Die DSGVO

Hinweise für kleine und mittlere Unternehmen

AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (Hg.)

AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (Hg.)

Die DSGVO

Hinweise für kleine und mittlere Unternehmen

Herausgeber
AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V.
www.awv-net.de | info@awv-net.de

Die Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. versteht sich als Netzwerk für Digitalisierung und Bürokratieentlastung. Sie ist ein bundesweites Forum, in dem Antworten auf aktuelle Fragen rund um die wirtschaftliche Gestaltung administrativer Prozesse entwickelt werden.

Verfasser der 2., aktualisierten Auflage
AWV-Arbeitskreis 4.3 „Datenschutz- und Informationssicherheit", mit folgenden Autorinnen und Autoren:
Dirk Erdmann, Köln
Dietmar Faude, Frickenhausen
Rudi Kramer, Nürnberg
(Leiter des AWV-Arbeitskreises 4.3)
Sebastian Meissner, Bonn
Yvette Reif, Bonn

Verfasser der 1. Auflage
AWV-Arbeitskreis 4.3 „Weiterentwicklung des Datenschutzrechts", mit folgenden Autorinnen und Autoren:
Dr. Bernd Beier, Stuttgart
Dirk Erdmann, Köln
Harald Eul, Brühl
Dr. Wulf Kamlah, Wiesbaden
Rudi Kramer, Nürnberg
Sebastian Meissner, Bonn
Yvette Reif, Bonn
Dr. Thomas Riemann, Neuss
Bettina Robrecht, Berlin
Johannes Schlattmann, Münster
Ulrich Strack, Berlin
Dr. Eduard Wessel, Münster

Der Verlag und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Spezielle Umstände einzelner Fallkonstellationen wurden nicht berücksichtigt. Bitte konsultieren Sie im Zweifelsfall, einen Rechtsanwalt oder einen Datenschutzexperten, um weitere Entscheidungen für Ihre Situation abzuleiten. Bitte beachten Sie auch mögliche Änderungen der Rechtslage bei oder nach Erscheinen dieser Publikation. Weder der Verlag noch die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Genderhinweis: Aus Gründen der leichteren Lesbarkeit wird in dieser Publikation nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung in der Regel für alle Geschlechter.

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

Redaktion: Sara Pour Abbasi, AWV e. V., Eschborn | Silke Schröder, AWV e. V., Eschborn | Nicole Wingender, AWV e. V., Eschborn
Satz und Layout: Cora Strasdat, AWV e. V., Eschborn

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Eschborn, Mai 2022
2., aktualisierte Auflage
AWV-Best.-Nr.: 43223-w

Die vorliegende Publikation steht als PDF-Datei mit Verlinkungen online zum kostenfreien Download zur Verfügung:

www.awv-net.de/DSGVO-KMU

Vorwort

Die Anwendung der Datenschutzgrundverordnung (DSGVO) ab Mai 2018 erfolgte mit vielen Erwartungen und Befürchtungen. Nicht alle davon waren berechtigt. Weder wurde bislang existenzgefährdendes Bußgeld verhängt, noch erfolgten Abmahnwellen. Aber auch die erhoffte europaweit einheitliche Rechtsanwendung hat sich, aufgrund der Vielzahl an unbestimmten Rechtsbegriffen und Interpretationsmöglichkeiten, noch nicht wahrnehmbar eingestellt. Dennoch deutet sich mit jeder Entscheidung des EuGH an, dass die Wahl einer Verordnung, die unmittelbar gilt und die die vorherige Richtlinie ablöste, richtig war. Nun muss jedoch auch die Anwendbarkeit der DSGVO mit den technischen Entwicklungen in Einklang gebracht werden. Transparenz, Nachvollziehbarkeit und die Möglichkeiten von Big Data, Blockchain und Künstlicher Intelligenz sind nur einige der Stichworte, die auch durch kleinere wirtschaftliche Einheiten zu beachten sind bzw. deren Einsatz möglich ist und die dadurch auch zu Herausforderungen für die Compliance werden. Die DSGVO hat nicht nur den Schutz der natürlichen Person zum Ziel, sondern auch den freien Datenverkehr. Diese Balance zu finden, ist eine tägliche Herausforderung, zu der die AWV mit dieser Broschüre eine Hilfestellung beisteuern möchte. Sie ersetzt nicht eine vertiefte Befassung mit Einzelfragen oder die Einbeziehung eines betrieblichen oder behördlichen Datenschutzbeauftragten, aber sie soll helfen, Fragestellungen zu erkennen und einzuordnen und erste Lösungsmöglichkeiten aufzeigen.

AWV-Arbeitskreis 4.3
„Datenschutz und Informationssicherheit“

Eschborn im Mai 2022

Inhalt

1. Die wichtigsten Änderungen durch die Datenschutzgrundverordnung im Überblick ... 1

2. Anwendungsbereich ... 3

2.1 Sachlicher Anwendungsbereich der neuen Regelungen ... 3

2.2 Räumlicher Anwendungsbereich der neuen Regelungen ... 3

3. Begriffsbestimmungen ... 5

3.1 Betroffene Person ... 5

3.2 Personenbezogene Daten ... 5

3.3 Besondere Kategorien personenbezogener Daten ... 6

3.4 Verarbeitung ... 6

3.5 Pseudonymisierung ... 8

3.6 Anonymisierung ... 8

3.7 Einwilligung ... 8

3.8 Dateisystem ... 9

3.9 Verantwortlicher ... 9

3.10 Gemeinsam Verantwortliche ... 9

3.11 Auftragsverarbeiter ... 9

3.12 Empfänger ... 10

3.13 Öffentliche Stelle ... 10

3.14 Nicht-öffentliche Stelle ... 10

3.15 Dritter ... 10

3.16 Übermittlung ... 10

3.17 Beschäftigte ... 11

3.18 Grenzüberschreitende Verarbeitung ... 11

3.19 One-Stop-Shop-Konzept ... 11

3.20 Datenschutz-Folgenabschätzung ... 12

3.21 Profiling ... 12

3.22 Auskunftsrecht oder Subjektzurgriff ... 12

3.23 Rechenschaftspflicht ... 13
3.24 Europäischer Datenschutzausschuss ... 13
3.25 Datenschutzbehörde/Aufsichtsbehörde/Federführende Behörde ... 13

