Schutzniveau . . . 115
7.5 Vertiefende Erläuterungen . . . 117
7.5.1 Angreifer, Motive und Ressourcen . . . 118
7.5.2 Schadenshöhe = Risiko/Eintrittswahrscheinlichkeit . . . 120
7.6 Zwischenstand: Datenschutzrisiken . . . 123
Literatur . . . 124

8 Technisch-organisatorische Maßnahmen . . . 125
8.1 Generische TO-Maßnahmen und Bausteine . . . 126
8.2 Gewährleistungsziele erreichen . . . 130
8.3 Maßnahmen für hohes Risiko . . . 152
8.4 MUSS oder SOLL oder SOLLTE? . . . 153
8.5 Zwischenstand: Technisch-organisatorische Maßnahmen . . . 155
Literatur . . . 156

9 SDM anwenden . . . 157
9.1 Datenschutz modellieren: Der SDM-Würfel . . . 158
9.2 Datenschutz prüfen . . . 163
9.3 Datenschutzfolgen abschätzen . . . 169
9.4 Datenschutz managen . . . 175
9.5 Zwischenstand: SDM anwenden . . . 184
Literatur . . . 185

10 Kontext . . . 187
10.1 SDM und IT-Grundschutz . . . 188
10.2 SDM und ISO/IEC 27701:2019 . . . 193
10.3 SDM und ITIL . . . 194
10.4 SDM und Zertifizieren . . . 197
10.5 SDM und KDM . . . 199
10.6 Zwischenstand: SDM im Kontext . . . 199
Literatur . . . 200

11 Fazit 201
Literatur 203

12 Anhang 205
12.1 Dank 205
12.2 Betriebskonzept des SDM 207
12.3 Lösungen der Aufgaben 208
12.3.1 „Prüfen als Verarbeitung“ 209
12.3.2 „Verarbeitung nach IFSG“ 211
12.3.3 „Zweck eines Datenschutzmanagements“ 213

Stichwortverzeichnis 215

Abkürzungsverzeichnis

Abs.	Absatz
AK-Technik	Arbeitskreis „Technik“ der DSK
Art.	Artikel
AV	Auftragsverarbeitung oder Auftragsverarbeiter
BayLfD	Der Bayerische Landesbeauftragte für den Datenschutz
BBfDSuI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BDI	Bundesverband der Deutschen Industrie e. V.
BDSG	Bundesdatenschutzgesetz
BfD EKD	Der Beauftragte für den Datenschutz der evangelischen Kirche Deutschlands
BfDI	Der Datenschutzbeauftragte für den Datenschutz und die Informationssicherheit
BGM	Bundesministerium für Gesundheit
BI	Business Intelligence
BMI	Bundesministerium des Innern und für Heimat
BuED	Bildungs- und Entwicklungsdokumentation
BPM	Business-Process-Model
BSI	Bundesamt für Sicherheit in der Informationstechnik
BvD	Der Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CCC	Chaos Computer Club
CNIL	Commission Nationale de l’Informatique et des Libertés
CoBIT	Control Objectives for Information and Related Technology
CR	Change Request
CWA	Corona-Warn-App
DSA	Datenschutzaufsichtsbehörde
DSFA	Datenschutz-Folgenabschätzung

DSGVO	Datenschutz-Grundverordnung
DSA	Datenschutzaufsichtsbehörde
DSK	Unabhängige Datenschutzbehörden des Bundes und der Länder
DSM	Datenschutz-Management
DSMS	Datenschutz-Managementsystem
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EDBP	European Data Protection Board
EG	Erwägungsgrund
EuGh	Europäischer Gerichtshof
EU-GrCh	Grundrechtecharta der europäischen Union (EU)
FIfF	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GDPR	General Data Protection Regulation (deutsch: DSGVO)
ggfs.	gegebenenfalls
GZ	Gewährleistungsziele
IFSG	Infektionschutzgesetz
HBDI	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
HIIG	Alexander von Humboldt – Institut für Internet und Gesellschaft
HmbBfDI	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
IFSG	Infektionsschutzgesetz
ISB	Informationssicherheitsbeauftragte/r
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
ITGS	IT-Grundschutz des BSI
ITIL	Information Technology Infrastructure Library
IZG	Informationszugangsgesetz
JRL	Justizrichtlinie
KI	Künstliche Intelligenz
KPI	Key-Performance-Indicator
KRI	Key-Risc-Indicator
KRITIS	Kritische Infrastrukturen
LDI	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LfDI M-V	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
LfD NI	Die Landesbeauftragte für den Datenschutz Niedersachsen
LDSG	Landesdatenschutzgesetz
JRL	„Justizrichtlinie“, RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
KDM	Kirchen-Datenschutzmodell

KI	Künstliche Intelligenz
lit	Buchstabe
NGO	Non-Governmental-Organisation
OVG	Oberverwaltungsgericht
pbD	personenbezogene Daten
pbV	personenbezogenes Verfahren
PII	Personally Identifiable Information
PIMS	Datenschutzinformationsmanagementsystem
PIMS	Privacy Information Management System
PKI	Public-Key-Infrastructure
RKI	Robert-Koch-Institut
RZ	Rechenzentrum
SDM	Standard-Datenschutzmodell
SD	Sächsische Datenschutzbeauftragte
s. Abb.	siehe Abbildung
s. Kap.	siehe Kapitel
TOM	technisch-organisatorische Maßnahmen
TO-Maßnahme	technisch-organisatorische Maßnahme
TOMen	technisch-organisatorische Maßnahmen
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
UAGSDM	Unterarbeitsgruppe „Standard-Datenschutzmodell“ des AK-Technik der DSK
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
vgl.	vergleiche mit
VPN	Virtual Private Network

Vorwort

1

Was leistet das Standard-Datenschutzmodell?
Mit Hilfe des Standard-Datenschutzmodells (SDM) können, für personenbezogene Verarbeitungstätigkeiten in Organisationen, die normativen Anforderungen der DSGVO in funktionale Anforderungen transformiert werden.