4. Rechtmäßigkeit der Verarbeitung personenbezogener Daten ... 15

4.1 Einwilligung ... 15
4.1.1 Einwilligung in Verträgen ... 16
4.1.2 Einwilligung eines Kindes ... 17
4.1.3 Einwilligung für Bilder und Filmaufnahmen ... 17
4.1.4 Einwilligung bei besonderen Datenkategorien ... 18
4.2 Vertragserfüllung und vorvertragliche Maßnahmen ... 18
4.3 Erfüllung einer rechtlichen Verpflichtung ... 19
4.4 Lebenswichtiges Interesse ... 20
4.5 Aufgaben im öffentlichen Interesse oder Ausübung hoheitlicher Gewalt ... 20
4.6 Überwiegendes Interesse des Verantwortlichen oder eines Dritten ... 21

5. Zulässigkeit der Weiterverarbeitung personenbezogener Daten ... 23

5.1 Besondere Kategorien personenbezogener Daten ... 24
5.2 Daten über Straftaten ... 25
5.3 Verarbeitung von Beschäftigtendaten ... 25
5.4 Zusätzliche besondere Voraussetzungen für die Datenübermittlung ... 26
5.4.1 Datenübermittlung in Drittländer ... 26
5.4.2 Videoüberwachung ... 31
5.4.2.1 Einsatzbereiche ... 31
5.4.2.2 Rechtsgrundlagen ... 32
5.5 Automatisierte Entscheidungsfindung im Einzelfall einschließlich Profiling ... 38
5.5.1 Scoring ... 40
5.5.2 Informationspflichten und Auskunftsrecht ... 40
5.5.3 Nationale Regelungen zum Profiling ... 40
5.6 Besondere Datenkategorien ... 41

6. Rechte und Pflichten ... 43

6.1 Rechte der Betroffenen ... 43
6.1.1 Information und Transparenz ... 43

6.1.1.1 Direkterhebung beim Betroffenen ... 45
6.1.1.2 Dritterhebung ... 46
6.1.1.3 Mögliche Gliederung für Datenschutzhinweise ... 47
6.1.1.4 Ausnahmen nach DSGVO und BDSG ... 49
6.1.1.5 Umsetzungshinweise ... 50
6.1.2 Auskunft ... 51
6.1.3 Datenübertragbarkeit ... 54
6.1.4 Weitere Betroffenenrechte ... 55
6.1.5 Fazit ... 56

6.2 Pflichten der Datenverarbeiter ... 56
6.2.1 Informationspflichten ... 57
6.2.2 Löschpflichten ... 59
6.2.3 Auftragsverarbeitung ... 60
6.2.4 Neue Dokumentationspflichten ... 61
6.2.4.1 Datenschutzgrundsätze und Rechenschaftspflicht ... 61
6.2.4.2 Datenschutzmanagementsystem ... 61
6.2.4.3 Verzeichnis der Verarbeitungstätigkeiten ... 62
6.2.4.4 Sicherheit der Verarbeitung ... 63
6.2.4.5 Meldung von bzw. Benachrichtigung bei Schutzverletzungen – „Datenpannen“ ... 63
6.2.4.6 Datenschutz-Folgenabschätzung ... 64
6.2.4.7 Benennung eines Datenschutzbeauftragten ... 65
6.2.5 Zusammenfassung ... 65

7. Auftragsverarbeitung ... 67

7.1 Angebotseinholung und Angebotsauswahl ... 67

7.2 Der Vertrag ... 68
7.2.1 Form des Vertrages ... 69
7.2.2 Übermittlungsprivileg künftig auch für Auftragsverarbeitung in Drittländern ... 70
7.2.3 Kontrollpflichten des Auftraggebers und des Auftragsverarbeiters ... 70
7.2.4 Pflichten des Auftraggebers bzw. des Auftragsverarbeiters im Zusammenhang mit einer Datenschutz-Folgenabschätzung ... 71
7.2.5 Vergütungsfragen frühzeitig klären ... 71
7.2.6 Haftungserweiterung auf Auftragsverarbeiter ... 71
7.2.7 Beauftragung von Dienstleistungen, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann ... 72
7.2.8 Regelung zum Einsatz von Unterauftragnehmern ... 72
7.2.9 Abgrenzung Auftragsverarbeitung zur „Funktionsübertragung“ ... 73
7.2.10 Gemeinsame Verantwortlichkeit ... 74

8. Datenschutzmanagementsystem ... 77

8.1 Vorteile eines Datenschutzmanagementsystems ... 78

8.2 Datenschutzmanagement und Informationssicherheit ... 78

8.3 Datenschutzmanagementsystem-Prozess ... 79

8.4 Inhalte einer Datenschutzrichtlinie ... 79
8.4.1 Datenschutzorganisation und Verantwortlichkeiten ... 79
8.4.2 Einbindung des Datenschutzbeauftragten ... 80
8.4.3 Verzeichnis von Verarbeitungstätigkeiten ... 81
8.4.4 Datenschutz-Folgenabschätzung ... 81
8.4.5 Vertragsmanagement ... 82
8.4.6 Verpflichtung auf das Datengeheimnis ... 82
8.4.7 Datenschutz-Schulung ... 83
8.4.8 Prozess zur Wahrnehmung von Betroffenenrechten ... 83

9. Zertifizierung ... 85

10. Der Datenschutzbeauftragte ... 89

10.1 Einführung ... 89

10.2 Voraussetzungen der Benennungspflicht ... 89
10.2.1 Benennungspflicht nach DSGVO ... 89
10.2.2 Benennungspflicht nach BDSG ... 91
10.2.3 Freiwillige Benennung ... 91
10.2.4 Übersicht zur Benennungspflicht ... 92

10.3 Aufgaben des Datenschutzbeauftragten ... 92
10.3.1 Allgemeines ... 92
10.3.2 Übertragung weiterer Aufgaben an den Datenschutzbeauftragten ... 95
10.3.3 Pflicht zur risikoorientierten Tätigkeit ... 95

10.4 Rechtsstellung des Datenschutzbeauftragten ... 96
10.4.1 Unabhängigkeit und organisatorische Einordnung ... 96
10.4.2 Abberufungsschutz, Kündigungsschutz und Benachteiligungsverbot ... 96
10.4.3 Anspruch auf Einbindung, Unterstützung und Fortbildung ... 97
10.4.4 Verpflichtung zur Wahrung der Vertraulichkeit ... 98

10.5 Anforderungen an den Datenschutzbeauftragten ... 98

10.6 Anforderungen an die Benennung ... 100
10.6.1 Optionen bei Benennung ... 100
10.6.2 Zeitpunkt, Form und arbeitsrechtliche Aspekte der Benennung ... 100
10.6.3 Dauer der Benennung ... 101
10.6.4 Kontaktdaten des Datenschutzbeauftragten ... 101

10.7 Fazit ... 102

11. Die Datenschutzaufsichtsbehörden – externe Kontrolle 103

11.1 Aufgaben der Aufsichtsbehörden 103

11.2 Prüfungs- und Informationsbefugnisse der Aufsichtsbehörden 104

11.3 Durchsetzungsbefugnisse der Datenschutzaufsichtsbehörden 104

12. Datensicherheit 107

12.1 Zum Risikobegriff der DSGVO 108

12.2 Technische und organisatorische Maßnahmen 109

12.3 Stand der Technik 110

12.4 Restrisiko 110

13. Bußgelder und Sanktionen bei Datenschutzverstößen 111

13.1 Bußgelder bei Verstößen gegen die DSGVO 111

13.2 Sanktionen bei Verstößen gegen die DSGVO 112

13.3 Sanktionen des BDSG 112

14. Öffentliche Stellen 115

Sammlung weiterführender Links 119

Abkürzungsverzeichnis

Abs.	Absatz
a. F.	alte Fassung
AG	Auftraggeber
AV	Auftragsverarbeiter
Art.	Artikel
BayLDA	Das Bayerische Landesamt für Datenschutzaufsicht
BayLfD	Der Bayerische Landesbeauftragte für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BCR	Binding Corporate Rule
BDSG	Bundesdatenschutzgesetz vom 30. Juni 2017 Ausfertigungsdatum: 30.06.2017 Vollzitat: „Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)“ Ersetzt G 204-3 v. 20.12.1990 I 2954, 2955 (BDSG 1990) Das Gesetz wurde als Art. 1 des Gesetzes vom 30.6.2017 I 2097 vom Bundestag mit Zustimmung des Bundesrates beschlossen. Es ist gem. Art. 8 Abs. 1 Satz 1 dieses Gesetz am 25. Mai 2018 in Kraft getreten.
BDSG a. F.	Bundesdatenschutzgesetz alte Fassung, d. h. Bundesdatenschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (BGBl. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (BGBl. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (BGBl. I, S. 2814) Aktualisierte, nicht amtliche Fassung Herausgeber: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stand: 11. Juni 2010
BetrVG	Betriebsverfassungsgesetz
BPersVG	Bundespersonalvertretungsgesetz
BPolG	Gesetz über die Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
CoC	Codes of Conduct
DAkkS	Deutsche Akkreditierungsstelle
Drs.	Drucksache
DSAnpUG-EU	Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680; Datenschutz-Anpassungs- und Umsetzungsgesetz EU

DSFA	Datenschutzfolgenabschätzung
DSGVO	Europäische Datenschutzgrundverordnung
DSK	Datenschutzkonferenz
DSMS	Datenschutzmanagementsystem
EDSA	Europäischer Datenschutzausschuss
EDPB	European Data Protection Board
EG	Erwägungsgrund
EU	Europäische Union
EU-DSGVO	Europäische Datenschutzgrundverordnung
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
gem.	gemäß
i. S. d.	im Sinne des/der
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
i. V. m.	in Verbindung mit
KMU	Kleine und mittlere Unternehmen
KUG	Kunsturhebergesetz
lit.	lateinisch: littera, Buchstabe
Nr.	Nummer
OWiG	Gesetz über Ordnungswidrigkeiten
QR-Code	Quick Response-Code
S.	Satz
sog.	sogenannte/r/s
StGB	Strafgesetzbuch
TMG	Telemediengesetz
TOM	technische und organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
TVG	Tarifvertragsgesetz
URL	Uniform Resource Locator
UWG	Gesetz gegen den unlauteren Wettbewerb
VPN	virtuelles privates Netzwerk
Ziff.	Ziffer

1. Die wichtigsten Änderungen durch die Datenschutzgrundverordnung im Überblick

Weder durch die Datenschutzgrundverordnung (DSGVO) noch durch das Bundesdatenschutzgesetz (BDSG) in der Fassung von 2018 wurde der Datenschutz neu erfunden. Bei vielen Fragestellungen wurden grundsätzlich bisherige Grundlagen und Prinzipien des Datenschutzes fortgeführt. Dazu zählen insbesondere

- das informationelle Selbstbestimmungsrecht des Einzelnen,
- das Verbotsprinzip mit Erlaubnisvorbehalt,
- der Grundsatz der Datenvermeidung und Datensparsamkeit,
- der Grundsatz der Zweckbindung,
- der Grundsatz der Transparenz,
- die Gewährleistung der Datensicherheit,
- eine nachhaltige Aufsicht.

Zu den wichtigen Neuerungen zählen vor allem

- **Marktortprinzip:** Die Anwendbarkeit europäischen Datenschutzrechts auf außereuropäische Internetdienstleister (Art. 3 Abs. 2 DSGVO).
- **Entfallen bürokratischer Melde- und Genehmigungspflichten:** Die bisherige Pflicht gem. § 4 d BDSG a. F., grundsätzlich alle Verfahren automatisierter Verarbeitungen personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden, ist entfallen.
- **One-Stop-Shop-Mechanismus:** Für Unternehmen, die Niederlassungen in mehreren Mitgliedstaaten haben, wird künftig nur die Aufsichtsbehörde an ihrem Hauptsitz zuständig sein.
- **Auskunftsbegehren:** Der Anspruch wurde um einen Anspruch auf eine Kopie der personenbezogenen Daten erweitert.
- **Datenportabilität:** Künftig hat der Betroffenen grundsätzlich das Recht, seine zur Verfügung gestellten Daten in einem gängigen maschinenlesbaren Format zu erhalten.
- **Erleichterungen für KMU:** Unternehmen mit weniger als 250 Mitarbeitern müssen grundsätzlich kein Verzeichnis über alle Verarbeitungsvorgänge mit personenbezogenen Daten mehr führen.