Das ist die rhythmisch zwar immer noch holperige, aber inhaltlich beste bündige Erklärung zum SDM, die mir bislang eingefallen ist. Das SDM soll helfen, dass Jurist*innen auf der Ebene der IT-Technik nicht irgendwie dilletieren und dass Techniker*innen Sachverhalte nicht mit Hilfe von für Sie widersprüchlichen Regelwerken durchdringen, abwägen und beurteilen müssen. So fordert bspw. ein/e Jurist*in, personenbezogene Daten zu löschen, weil sie nicht mehr erforderlich sind. Juristisch ist damit alles Wesentliche gesagt. Daten dann tatsächlich aus der Welt zu schaffen ist anspruchsvoll; und der Nachweis darüber, dass diese Daten wirksam gelöscht wurden, macht den Vorgang kompliziert. Außerdem dürfen nur dazu befugte Mitarbeiter*innen etwas löschen und auf keinen Fall darf etwas Falsches gelöscht werden. Zuvor sollte geprüft worden sein, ob das verwendete Löschprogramm die Daten tatsächlich löscht oder nur den Zugang zu den Daten erschwert. Standardmäßig ist bekanntlich letzteres der Fall. Das Löschen von Daten meint dabei nicht zwingend gleich das Vernichten auch des Datenträgers. Müssen die Daten vernichtet werden oder reicht es, sie zu löschen, weil sie mit dem nächsten Schreibvorgang wahrscheinlich überschrieben werden? Wie sieht es aus mit den Daten in den mehrere Generationen umfassenden Backups, müssen auch die unverzüglich gelöscht werden? So, und diese Aktivitäten dienen nicht der Sicherung der Datenverarbeitung, sondern dem Schutz von Personen vor dieser Datenverarbeitung.

Die sachgerechte Entkoppelung des Fachwissens und die Integration in Bezug auf die konkrete Verarbeitung kann gelingen, wenn die beteiligten Expert*innen ihre Anforderungen mit den begrifflichen Mitteln des SDM auszudrücken verstehen. Sie müssen darauf vertrauen können, dass mit dem SDM eine allseitig zufriedenstellende Integration der Anforderungen und Aktivitäten gelingen kann. Denn genau dieses Zusammenwirken ist

M. Rost, *Das Standard-Datenschutzmodell (SDM)*,
https://doi.org/10.1007/978-3-658-38880-5_1

in der Datenschutzpraxis gefordert. Für diese Integration ist vor allem ein Verständnis der „Gewährleistungsziele“ notwendig: Jurist*innen im Datenschutz müssen bereit sein, Normen und Regeln als „Ziele“ zu rekonstruieren und zu kommunizieren; Techniker*innen im Datenschutz müssen bereit sein, „Ziele“ in Form von aufeinander abgestimmten Techniken zu verstehen und umzusetzen, bei denen nicht die Nützlichkeit von Funktionen, Kosten oder Sicherheit die allein entscheidenden Maßstäbe bilden. Und beide müssen bereit sein, ihre Aufmerksamkeit auf die Gestaltung bestimmter Eigenschaften von Verarbeitungstätigkeiten zu richten. Denn es sind die personenbezogenen *Verarbeitungen,* die im Zentrum der DSGVO stehen, nicht nur schützenswerte personenbezogene Daten.

Was leistet das SDM nicht?

Das SDM definiert nicht endgültig, welche Schutzmaßnahmen in welcher Ausprägung zur Umsetzung von Anforderungen der DSGVO zu treffen sind. Das SDM kann keinen Algorithmus zur endgültigen Wahl, Konfiguration und Dauerüberwachung von technisch-organisatorischen Maßnahmen anbieten, allenfalls ein Kalkül. Es liegt nicht am SDM, dass es das nicht leisten kann, aus zwei Gründen:

a) Operativer Datenschutz muss den Schutz der Rechte und Freiheiten von Personen auf Seiten der Organisationen und deren Verarbeitungen umsetzen; diese Anforderungen werden jedoch häufig nicht eindeutig interpretiert. Datenschutz ist einem starken politischen Konfliktfeld ausgesetzt, weshalb es mitunter Jahre dauern kann, bis für ein Detail eine Klärung bzw. ein Urteil herbeigeführt wurde, sei es durch eine Datenschutzaufsichtsbehörde (DSA) oder durch ein einfaches Gericht oder das Bundesverfassungsgericht (BVerfG) oder den europäischen Gerichtshof (EuGH). Man sieht allein anhand der aufgezählten Instanzen, dass es kompliziert werden kann. Wenn die Auslegung der Normen und Regeln nicht fix ist, können auch die darauf gegründeten Funktionen und Begründungen von Schutzmaßnahmen nicht fix sein.

b) Die im Datenschutz zu analysierende Menge an Risiken kann sehr groß werden. Dies hat zur Folge, das damit auch die Menge der zu treffenden Schutzmaßnahmen sehr groß werden kann. Es gibt keine operativ begründbare Regel zum Stoppen der Analyse von Datenschutzrisiken. Das SDM bietet eine Strategie zur integer kalkulierbaren Komplexitätsreduktion auf der Grundlage der Grundsätze aus Art. 5 DSGVO an. Am Ende aller datenschützerischen Aktivitäten steht immer ein rechtliches Urteil über die Intensität eines Grundrechtseingriffs einer Verarbeitung, inklusive der TO-Maßnahmen zu deren Risikominderungen. Vielleicht gibt es irgendwann einmal eine Datenschutz-Prüf-KI als Assistenz, die sehr viele Risikokonstellationen zu bearbeiten verspricht. Bis dahin bedarf es vertretbarer Strategien für eine verantwortbare, angemessen methodische und rechtliche Komplexitätsreduktion und einige kontrafaktische Fiktionen.

Für welche Leser*innen habe ich das Buch geschrieben?

Das Buch richtet sich selbstverständlich vor allem an *Datenschutzbeauftragte.* Sehr nützlich ist eine Befassung mit dem SDM darüber hinaus für *Projektmanager*innen,* die

Datenschutz-Folgenabschätzungen (DSFA) durchführen sowie Mitarbeiter*innen und Leiter*innen von Datenschutzabteilungen. Das SDM hilft, eine gemeinsame methodische Grundlage für interdisziplinäre Arbeit sowohl im Kontext von Datenschutzprüfungen, DSFAen als auch des Datenschutzmanagements zu bilden. Das Buch richtet sich deshalb ebenso an Spezialist*innen wie *Jurist*innen, Systemdesigner*innen, Informatiker*innen, Techniker*innen und Administrator*innen,* die Datenverarbeitungen maßgeblich gestalten. Interessant ist das SDM nicht zuletzt auch für *Generalist*innen,* wie bspw. *Verantwortliche, Journalist*innen* oder *Sozialwissenschaftler*innen,* die wissen wollen, was eine wirkungsvolle Datenschutzpraxis ausmacht.