- **Erlaubnistatbestände:** Die Sonderregelungen für den Adresshandel und die Werbung sowie für die Datenübermittlung an Auskunfteien und das Scoring (Hinweis BDSG) sind entfallen.
- **Einwilligungen:** Das bisherige Schriftformerfordernis ist entfallen.
- **Folgenabschätzung:** In den Fällen, in denen die Verarbeitung der personenbezogenen Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, muss der Verantwortliche (das Unternehmen) eine Datenschutz-Folgenabschätzung durchführen.
- **Rechenschaftspflicht des Verantwortlichen:** Die Pflicht nachzuweisen, dass die Vorschriften der DSGVO eingehalten werden.
- **Haftung und Sanktionen:** Eine drastische Erhöhung des Sanktionsrahmens bei Datenschutzverstößen
- **Schadenersatz:** Nun ist bei Verletzungen des Datenschutzes auch ein immaterieller Schadenersatz möglich.

2. Anwendungsbereich

2.1 Sachlicher Anwendungsbereich der neuen Regelungen

Wie bisher gilt das Datenschutzrecht für jede Form der Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes und der Länder (§ 1 Abs. 1 S. 1 BDSG) und durch nichtöffentliche Stellen. Öffentliche Stellen des Bundes und der Länder werden für Deutschland in § 1 Abs. 1 S. 1 BDSG definiert. Erforderlich ist dabei, dass eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten bzw. eine nichtautomatisierte Verarbeitung personenbezogener Daten erfolgt, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Daneben regelt die DSGVO in Art. 2 aber auch Ausnahmen des sachlichen Anwendungsbereiches.

> **Beispiel:** Wenn die Verarbeitung durch natürliche Personen ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit erfolgt, gelten weder DSGVO noch das BDSG. Hierzu zählt z. B. das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten.

Die Regelungen gelten nicht für die Verarbeitung personenbezogener Daten juristischer Personen. Akten oder Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind, fallen nicht in den Anwendungsbereich der DSGVO. Ferner gelten die Regelungen nicht für die personenbezogenen Daten Verstorbener.

2.2 Räumlicher Anwendungsbereich der neuen Regelungen

Auf nichtöffentliche Stellen finden die neuen Regelungen Anwendung, wenn

- der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Inland, d. h. im jeweiligen Mitgliedstaat, verarbeitet oder

- die Verarbeitung im Rahmen der Tätigkeit einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters in der EU erfolgt.

Wenn sich die betroffene Person in der EU befindet, gilt die DSGVO auch für Unternehmen außerhalb der EU (ohne inländische Niederlassung), wenn

- sie in der EU Waren oder Dienstleistungen anbieten oder
- die Datenverarbeitung dazu dient, das Verhalten betroffener Personen in der EU zu beobachten. Letzteres ist z. B. der Fall, wenn Internetaktivitäten nachvollzogen werden. Für europäische und außereuropäische Anbieter gelten damit in den genannten Fällen dieselben Regelungen (Marktortprinzip).

Anmerkung: Die DSGVO sieht eine Reihe von „Öffnungsklauseln" in Form von Spezifikationen, Regelungsgeboten und Regelungsoptionen vor. Damit wurde den Mitgliedstaaten in diesen Fällen ein Handlungsspielraum eingeräumt, der zu unterschiedlichen Regelungen, z. B. der betrieblichen Datenschutzbeauftragten, der Altersgrenze eines Kindes für die Einwilligung oder des Arbeitnehmerdatenschutzes, führte. Kommt es in diesen Fällen zu einer grenzüberschreitenden Verarbeitung, bei der z. B. die Altersgrenze eines Kindes für die Wirksamkeit einer Einwilligung von Bedeutung ist, fehlt in der DSGVO eine Regelung zum anwendbaren Recht. In diesen Fällen besteht grundsätzlich Rechtswahlfreiheit, aber bei Verbraucherverträgen kommt dann das Recht des Mitgliedstaates des Verbrauchers zur Anwendung.

3. Begriffsbestimmungen

Verschaffen Sie sich einen Überblick über alle personenbezogenen Daten, die Sie erheben, verarbeiten oder nutzen. Hierbei sind die nachstehenden Begriffsbestimmungen zu beachten.

3.1 Betroffene Person

Eine „betroffene Person" ist eine natürliche Person. Eine betroffene Person kann beispielsweise eine Person, ein Kunde, ein Interessent, ein Mitarbeiter, eine Kontaktperson usw. sein.

3.2 Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen („betroffene Person" im Sinne der DSGVO), also eines Menschen, z. B.:

- Name,
- Titel,
- Anschrift,
- Familienstand,
- Religionszugehörigkeit,
- Ausbildungsgrad,
- Gesundheitsangaben,
- Partei- oder Verbandszugehörigkeit,
- Einkommen,
- Besteuerungsmerkmale,
- Steueridentifikationsnummer,
- Zahlungsgewohnheiten,
- IP-Adresse,
- evtl. Firmendaten (Personengesellschaften, Kapitalgesellschaften mit einem einzigen Anteilseigner).

3.3 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten sind solche personenbezogene Daten, aus denen die rassische und ethnische Herkunft, die politische Meinungen, die religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgeht, genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person sowie Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

Mit genetischen und biometrischen Daten werden zwei neue besondere Datenkategorien eingeführt, die in Art. 4 Nr. 13 und 14 DSGVO näher definiert werden.

- **Genetische Daten:** sind danach personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

- **Biometrische Daten:** sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten, also Fingerabdrücke oder Venenabdrücke. Erwägungsgrund 51 stellt klar, dass nicht jedes Foto („Lichtbild“) eine Verarbeitung biometrischer Daten darstellt.

3.4 Verarbeitung

Eine Verarbeitung ist gemäß Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten, etwa das/die

- **Erheben:** das Beschaffen von personenbezogenen Daten bei dem Betroffenen selbst (z. B. durch Befragen, Beobachten, Übernahme aus Akten).