Die Ausführungen in diesem Buch mache ich als Privatperson; sie geben meine persönlichen Einschätzungen, Urteile und Empfehlungen wieder.

Man sollte sich mit dem SDM vertraut machen, wenn man Datenschutz in Organisationen professionell prüfen und durchsetzen, Datenschutz-Folgenabschätzung durchführen und ein Datenschutzmanagement aufbauen muss, damit dies alles möglichst methodisch und effizient geschieht, um Kosten und unnötige Konflikte zu vermeiden. Eine ganze Reihe maßgeblicher Organisationen empfehlen das SDM genau deshalb für Prüfungen und Beratungen im Datenschutz.

Selbstverständlich verspreche ich nicht, dass ein wirksamer Datenschutz mit wenig Aufwand durch das SDM umsetzbar ist. Nein, vielmehr ist das Gegenteil der Fall: *Das SDM zeigt auf, welch unbestreitbar hoher Aufwand zu betreiben ist, um wirksamen Datenschutz gemäß DSGVO zu erreichen. Allerdings ist dieser Aufwand nicht größer, als wenn eine Organisation sich anhand von ISO-Standards oder mit ITIL (Information Technology Infrastructure Library) und CoBIT (Control Objectives for Information and Related Technology) strukturiert oder, speziell für die standardisierte Umsetzung der Informationssicherheit, den IT-Grundschutz (ITGS) des BSI einführt.*

Traditionell werden die Anforderungen des Datenschutzes von der Beratungsliteratur kleingeredet. Es reichte noch nie und es reicht weiterhin nicht, einige Vorlagen aus Formularsammlungen zu kopieren und diese auszufüllen, dann vielleicht noch ein „Verzeichnis der Verarbeitungstätigkeiten“ einzurichten (und zu glauben, damit seien die Dokumentationsanforderungen der DSGVO erfüllt) und am Ende einige Einwilligungserklärungen anzupassen, die aus dem Internet kopiert wurden. Das sind sinnlose, leerdrehende Aktivitäten. Auf dem gleichen Niveau befindet sich die Vorstellung, dass ein/e externe/r Datenschutzbeauftragte/r für 30 EUR – oder eine Mitarbeiterin oder ein Mitarbeiter mit einem Zeitbudget von 10 % im Monat – für eine kleine oder mittlere Organisation die Anforderungen der DSGVO umsetzen kann. Das kann selbstverständlich niemand, ob mit oder ohne SDM. Solche Situationen erzeugen zu Beginn gestresste und später dann lethargische Datenschutzbeauftragte, die nicht einmal die Aufgabenstellung umfassend verstehen, geschweige denn eine Strategie zu deren Bewältigung ausbilden können. Das muss einen DSB trotzdem nicht daran hindern, sich auf irgendetwas aus der DSGVO zu berufen und ganze Abteilungen lahmzulegen, was alles nicht geht. Viele betriebliche DSB sind schlecht ausgebildet, trotz der Zertifikate, die sie in der Regel vorweisen können. Den Leitungen der Organisationen ist all das recht. Die

Folge ist eine viele Jahre währende Tätigkeitssimulation im Bereich des Datenschutzes. Und auch die Organisationen leiden unnötig, denn vieles ist machbar, ohne dass deshalb Datenschutz vernachlässigt werden muss. Einiges an Verarbeitungen geht wiederum gar nicht, ganz gleich, was da rechtlich um den nicht-legitimen Zweck drumherum gestrickt wird. Vielleicht leiden Sie genau an einer solchen Situation?

Welche Lesepfade können durch das Buch sinnvoll eingeschlagen werden?
Ich habe das Buch für drei Nutzungsformen strukturiert: Typ „Schlendern", Typ „Intensiv" und Typ „Effizient".

Der Nutzungstyp *Schlendern* will einen entspannten Einblick in eine Datenschutzmethodik bzw. gezielt in das SDM bekommen. Mit diesem Interesse ist es sinnvoll, zunächst den Überblick im Kap. 3, die Einleitungen und jeweils die Zwischenfazite der Kapitel zu lesen, denn jedes Kapitel wird mit einem Überblick zum Inhalt eingeleitet und durch ein Zwischenfazit abgeschlossen, in dem die Hauptthesen des Kapitels zusammengestellt sind. Das ist, über das gesamte Buch gesehen, ein bisschen redundant, erlaubt aber ein abgerundetes Befassen zunächst nur mit einzelnen Themen und ein schnelles Wiederreinkommen zur Fortsetzung der Lektüre zu einem späteren Zeitpunkt.

Der Nutzungstyp *Intensiv* lässt sich unabhängig vom Vorwissen auf das Thema „Datenschutzmodellierung mit SDM" ein und nimmt sich vor, das Thema mit Hilfe des Buches intensiv zu bearbeiten. Diesem Nutzungstyp empfehle ich, das Buch einmal vollständig durchzulesen und dann noch einmal durchzuarbeiten: Im ersten Durchgang sollten die Kapitel vollständig zumindest bis zu den Kapiteln „Vertiefende Erläuterungen" gelesen werden. Dadurch entsteht ein Gesamtüberblick, so wie er sich durch eine gründliche Befassung mit den offiziellen Publikationen zum SDM bestenfalls einstellen könnte. Danach sollte es inklusive der vertiefenden Erläuterungen durchgearbeitet werden, mit ernsthaftem Bearbeiten der Aufgaben und jeder Menge an eigenen Notizen. Redundanz ist nicht zu vermeiden, sondern unverzichtbarer Bestandteil eines jeden Lernens. Der hermeneutische Zirkel besagt, dass man eigentlich nur das versteht, was man schon verstanden hat. Sie stellen erst beim zweiten Mal Lesen bzw. Bearbeiten des Buches fest, dass Sie bereits etwas verstanden haben. In den vertiefenden Erläuterungen finden sich Herleitungen, Hintergründe und Fortentwicklungen zur offiziellen Darstellung des SDM, die Sie in die Lage versetzen sollen, das SDM kreativ anzuwenden und vielleicht eigenständig weiterzuentwickeln. Ich wünsche mir natürlich genau diese Art von Intensivnutzung des Buches. Dann einige Monate später noch eine SDM-Schulung obendrauf, und Sie können sichergehen, fortan tatsächlich jedes Problem der Datenschutzpraxis methodisch in den Griff zu bekommen.

Der Leser oder die Leserin vom Nutzungstyp *Effizient* kennt das SDM schon, zumindest grob umrissen aus dem Methodik-Handbuch, und bringt Erfahrungen aus der Umsetzungspraxis mit. In diesem Falle kann es sinnvoll sein, vom Ende des Buches her das Wissen zu vertiefen. Konkret hieße das: Vorblättern zum SDM-Würfel im Abschn. 9.1, der das gesamte SDM in einer einzigen Grafik vereint. Und anschließend denken Sie dann erst einmal eigenständig längere Zeit über den Würfel und seine Möglichkeiten nach. Legen

Sie dafür das Buch schlicht zur Seite. Erfinden Sie den SDM-Würfel nach, verbessern Sie ihn, er soll nur eine Orientierungshilfe bieten. Ich weiß, dass viele SDM-Nutzer*innen primär an den SDM-Bausteinen bzw. technisch-organisatorischen Maßnahmen interessiert sind. Bei diesen Kolleg*innen beobachte ich häufig, zumindest wenn sie aus dem Bereich der IT-Sicherheit kommen und mit operativem Datenschutz kaum befasst waren, dass sie, aufgrund der Verwendung der gleichen Schutzmaßnahmen sowohl in der IT-Sicherheit als auch dem operativen Datenschutz, den Datenschutz als eine Fortsetzung der IT-Sicherheit begreifen. Und dann entsteht in der Regel die Idee, dass man doch IT-Sicherheit und operativen Datenschutz gleich zusammenbringen oder zusammen denken müsse. Dass da noch niemand drauf gekommen ist…Doch doch, da sind schon Anwender*innen drauf gekommen! Eigentlich jede/r, weil trivial. Es gilt, die beiden Disziplinen „operativer Datenschutz“ und „Informationssicherheit“ erst einmal klar von einander zu unterscheiden, bevor man sich anschließend daran machen kann, sie in eine überwiegende Win-Win-Beziehung zu bekommen. Nicht nur echten Datenschützer*innen, auch den methodisch wirklich gut ausgebildeten IT-Grundschutz-Auditoren und den Entwicklern im BSI ist diese Unterscheidung erfahrungsgemäß wichtig. Bei anderen Interessenten an diesem Buch könnte die Durchführungen einer Schwellwertanalyse oder einer DSFA (Abschn. 9.3) drücken. Oder es steht die Erarbeitung des „Verzeichnisses der Verarbeitungstätigkeiten“ (Art. 30 DSGVO) an und man sucht ganz spezifisch nach Informationen zur Dokumentation von Verarbeitungen (s. Kap. 4) und technisch-organisatorischen Maßnahmen (s. Kap. 8).

Das SDM mit Hilfe dieses Buches anwenden zu lernen, wird sich über Monate ziehen. Dafür einmal das Buch durchzulesen wird nicht reichen. Ich habe Folien von SDM-Dozenten (nur Männer!) gesehen, die offenbaren, dass sie das SDM-Methodik-Handbuch nicht auch nur ein einziges Mal bis zum Ende gelesen haben. Wie bei jedem anderen Handwerk oder jeder anderen anspruchsvollen Dienstleistung dauert es, bis man mit einer Methode Laufen lernt und es anfängt, Spaß zu machen, weil man weiß, was man wann in welcher Reihenfolge mit welchen Gründen macht oder nicht macht. Und wo mit guten Gründen die vernachlässigbar erscheinenden kleinen Unterschiede zu den benachbarten Methoden liegen. Ja, Datenschutz kann sogar richtig viel Spaß machen. Ein kluger Kollege, von dem ich viel lernen durfte, meinte anlässlich einer Kaffeepause, dass ihm auf der Hinfahrt zur Konferenz klar geworden sei, dass er wohl zehn lange Jahre gebraucht habe, bis er Datenschutz konnte. Zehn Jahre! Dass es so lange gedauert hätte, habe ihn nicht gerade fröhlich gestimmt, schließlich ließe das an seiner Intelligenz zweifeln. Denn eigentlich dürfe man erwarten, jeden Job spätestens nach drei Jahren ausüben zu können. Ich stimmte sofort zu, ich hatte wohl ebenso lange gebraucht. Zehn Jahre, nicht zehn Wochen, bei hohem Engagement und in einer anregenden Umgebung. Auch wenn man drei Minuten nach der frischen Bestellung als DSB bereits relevante Effekte auslösen kann: „Ok, dann fange ich mal an: Wo ist bitte die Rechtsgrundlage für diese Verarbeitung?“ Und „Kann ich bitte eine Aufstellung aller Verarbeitungen bekommen?“ Darin erschöpft sich Datenschutz nicht. Diese Fragen bieten einen guten Einstieg, und sind doch kaum mehr als ein Strohfeuer. Wie geht es anschließend weiter? Eine Übersicht der Verarbeitungstätigkeiten nach Art. 30 DSGVO und die

dazugehörigen Rechtsgrundlagen nach Art. 6 DSGVO allein erzeugen noch keinen Schutz vor den möglicherweise zu intensiven Zugriffen einer Organisation auf deren Bürger*innen, Kund*innen oder Patient*innen. Also: Wie macht man echten Datenschutz?

Mein Ehrgeiz ist, Ihre Lehrzeit für die Umsetzung von Datenschutzanforderungen mit Hilfe des SDM drastisch zu verkürzen.

Einleitung, oder: Wozu Datenschutz?

2

Das Standard-Datenschutzmodell (SDM) ist mit seinen wenigen Komponenten leicht zu verstehen. Es sollte Sie nicht wundern, wenn Sie sich am Ende der Lektüre fragen: Soll das jetzt schon alles gewesen sein? Es sah doch erst alles so kompliziert aus? Datenschutz mit Logik ist möglich. Voraussetzung für Logik ist eine klare Vorstellung vom Zweck des Datenschutzes und dass man Datenschutz nicht mit Datenschutzrecht gleichsetzt, so wie man Umweltschutz ja auch nicht mit Umweltschutzrecht verwechselt. Was „Datenschutz" meint und welchen Zweck operativer Datenschutz verfolgt, muss man erst einmal klarstellen; doch ein Wissen darum darf man nicht einmal Profis unterstellen. Das war mal anders.