- **Erfassen:** das Aufnehmen personenbezogener Daten auf einem Datenträger zum Zwecke der weiteren Verarbeitung oder Nutzung.
- **Ordnen:** das Aufbauen einer wie auch immer gearteten Struktur der Daten.
- **Auslesen:** die Datenerhebung durch Konsultieren eines vorhandenen Datensatzes.
- **Abfragen:** die Datenerhebung durch Konsultieren eines Datensatzes einer externen Datenbank.
- **Abgleichen oder Verknüpfen:** die Überprüfung von Daten dahingehend, ob die in mehreren Dateisystemen über eine betroffene Person gespeicherten Daten konsistent sind, oder das Zusammenführen von personenbezogenen Daten über eine betroffene Person aus mehreren Dateisystemen.
- **Löschen oder Vernichten:** das Unkenntlichmachen gespeicherter personenbezogener Daten. Das Löschen muss physikalisch erfolgen, d. h., die Reproduzierbarkeit der Daten muss ausgeschlossen sein. Das wird in der Regel durch (mindestens siebenfaches) Überschreiben der Daten erreicht. Das Vernichten ist das endgültige Zerstören des Datenträgers.
- **Organisation:** die sorgfältige und systematische Vorbereitung von Datensätzen bzw. der Aufbau von Datensätzen zur einheitlichen Nutzung.
- **Speicherung:** das Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke der weiteren Verarbeitung oder Nutzung.
- **Anpassung oder Veränderung:** jede inhaltliche Umgestaltung von gespeicherten Daten.
- **Verwendung:** die Nutzung personenbezogener Daten, z. B. eine Kenntnisnahme, die interne Weitergabe, eine Auswertung oder das Kopieren von Daten
- **Offenlegung durch Übermittlung:** das Bereithalten personenbezogener Daten und die Bekanntgabe an einen Dritten (z. B. wenn ein Seminarveranstalter Namen und Kontaktadresse an ein Hotel zwecks Zimmerreservierung übermittelt).
- **Offenlegung durch Verbreitung:** z. B. die Preisgabe von personenbezogenen Daten auf einer Webseite oder in einem Internet-Forum.

Dem Begriff der Verarbeitung unterliegen – wie bisher auch – nicht nur die automatisierten Verfahren, sondern auch manuelle, nicht automatisierte Verfahren. Manuelle Verarbeitungen müssen jedoch Dateisysteme betreffen, nicht bloß unstrukturierte Akten, Aufzeichnungen oder Notizen.

3.5 Pseudonymisierung

Pseudonymisierung ist gemäß Art. 4 Nr. 5 DSGVO das Ersetzen des Namens oder anderer Identifikationsmerkmale durch ein Kennzeichen, so dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Es darf also keine Kenntnis der jeweiligen Zuordnungsregel zwischen Kennzeichen und Person bestehen. Mit der getrennten Aufbewahrung der eigentlichen Daten von den zusätzlichen Informationen und begleitenden technisch-organisatorischen Maßnahmen soll die Wahrscheinlichkeit, dass Daten dieser Person zugeordnet werden können, praktisch ausgeschlossen werden. Eine solche Maßnahme ist z. B. der Einsatz eines Generators, der für einzelne Personen einen eindeutigen pseudonymen Identifikator generiert.

3.6 Anonymisierung

Anonymisierung ist das Verändern personenbezogener Daten derart, dass die hinter den Einzelinformationen stehende betroffene Person nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer Person zugeordnet werden können. In der DSGVO gibt es bei den Begriffsbestimmungen dazu keine Vorgabe, aber in dem EG 22 findet sich eine Beschreibung dazu.

3.7 Einwilligung

Eine Einwilligung ist jede freiwillig, für den bestimmten Fall unmissverständlich abgegebene Willensbekundung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Sie kann in Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung abgegeben werden. Die Einwilligung setzt voraus, dass der Einwilligende informiert ist, das heißt, er mindestens wissen muss, wer der Verantwortliche ist und für welche Zwecke seine personenbezogenen Daten verarbeitet werden sollen.

3.8 Dateisystem

Ein Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. Das können sowohl manuelle Sammlungen (z. B. Akten) oder digitale Sammlungen (z. B. eine Excel-Tabelle oder eine Datenbank) sein.

3.9 Verantwortlicher

Als Verantwortlicher gilt gemäß Art. 4 Nr. 7 DSGVO jede Person oder Stelle (Behörde, Unternehmen, Einrichtung oder sonstige Organisation), die allein oder mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Zwecke umfassen die Zielsetzungen der Verarbeitung, Mittel die hierzu eingesetzten Verfahren und technischen Unterstützungen. Zum Beispiel legt der Verantwortliche fest, dass der Zweck der Datenverarbeitung in der Abwicklung einer Bestellung liegt. Hierzu bedient er sich eines Dienstleisters als Mittel. Der Dienstleister entscheidet dann, wie er die Zustellung tatsächlich vornimmt, kann aber keine eigenen Zwecke verfolgen, beispielsweise die Nutzung der Anschriften für eigene Werbung.

3.10 Gemeinsam Verantwortliche

Zwei oder mehr für die Verarbeitung Verantwortliche, die gemeinsam für eine oder mehrere Organisationen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten bestimmen. Zur Festlegung ihrer jeweiligen Verantwortlichkeiten bei der Verarbeitung personenbezogener Daten bedarf es einer transparenten Regelung. Der wesentliche Inhalt der Regelung wird der betroffenen Person zur Verfügung gestellt.

3.11 Auftragsverarbeiter

Gemäß Art. 4 Nr. 8 DSGVO ist ein Auftragsverarbeiter eine natürliche oder juristische Person oder andere Stelle oder Organisation, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Das wesentliche Element der Dienstleistung ist auf die Verarbeitung personenbezogener Daten für Zwecke des Auftraggebers gerichtet, wie z. B. bei der Nutzung

von Cloud-Diensten für die Personal- oder Kundenverwaltung oder die Aktenvernichtung bzw. Vernichtung von Datenträgern. Erfolgt die Weitergabe personenbezogener Daten nur als Mittel zur Erbringung anderer Leistungen durch den eigenverantwortlich agierenden Dienstleister, dann liegt noch keine Auftragsverarbeitung vor.

3.12 Empfänger

Ein Empfänger ist jede Person oder Stelle, die Daten erhält. Noch nicht ganz geklärt ist, ob dabei auch interne Zuständigkeiten innerhalb einer Behörde oder eines Unternehmens umfasst sind.

3.13 Öffentliche Stelle

Öffentliche Stellen sind Behörden und Institutionen des Bundes und der Länder.