In den Anfangsjahren war der Zweck des Datenschutzes nicht nur den Spezialist*innen, sondern ebenso den politisch gebildeten Bürger*innen klar. Das Volkszählungsurteil von 1983 wurde breit diskutiert unter dem Aspekt des Zugriffs eines übermächtig werdenden Staates auf sämtliche Daten der Bürger*innen. Diese Klarheit des Bezug auf die Bedeutung von Macht zur Gestaltung von Informationsverarbeitungen umfasst auch private Organisationen, aber sie hat sich verflüchtigt. Zwar nimmt seit dem Jahrtausendwechsel der Skandalisierungsdiskurs zum Datenschutz zu. Einige Skandale erreichten inzwischen sogar den Status eines größten anzunehmenden Unfalls (GAU) – für mich zählten die Offenbarungen Edward Snowdens 2013 zu den weltweiten Überwachungs- und Spionagepraktiken der Geheimdienste zu einem Super-GAU –, mit exakt keinerlei Folgen. Die inzwischen nahezu omnipräsenten Meldungen zu Grundrechtsverstößen halten ersichtlich die „Erosion des Datenschutzes" (Simitis 1999) nicht auf, im Gegenteil: Man hat sich achselzuckend allseits eingerichtet. Es fehlen ernsthafte Analysen und konsequente Strategien gegen diese Erosion. Das SDM will, aus einer gefestigten Analyse heraus, einen ernsthaften Beitrag zur wirksamen Umsetzung von Datenschutz leisten. Eine moderne Gesellschaft kann vom Datenschutz als Operationalisierung der Grundrechte nicht lassen; Datenschutz ist DER Indikator für die Moderne einer modernen Gesellschaft. Der Zusammenhang von Datenschutz und Gesellschaft ist schlicht: Werden Grundrechte nicht geachtet, regrediert die Moderne. Datenschutz wird beschworen wie vielleicht noch nie in der Geschichte der Menschheit, aber durch die

M. Rost, *Das Standard-Datenschutzmodell (SDM)*,
https://doi.org/10.1007/978-3-658-38880-5_2

Organisationen nicht ernsthaft umgesetzt. So wenig wie der Naturschutz. Ich werde auf diesen Aspekt immer mal wieder knapp zu sprechen kommen.

Was bezeichnet „Datenschutz“?

Datenschutz gibt es nicht, weil es die Datenschutzgrundverordnung („DSGVO“) gibt. Und die DSGVO gibt es nicht, weil man sich seit 2010 daran machte, die nationalen Datenschutzgesetz EU-weit zu vereinheitlichen. Der Sinn und Zweck von Datenschutz gründet zudem nicht in bloßen Meinungen zu Privatheit, die mal so oder auch mal ganz anders ausfallen können. Stattdessen steht Datenschutz für eine präzise definierbare Konfliktkonstellation in modernen Gesellschaften, denen das Datenschutzrecht eine erwartbare Form des Umgangs mit ihnen gibt. So wie Diebstahl eine genau definierbare Konfliktkonstellation ist, die im Strafgesetzbuch geregelt wird. Datenschutzkonflikte bestehen strukturell, d. h. sie kehren erwartbar immer wieder, ohne dass diese durch das Recht endgültig dauerhaft aufgelöst und aus der Welt geschafft werden können, selbst wenn sich alle Menschen entschlössen, gut zu handeln.

Welchen Konflikt bearbeitet das Datenschutzrecht? Die Lektüre der DSGVO allein hilft dabei wenig, dem Datenschutzkonflikt auf die Spur zu kommen. Viele Jurist*innen im Datenschutz kennen „Datenschutz“ nur aus dem Datenschutzrecht, sie setzen die soziale Konstitution des Datenschutzkonflikts mit dem Datenschutzrecht gleich: Weil es das Datenschutzrecht gibt, gibt es für sie Datenschutz. Das ist vergleichbar der Vorstellung, dass das Umweltschutzrecht bestimmt, was die Umwelt ist. Dabei wird das Umweltschutzrecht erst verständlich mit einem Vorverständnis für Natur und Umwelt. Genau ein solches, am besten theoretisch kontrolliertes, Vorverständnis ist auch im Datenschutz unerlässlich. Im Unterschied zum Datenschutz ist Umweltschutz dabei immerhin intuitiv zugänglich. Vorstellungen zum Datenschutz, die vielleicht sogar als intuitiv zugänglich gelten mögen – bspw. Schutz einer betroffenen Person, Schutz der personenbezogenen Daten, Schutz der Privatheit oder abstrakter „Schutz der informationellen Selbstbestimmung“ –, treffen dabei aber nicht hinreichend genau den wesentlichen Konflikt des Datenschutzes.

Bitte legen Sie das Buch beiseite und beantworten Sie diese beiden Fragen für sich: Was meint „Datenschutz“? Und: Welcher Konflikt wird durch das Datenschutzrecht geformt und bearbeitet?

(...)

Und? Hatten Sie das Buch beiseite gelegt und über diese beiden Fragen nachgedacht? Sind Sie der Überzeugung, dass Sie durch genügendes Nachdenken gehaltvolle Antworten gefunden haben? Oder stellen Sie gerade fest, dass Ihnen dazu nicht allzuviel einfällt? Und Sie deshalb einfach mal weiter lesen?

Wollen Sie das Buch nicht vielleicht wirklich zumindest kurz beiseite legen und über den zentralen Datenschutzkonflikt nachdenken?

Selbst wenn man zu Datenschutz bereits eine starke, fokussierte Vorstellung entwickelt hat ... Datenschutz in die Praxis zu bringen, bleibt ein überaus schwieriges Geschäft. Datenschutz bedeutet in jedem Falle Aufwand und kostet Geld, ohne dass sich für denjenigen, der

für die Datenschutzmaßnahmen zahlen muss, nämlich für den Verantwortlichen, ein Nutzen abzeichnet. Da ist der Nutzen der zunehmend teurer werdenden Auflagen des Umweltschutzrechts – man denke an die Anforderungen des Energiemanagements von Gebäuden oder an die Anforderungen der GreenIT – ungleich leichter als der des Datenschutzes zu verstehen.