3.14 Nicht-öffentliche Stelle

Nicht-öffentliche Stelle sind eine natürliche oder juristische Person, Gesellschaft und andere Personenvereinigung des privaten Rechts.

3.15 Dritter

Ein Dritter ist eine natürliche oder juristische Person oder andere Stelle oder Organisation, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die befugt sind, für den Verantwortlichen oder Auftragsverarbeiter personenbezogene Daten zu verarbeiten.

3.16 Übermittlung

Die Übermittlung personenbezogener Daten an Länder außerhalb des Europäischer Wirtschaftsraums (EWR) oder an internationale Organisationen unterliegt Beschränkungen. Diese müssen nicht physisch transportiert wer-

den, um übertragen zu werden (Beispiel: Cloud Datenspeicher). Die reine Anzeige von Daten, die an einem anderen Ort gehostet werden, kann eine Übermittlung für Zwecke der DSGVO bedeuten (Beispiel: Web-Anwendung).

3.17 Beschäftigte

Beschäftigte sind Arbeitnehmer, Leiharbeitnehmer im Verhältnis zum Entleiher, Auszubildende, Rehabilitanden, in anerkannten Werkstätten für behinderte Menschen Beschäftigte, Freiwillige, die einen Dienst nach einem Freiwilligendienstgesetz leisten, die in Heimarbeit Beschäftigten, Beamte, Richter, Soldaten sowie Zivildienstleistende. Auch Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte. Dies ergibt sich nicht aus der DSGVO, sondern aus der Regelungsmöglichkeit des Art. 88 DSGVO; von der der deutschen Gesetzgeber z. B. in § 26 Abs. 8 BDSG Gebrauch gemacht hat.

3.18 Grenzüberschreitende Verarbeitung

Die grenzüberschreitende Verarbeitung ist entweder eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in mehr als einem Mitgliedstaat der EU erfolgt, wenn der Verantwortliche oder der Auftragsverarbeiter in mehr als einem Mitgliedstaat der EU niedergelassen ist, oder wenn eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters erfolgt, gleichwohl aber erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat der EU haben kann. Datenschutzrechtlich relevant wird der Drittstaatentransfer, wenn Daten in einen Staat außerhalb der EU/des EWR übermittelt werden.

3.19 One-Stop-Shop-Konzept

Wenn ein Unternehmen in mehr als einem Mitgliedstaat ansässig ist, gibt es eine „federführende Behörde“, die durch den Ort seiner „Hauptniederlassung“ in der EU bestimmt wird. Eine Aufsichtsbehörde, die keine federfüh-

rende Behörde ist, kann auch eine Regulierungsfunktion haben, z. B. wenn die Verarbeitung betroffene Personen in dem Land betrifft, in dem diese Aufsichtsbehörde die nationale Behörde ist.

3.20 Datenschutz-Folgenabschätzung

Die Datenschutzfolgenabschätzung (DSFA) ist Teil des Risikobewertungsprozesses für personenbezogene Daten. Dabei wird festgestellt, welches Risiko entsteht oder wie hoch das Risiko für die Rechte der Betroffenen ist, wenn gewisse Prozesse und Technologien eingesetzt werden. Datenverantwortliche und Datenauftragsverarbeiter unterliegen einer Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung (auch als Datenschutz-Verträglichkeitsprüfung oder DSFA bekannt), bevor sie eine Verarbeitung vornehmen, die aufgrund ihrer Art, ihres Umfangs oder ihres Zweckes voraussichtlich ein hohes Risiko für die Privatsphäre der Betroffenen darstellt.

3.21 Profiling

Profiling ist jede Form der automatisierten Verarbeitung personenbezogener Daten, die bestimmte personenbezogene Aspekte des Einzelnen bewerten oder die Leistung dieser Person, deren Arbeitsleistung, die wirtschaftliche Situation, den Standort, die Gesundheit, persönliche Vorlieben, Zuverlässigkeit oder Verhalten analysieren oder vorhersagen sollen.

3.22 Auskunftsrecht oder Subjektzugriff

Das Auskunftsrecht der betroffenen Person, vom Datenverantwortlichen auf Anfrage bestimmte Informationen bezüglich der Verarbeitung ihrer personenbezogenen Daten einzuholen bezieht sich auf:

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten, die verarbeitet werden
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen

- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
- automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

3.23 Rechenschaftspflicht

Die Rechenschaftspflicht bezieht sich auf die Fähigkeit, die Einhaltung der DSGVO nachzuweisen. In der Verordnung heißt es ausdrücklich, dass dies die Verantwortung der Organisation ist, die im datenschutzrechtlichen Sinne als Verantwortliche gemäß Art. 4 Nr. 7 DSGVO gilt. Um die Einhaltung nachzuweisen, müssen geeignete technische und organisatorische Maßnahmen umgesetzt werden.

3.24 Europäische Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA – oder EDPB für European Data Protection Board) ersetzt die Artikel-29-Datenschutzgruppe. Seine Aufgaben umfassen die Gewährleistung der Übereinstimmung bei der Anwendung der Datenschutzgrundverordnung, die Beratung der EU-Kommission, die Erteilung von Richtlinien, Leitfäden und Empfehlungen, die Akkreditierung von Zertifizierungsstellen und die Erarbeitung von Stellungsnahmen zu Entwürfen von Entscheidungen der Aufsichtsbehörden.

3.25 Datenschutzbehörde/Aufsichtsbehörde/ Federführende Behörde

Datenschutzbehörden sind nationale Datenschutzbehörden, die nach der DSGVO für den Schutz der Privatsphäre und der personenbezogenen Daten zuständig sind. Jeder Mitgliedstaat benannte ein Gremium der Daten-

schutzbehörde, um das lokale Datenschutzrecht um- und durchzusetzen und eine beratende Funktion einzunehmen. Datenschutzbehörden verfügen über signifikante Durchsetzungsbefugnisse, einschließlich der Möglichkeit zur Erhebung beträchtlicher Geldbußen.

4. Rechtmäßigkeit der Verarbeitung personenbezogener Daten

In der DSGVO gilt das Verbot mit Erlaubnisvorbehalt. Die Verarbeitung von personenbezogenen Daten ist demnach nur zulässig, wenn eine Einwilligung oder eine andere in der DSGVO normierte Ausnahme vorliegt. Die zentrale Norm ist Art. 6 DSGVO. Danach sind neben der Einwilligung folgende Erlaubnistatbestände genannt:

- die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen
- wenn sie im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist
- sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dieser Rechtfertigungsgrund gilt nicht für Behörden.

Der für die Datenverarbeitung Verantwortliche muss geeignete Maßnahmen treffen, um die notwendigen Nachweise für das Vorliegen einer Ausnahme erbringen zu können. Alle Zulässigkeitstatbestände des Art. 6 Abs. 1 DSGVO stehen unter dem Vorbehalt der Erforderlichkeit. Diese ist nur gegeben, wenn die Aufgabe sonst nicht, insbesondere auch nicht ohne Datenverarbeitung, erfüllt werden kann.

4.1 Einwilligung

Mit einer Einwilligung gestattet der Betroffene dem Verarbeiter die Verarbeitung von personenbezogenen Daten. Für die Einwilligung sieht die DSGVO keine Formvorschrift vor. Es reichen auch mündliche Erklärungen oder entsprechende Verhaltensweisen, z. B. das Anklicken eines Käst-

chens beim Besuch einer Internetseite. Entscheidend ist, dass die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der vorgesehenen Verarbeitung ihrer Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit stellen keine Einwilligung dar. Weiterhin muss der Verantwortliche in der Lage sein, nachzuweisen, dass der Betroffene seine Einwilligung zur Datenverarbeitung wirksam erklärt hat.

Die DSGVO stellt klar, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen. Sie ist vor Abgabe der Einwilligung auf dieses Recht hinzuweisen. Die bis zum Zeitpunkt des Widerrufs erfolgten Verarbeitungen bleiben aber rechtmäßig. Der Widerruf muss auf demselben Weg möglich sein, auf dem die Einwilligung erteilt wurde. Wenn die Voraussetzungen für einen anderen Erlaubnistatbestand (z. B. Vertrag, berechtigtes Interesse) vorliegen, kann eine Verarbeitung trotz eines Widerrufs weiterhin möglich/rechtmäßig sein. Einwilligungen von Kindern können auch im Erwachsenenalter noch widerrufen werden.

> **Wichtig:** Bei der Einholung von Einwilligungen ist darauf zu achten, dass auf die Widerrufsmöglichkeit hingewiesen wird und dass der Nachweis einer wirksamen Einwilligung geführt werden kann.

4.1.1 Einwilligung in Verträgen

Erfolgt die Einwilligung durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft (in der Regel also Verträge bzw. vertragsähnliche Gestaltungen im öffentlichen Bereich), muss die vorformulierte Einwilligungserklärung in einer verständlichen und leicht zugänglichen Form und in einer klaren und einfachen Sprache so erfolgen, dass sie von anderen Sachverhalten klar zu unterscheiden ist. Die Einholung einer Einwilligung im Rahmen eines Vertrages ist daher bei Beachtung der genannten Kriterien, z. B. durch Fettdruck, weiterhin möglich.

Ein wichtiges Kriterium für die Rechtmäßigkeit einer vorformulierten Einwilligungserklärung ist wie bisher die Frage der Freiwilligkeit der Erklärung. Nach der DSGVO ist diese dann nicht gegeben, wenn

- zu verschiedenen Verarbeitungsvorgängen nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist oder
- die Erfüllung eines Vertrages oder einer Dienstleistung von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

Für weitergehende Daten ist eine gesonderte Einwilligungserklärung erforderlich. Dem EuGH ist derzeit die Fragestellung vorgelegt, ob in Nutzungsbedingungen von Dienstleistungen wie sozialen Netzwerken auch Verarbeitungen geregelt sein können, die ansonsten über einer Einwilligung ihre Grundlage fänden. Der Europäische Datenschutzausschuss hat zur Verarbeitung auf Basis einer Einwilligung auch eine Leitlinie veröffentlicht.[1]

4.1.2 Einwilligung eines Kindes

Neu ist eine Sonderregelung für die Einwilligung eines Kindes bei Angeboten von Diensten der Informationsgesellschaft. Kinder ab 16 Jahren können ohne nachgewiesene Zustimmung der Erziehungsberechtigten Einwilligungen in die Verarbeitung ihrer Daten auf Webseiten oder über Apps („Dienste der Informationsgesellschaft") erteilen. Für die Einwilligung von Kindern unter 16 Jahren ist die Zustimmung der Erziehungsberechtigten notwendig. Relevant wird dies insbesondere bei Gewinnspielen oder Onlineplattformen, die sich speziell an Kinder und Jugendliche richten. Von der Möglichkeit, diese Altersgrenze bis auf 13 Jahre herabzusetzen, hat der deutsche Gesetzgeber bisher keinen Gebrauch gemacht.

4.1.3 Einwilligung für Bilder und Filmaufnahmen

Häufig werden im Unternehmen Bilder oder Filmaufnahmen von Veranstaltungen gemacht und in firmeninternen Publikationen wie Mitarbeiterzeitung oder Intranet veröffentlicht. Dabei steht in erster Linie der Dokumentationscharakter im Vordergrund. Hier können nach wie vor

1 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679. Mai 2020. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf (abgerufen am 11.05.2022).

die Grundsätze des Kunsturhebergesetzes (insbesondere § 23 KUG) herangezogen werden, wonach die Einwilligung formfrei erfolgen kann, also auch durch eine aktive Mitwirkung („in die Kamera lächeln"). Es empfiehlt sich, schon bei der Einladung zur Veranstaltung auf die Foto- und Filmaufnahmen hinzuweisen und dies zu Beginn der Veranstaltung ausdrücklich zu erwähnen. So haben die Beteiligten die Möglichkeit, dem Fotografen auszuweichen.

Sollen allerdings Foto- und Filmaufnahmen zu Werbezwecken, z. B. zum Zwecke einer Recruitingkampagne oder auch außerhalb des Unternehmens veröffentlicht werden, empfiehlt sich schon aus Gründen der Nachweisbarkeit eine schriftliche Einwilligung, die sich ausdrücklich auf Werbezwecke und geplante Veröffentlichungskanäle bezieht. Im letztgenannten Fall empfiehlt sich eine vertragliche Regelung zwischen den Beteiligten, insbesondere bei geplanter Veröffentlichung in sozialen Medien.