Denken Sie noch über Datenschutz nach? Haben Sie eine klare Vorstellung davon, was als Grundrechte bezeichnet wird? Könnten Sie mit ihrer Vorstellung den Nutzen von Datenschutz einem Kritiker oder einer Kritikerin des Datenschutzes, der oder die gar keinen Nutzen im Datenschutz sehen WILL, erklären? Das ist die typische Situation, die für eine(n) DSB in der Praxis der Normalfall ist. Welche Funktion hat die Datenschutzaufsicht, sei es als organisationsinterne DSB oder als Datenschutzaufsichtsbehörde?

...

Meine Erklärungen zum Datenschutz, zum Datenschutzrecht und zur Datenschutzkontrolle lauten wie folgt: *Organisationen in modernen Gesellschaften sind latent motiviert, und in der Regel auch in der Lage, die Grundrechte von Personen nicht wirksam zu beachten. Die Funktion des Datenschutzes besteht deshalb darin, Personen vor latent übergriffigen Organisationen zu schützen. Die Funktion des Datenschutzrechts besteht darin, die Machtasymmetrie beim Zugriff von Organisationen auf Personen unter normative Bedingungen zu stellen. Die Funktion der organisationsinternen Datenschutzbeauftragten und der Datenschutzaufsichtsbehörden besteht darin zu beobachten, zu kontrollieren, zu prüfen und zu beurteilen sowie darauf hinzuwirken, dass Organisationen sich mit ihren Verarbeitungstätigkeiten an die datenschutzrechtlichen Normen und Regeln halten.*

Wenn Organisationen gegenüber Personen fair agieren, dann kann Privatheit, was auch immer damit gemeint ist, entstehen (vgl. Solove 2006; Zimmermann 2014; Matzner und Ochs 2019). Es besteht dann eine Chance, so die gängige Vorstellung, auf die Ausbildung einer „informationellen Selbstbestimmung“ der Personen. Diese Wendung scheint durch eine klare Vorstellung gedeckt, sie geht vielen Datenschützer*innen zumindest locker über die Lippen. „Informationelle Selbstbestimmung“ ist psychologisch oder soziologisch jedoch eine rätselhafte Vorstellung, die mit empirischen Ansprüchen an eine Deckung des Gesagten schlichter Unsinn ist. Kommunikationstheoretisch betrachtet funktioniert diese Wendung jedoch als Beschwörungsformel, mit der weitere Nachfragen gestoppt werden. Die Privacy-Forschung wechselt an dieser Stelle gern unter der Hand das Thema und beleuchtet stattdessen den Wandel der „Subjektivierungen“ im Kontext der Digitalisierung der „Kommunikationsverhältnisse“ oder „Arbeitsformen“ (vgl. Friedewald 2018). Erfunden wurde diese griffige Formel der informationellen Selbstbestimmung von Wilhelm Steinmüller im Kontext des weltweit ersten Datenschutzgutachtens. Es handelte sich mehr um eine fixe Marketingidee als um ein durchdachtes Konzept (vgl. Rost und Krasemann 2008).

Klar und empirisch zugänglich kann man dagegen folgendes sagen: Wenn Organisationen fair gegenüber Personen agieren, dann haben die Personen ihren praktischen Nutzen dadurch, dass Organisationen sie in Ruhe lassen. Das ist der Nutzen von Datenschutz für Personen: Datenschutz hält Organisationen gegenüber Personen auf Distanz. Datenschutz

ist die Praxis, die helfen soll, dass Organisationen in modernen Gesellschaften ihren Machtvorteil bei der Gestaltung der Beziehungen nicht (bedingungslos) ausspielen können. Und wenn Organisationen mit Menschen interagieren, dann wachen Datenschützer*innen darüber, dass die edelsten Versprechen des Grundgesetzes und der EU-Grundrechtecharta in der Praxis tatsächlich wirksam eingelöst werden. Deren Versprechen lautet schließlich, dass die Würde des Menschen und dessen Freiheit nicht angetastet werden sollen. Die Passage im Grundgesetz ist dabei interessanterweise weder als ein Versprechen noch als eine Forderung formuliert, was man zunächst erwarten würde, sondern als Behauptung: „Die Würde des Menschen ist unantastbar." Diese Formulierung löst mit einem Blick auf die Praxis zwar sofort großen Zweifel aus, besagt aber, dass die Würde auch nicht durch das Recht „angetastet werden kann"; sie ist selbst noch dem Zugriff durch das Recht entzogen, das sie schützen soll (vgl. Bock und Engeler 2016). Ein derartiger Satz lässt sich ganz leicht als Floskel abtun. Oder aber man interpretiert ihn im Gegenteil als eine einklagbare Zusage an Menschen und eine Anweisung an mächtige Organisationen, vorsichtig mit Menschen umzugehen. Datenschutz wäre in diesem Sinne ein sozialer Naturschutz, wobei die Evolution auf das Zutun der Menschen angewiesen ist.

Die Umsetzung von Datenschutz gelingt nicht, wenn die Aktivitäten von Organisationen nur ethisch reflektiert werden, anstatt diese anhand der EU-Grundrechtecharta, des Grundgesetzes, der DSGVO und der Methoden zur Bearbeitung der Datenschutzkonflikte wirksam zu bearbeiten und einzugrenzen. Datenschutzkonflikte mit ethischen Reflexionen zu bearbeiten ist in der Regel ein Ausweichmanöver, das den Interessen der Organisationen nützt und die Stellung, vermutlich entgegen den Intentionen der meisten Ethiker*innen, von Personen schwächt (vgl. am Beispiel der Corona-Warn-App diskutiert Rehak 2022). Dies zeigt sich besonders deutlich im Kontext von Automaten mit „künstlicher Intelligenz", bei denen es – entgegen dem langsam abklingenden leichten Grusel in manchen Feuilletons, die den smarten Automaten zu Beginn des fünften Hypezyklus sogar Subjektqualitäten andichteten – gar keine sonderlichen Probleme bereitet, diese DSGVO-konform zu gestalten und zu betreiben (vgl. AK-Technik 2019).

Die Staaten des EU-Lands helfen ihren Bürger*innen, dass diese sich, mit Bezug auf die DSGVO, vor übergriffigen Aktivitäten von Organisationen schützen können. Die Staaten helfen dabei ein bisschen, so im Grundsätzlichen. Sagen wir klar, wie es ist: Diese staatliche Hilfe beim Schutz vor dem Staat und vor anderen mächtigen Organisationen geschieht real auf einem bestenfalls niedrigen Niveau. Gegen die Aktivitäten von Google, Amazon, Facebook, Apple, Microsoft, um nur die größten und aggressivsten Unternehmen bei der Verwertung personenbezogener Daten zu nennen, werden die Personen, die deren Dienste nutzen (inzwischen: teilweise müssen) – und nicht zu vergessen auch die Personen, die diese nicht nutzen, aber trotzdem betroffen sind, wenn sie das Internet nutzen –, weitgehend allein gelassen. Ebenso wie gegenüber den Aktivitäten der Nachrichtendienste, insbesondere der ausländischen (vgl. Roßnagel et al. 2022). Bedrückenderweise bleibt es einzelnen Aktivist*innen, wie der inzwischen vergessenen Chelsea Manning, dem fast vergessenen Julian Assange oder dem noch etwas präsenteren Edward Snowden und Max Schrems im Helden-

modus überlassen, dass überhaupt etwas von Relevanz in Richtung Zurückweisung übergriffiger Aktivitäten durch staatliche Behörden und mächtige Privatunternehmen geschieht. Eigentlich wären moderne Gesellschaften, wären sie tatsächlich modern, nicht mehr auf Helden angewiesen (zur aktuell erstaunlich großen Zahl insbesondere an Heldinnen vgl. Leister 2020).

Das grundrechtlich gegebene Versprechen einzulösen, dass Menschen gegen unfair agierende Organisationen durch professionelle Datenschützer*innen geholfen wird, verlangt von Datenschützer*innen Parteinahme zugunsten der Menschen und zuungunsten der Organisationen. Etwa in der Form und dem Umfang, mit denen Umweltschützer*innen Partei für die Natur und gegen die umweltbelastenden Organisationen nehmen. Datenschützer*innen müssen Partei ergreifen zum Ausgleich dafür, dass die gesellschaftlichen Verhältnisse bereits Partei für die Organisationen genommen haben: Es sind die Organisationen, die mit ihren Datenverarbeitungen und deren Inhalten, Formen und Techniken die Ziele und die Mittel der Verarbeitung von Personendaten bestimmen. Und praktisch niemand stoppt sie, sich alles genau so hinzulegen, wie es von Vorteil für die Organisationen ist. Die davon betroffenen Personen können diese Verarbeitungen tatsächlich nur akzeptieren; die Einwilligung, die vielfach als Rechtsgrundlage herhalten soll, erzeugt dabei keine Schutzwirkungen vor unfairen Verarbeitungen. Vielmehr erwarten Organisationen mit der Einwilligung perfiderweise noch die Zustimmung der Menschen zu ihrer Unterwerfung, eben unter die Bedingungen der Organisationen. Es gibt viele vermeintliche Datenschützer*innen, die ausgerechnet in der Kapitulationserklärung „Einwilligung“ einen souveränen Akt der Willensausübung von Personen sehen. Wenn sich mit jedem neuen Webseitenaufruf Einwilligungs-Einblendungen reindrängen, dann erscheint Datenschutz nur noch als ein fragwürdiger Formalkram, als Datenschutzsimulation, weil vollständig sinnlos und ohne nennenswerte Schutzwirkung für die betroffenen Nutzer*innen. Niemand verklagt solche Webseitenbetreiber; Webseiten könnten, es ist ganz leicht, minimal invasiv präsentiert werden.

Datenschutzbeauftragte müssen somit entschieden als Anwält*innen der Interessen von Bürger*innen gegenüber Behörden, von Kund*innen gegenüber Unternehmen, von Patient*innen gegenüber Krankenhäusern, von Schüler*innen gegenüber Schulen und Kultusministerien, von Gefangenen gegen den Strafvollzug oder von Mitarbeiter*innen gegen Arbeitgeber auftreten. Wie gesagt: Das stand den Datenschützer*innen Ende der 1970er Jahre bis Anfang der 1990er Jahre vollkommen klar vor Augen; dieses Wissen oder diese Haltung ist nur noch selten anzutreffen. Ein solches Wissen und eine solche Haltung werden sogar als obsolet und veraltet geframt, mit Hinweisen auf die sich rasend schnell verändernden Techniken. Die Techniken mögen immer raffinierter und beeindruckender werden, aber die Konflikte haben mit digitalisierter Technik nichts zu tun. Technik materialisiert die Machtasymmetrie zwischen Organisationen und Personen und verstärkt die vorhandene Machtasymmetrie. Datenschutz ist in Wahrheit heute so nötig wie noch nie zuvor, damit die moderne Gesellschaft eine moderne Gesellschaft bleibt (oder erst noch wird?) und nicht in die stratifizierte Vormoderne zurückfällt, in der wenige Organisationen das gesamte Leben

der Menschen verwalteten, in den Grenzen, die die Organisationen den Menschen vorgaben (vgl. Pohle und Rost 2021).

Diese geforderte Parteinahme gegen Organisationen ist selbstverständlich keine gemütliche Aufgabe für Datenschutzbeauftragte, gleichgültig, ob sie als behördliche DSBe in Behörden und als betriebliche DSBe in Unternehmen oder in einer Datenschutzaufsichtsbehörde arbeiten. *Eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter, die oder der keinen Ärger macht oder keinen Ärger hat, erledigt ihren oder seinen Job nicht.* Ich wüsste keinen gültigeren Indikator für das Wirken eines(r) DSB. Sehr viele Datenschutzbeauftragte agieren mit der Vorstellung, dass Datenschutz bereits dann sichergestellt ist, wenn (irgend)eine Rechtsgrundlage vorliegt und wesentliche Maßnahmen der IT-Sicherheit ergriffen wurden. Das ist geschenkt, das allein reicht nicht im Hinblick auf Sicherung der Grundrechte von Personen. Die NGOs, die im Kontext Datenschutz agieren und die gesellschaftliche Kommunikationen mit dem notwendigen Ärger versorgen – ich denke da bspw. an die Humanistische Union (HU), an die Deutsche Vereinigung für Datenschutz (DVD), Netzwerk Datenschutzexpertise und insbesondere an die Aktivitäten des CCC mit Linus Neumann, Digitalcourage, FIfF, netzpolitik.org, bspw. allein mit ihren Aktivitäten zur Corona-Warn-App oder Luca-App, sowie an NOYB mit Max Schrems als Galionsfigur oder einzelne Aktivist*innen wie bspw. Dr. Patrick Breyer, Katharina Nocun oder Lilith Wittmann – scheinen mir ungleich konfliktbewusster und sogar in der Öffentlichkeit präsenter als die meisten Datenschutzaufsichtsbehörden zu sein. Selbst wenn sich Datenschutzaufsichtsbehörden in der Öffentlichkeit zurückhalten und vor allem nach Innen wirken, in vielen Fällen tun sie sich sogar auch noch schwerer mit technischen Prüfungen (vgl. Schulzki-Haddouti 2017). In welchem Ausmaß dann sogar sachfremde Eigenschaften die Bestellungen der Leitungen von Datenschutzaufsichtsbehörden, trotz der klaren Vorgaben der DSGVO, beeinflussen können, zeigt ein Gutachten des Netzwerk Datenschutzexpertise (vgl. Bernhardt et al. 2021, S. 12).

Aber auch echte Datenschützer*innen der NGOs sind auf eine gehaltvolle Datenschutztheorie, wirksame Methoden und Tools angewiesen, die dabei helfen, über „bloßes“ journalistisches Aufdecken, juristische Abwägungen und politische Aktivitäten hinauszukommen. Hinzukommt, dass auch Aktivist*innen nicht immer eine hinreichend fokussierte Vorstellung von Grundrechten haben. Operativer Datenschutz erschöpft sich nicht mit der Bereitstellung und Nutzung von OpenSource-Programmen, wirksamer Verschlüsselung und Anonymitätsservern.

Datenschutz wirksam umzusetzen – und das meint eigentlich immer: gegen Widerstand von Organisationen, die die Kosten dafür zu tragen haben, durchzusetzen – gelingt nicht durch Schulungen und Beratungen von Mitarbeiter*innen oder Bürger*innen oder Jugendlichen, die sich bspw. naiv der ganzen Welt auf Instagram präsentieren. Diese Personen sind, wie sie sind, nicht-festgestellt, das ist die Pointe des Humanismus. Menschen sind individuell, wenn auch als Massenphänomen, mit einem *Zwang zum Individuellsein* (vgl. Meuter 2002). Wir müssen witzig, intelligent, geistreich und alles in allem tolle Erscheinungen sein, elegant und tätowiert zugleich. Datenschutz stellt sich als Problem nicht durch die Analyse

von Menschen mit ihren Meinungen und Eigenschaften, sondern durch die Analyse der in Techniken gegossenen kommunikativen Aktivitäten der Organisationen gegenüber Personen. Die Verführungen für Organisationen, in der Praxis unfair zu agieren und zu versuchen, die Risiken des Marktes und des Rechtsstaates auf die Kund*innen und Bürger*innen abzuwälzen, sind dabei sehr groß.

Die Chancen der Organisationen, mit unfair gestalteten Prozessen personenbezogener Datenverarbeitungen ungeschoren davon zu kommen, stehen gut. Die Organisationen bestimmen über die Formen der Informationsverarbeitung und der Kommunikation mit den Menschen; sie sind bestrebt, den Umgang mit Menschen, allein aus Vereinfachungs- und Kostengründen, zu standardisieren und zu automatisieren. Dabei ist es mit der Würde des Menschen nicht vereinbar – darin stimmen übergreifend, über alle politischen Differenzen der Autor*innen hinweg, die Kommentare zum Grundgesetz überein –, wenn Menschen als Objekt behandelt werden. Datenschutzmaßnahmen, die mit der DSGVO begründet den Angriffen auf die Würde durch Organisationen etwas entgegensetzen, verursachen Kosten. Immer. Datenschutz muss deshalb den Verantwortlichen in den Organisationen abgetrotzt werden. Immer. Mehr denn je. Denn Organisationen befinden sich strukturell immer schon im Vorteil.

Den Verantwortlichen der Organisationen ist deren mehr oder weniger offene Widerstand gegen Datenschutz selbstverständlich nicht persönlich vorzuwerfen. Wobei es sich überwiegend gar nicht um Widerstand handelt – denn der setzte ein klares Verständnis von dem voraus, was nicht gewollt wird –, sondern ungleich mehr um Ignoranz. Die Konflikte, die im Kontext Datenschutz bearbeitet werden, sind struktureller, gesellschaftlicher Art. Man lasse sich bei Gelegenheit auf der nächsten Party mal von Soziolog*innen „Gesellschaft“ erklären, weil das mehr als nur „irgendwie viele Menschen“ und „Normen und Rituale“ meint. Soziolog*innen unterscheiden bspw. Interaktionssysteme von Organisationssystemen von Funktionssystemen, die sich „funktional differenziert“ reproduzieren (vgl. Luhmann 1997). Datenschutz ist nicht mit der Behandlung von individuellen Einzelinteressen und einzelnen Konflikten beizukommen. Auch Verantwortliche sind Bürger*innen, Kund*innen, Patient*innen, die von den Leistungen eines funktionierenden Datenschutzes profitieren. Die Ignoranz der Datenschutzanforderungen seitens der Organisationen ist insofern „normal“, sozio-logisch in der täglichen Arbeit einer oder eines DSB in Rechnung zu stellen und in der Form des Umgangs mit strukturellen Differenzen zu bearbeiten. Zumal die Leistungen der Organisationen – angefangen bei den Verwaltungen der Kommunen bis zu den großen Plattformen des Internet – grandios sind und auch von betroffenen Personen geschätzt werden. Niemand will auf die Leistungen von Unternehmen und Behörden verzichten. Wobei von „Wollen“ keine Rede sein kann: Die Leistungen von Organisationen sind unverzichtbar, sie halten uns Menschen am Leben und verhindern, dass eine Gesellschaft auseinanderfällt.

Organisationen greifen mit ihren personenbezogenen Verfahren in die Grundrechte und Grundfreiheiten von Personen ein. Immer. Es ist falsch, zu fordern, dass Organisationen nicht in Grundrechte eingreifen dürfen. Sie dürfen das. Es geht gar nicht anders. Aber es ist eine Frage angemessener Bedingungen, unter die die Eingriffe zu stellen sind. Dazu muss