4.1.4 Einwilligung bei besonderen Datenkategorien

Wie bisher auch ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich an eine Einwilligung gebunden. Der Begriff der besonderen Kategorien personenbezogener Daten wird durch die Einbeziehung genetischer und biometrischer Daten erweitert (s. ggf. für nähere Erläuterungen Kap. 3.3, S. 6).

> **Wichtig:** Bestehende Einwilligungen bleiben wirksam, wenn die Art der bereits erteilten Einwilligung den Bedingungen der DSGVO entspricht, d. h., sie muss freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich erfolgt sein. Die bestehenden Einwilligungen sind darauf zu überprüfen. Auch sind geeignete Maßnahmen zu treffen, um den erforderlichen Nachweis einer wirksamen Einwilligung zu erbringen, z. B. durch Double Opt-In. Die Beweislast liegt also weiterhin bei der verantwortlichen Stelle.

4.2 Vertragserfüllung und vorvertragliche Maßnahmen

Die Datenverarbeitung kann gem. Art. 6 Abs. 1 lit. b DSGVO auf die vertragliche oder vorvertragliche Beziehung gestützt werden, die mit

der betroffenen Person besteht. Die Verarbeitung von personenbezogenen Daten ist dann zulässig, wenn sie für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Eine Verarbeitung ist jedenfalls immer dann erforderlich, wenn der Vertrag oder die Maßnahme ohne sie nicht so erfüllt werden könnte, wie die Parteien sich geeinigt haben. Für Detailfragen, welche Datenverarbeitung für die Vertragserfüllung unentbehrlich und objektiv sinnvoll ist, hat der Europäische Datenschutzausschuss eine Leitlinie für die Verarbeitung personenbezogener Daten gem. Art. 6 Abs. 1 lit. b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen veröffentlicht.[2]

> **Beispiel:** Verträge mit Kunden oder Lieferanten, Vertragsanbahnung mit interessierten Neukunden oder Stellenbewerbern

4.3 Erfüllung einer rechtlichen Verpflichtung

Laut Art. 6 Abs. 1 lit. c DSGVO handelt es sich um eine rechtliche Verpflichtung, die nicht auf einer freien Entscheidung beruht, sondern kraft Rechts der Europäischen Union oder eines Mitgliedstaats erforderlich ist. Dieser Erlaubnistatbestand betrifft nicht nur den öffentlichen Sektor, sondern beispielsweise auch Unternehmen, die gesetzliche Vorgaben umsetzen. Danach ist eine Datenverarbeitung erlaubt, sofern diese durch eine andere Rechtsgrundlage vorgegeben wird. Voraussetzung hierfür ist, dass die Datenverarbeitung zur Erfüllung eigener Rechtspflichten erforderlich ist.

> **Beispiel:** Übermittlung personenbezogener Daten aufgrund (lohn-)steuerlicher oder sozialrechtlicher Vorgaben, Meldepflichten des Arbeitgebers bezüglich der Einhaltung gesetzlicher Bestimmungen (z. B. Mindestlohn)

2 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen. Oktober 2019. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf (abgerufen am 11.05.2022).

4.4 Lebenswichtiges Interesse

Art. 6 Abs. 1 lit. d DSGVO trägt der Selbstverständlichkeit Rechnung, dass in Notlagen für den Betroffenen oder einen Dritten der Schutz personenbezogener Daten gegenüber lebenswichtigen Interessen zurücktreten muss. Diese Norm sollte nur in expliziten Ausnahmefällen herangezogen werden (EG 46, S. 2). In Betracht kommen insbesondere Art. 6 Abs. 1 lit. e und lit. c DSGVO.

> **Beispiel:** Medizinischer Notfall, Katastrophen

4.5 Aufgaben im öffentlichen Interesse oder Ausübung hoheitlicher Gewalt

Eine Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 lit. e DSGVO auch dann rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Jede staatliche Stelle darf danach Verarbeitungen in dem Rahmen vornehmen, der durch Gesetz ihrem Aufgaben- und Zuständigkeitsbereich zugewiesen ist. Den Gesetzgebern wird für die Verarbeitung durch öffentliche Stellen das Recht zur Konkretisierung der Rechtsgrundlagen eingeräumt. Diese müssen eine Festlegung der Zweckbestimmung erhalten. Zu beachten ist, dass ein im öffentlichen Interesse liegendes Ziel in verhältnismäßiger Weise verfolgt wird. Damit können die meisten in Deutschland geltenden bereichsspezifischen Datenschutzregelungen zur Zulässigkeit der Datenverarbeitung beibehalten werden.

> **Beispiel:** Polizeibeamter fragt in einer spezifischen Gefahrenlage Daten über eine Person ab, Zeugenschutzprogramm

4.6 Überwiegendes Interesse des Verantwortlichen oder eines Dritten

Art. 6 Abs. 1 lit. f DSGVO enthält die zentrale Interessenabwägungsklausel der DSGVO. Eine zulässige Verarbeitung von personenbezogenen Daten darf hiernach nur dann erfolgen, wenn damit die Interessen eines Verantwortlichen/Dritten gewahrt werden können und gleichzeitig die schutzwürdigen Interessen der betroffenen Person nicht untergraben werden. Die Interessen der beteiligen Parteien werden einander gegenübergestellt. Die Frage, ob ein berechtigtes Interesse vorliegt, ist zunächst unter Berücksichtigung des Zwecks der Verarbeitung zu beurteilen. Neben rechtlichen Interessen können auch wirtschaftliche und ideelle Interessen des Verarbeiters berücksichtigt werden. Wie alle Zulässigkeitstatbestände des Art. 6 Abs. 1 DSGVO steht auch die die Verarbeitung zur Wahrung des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DSGVO unter dem Vorbehalt der Erforderlichkeit.

Eine Interessenabwägung fällt aber zulasten des Datenverarbeiters aus, wenn „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person" überwiegen. Dabei sind nach EG 47 DSGVO die „vernünftigen Erwartungen" des Betroffenen zu berücksichtigen. Zur angemessenen Durchführung der Interessenabwägung nach lit. f ist also eine Drei-Stufen-Prüfung mit folgenden Prüfungsstufen durchzuführen:

1. Prüfungsstufe: Identifikation der verfolgten Interessen und Einstufung als berechtigt/nicht berechtigt (Interessenidentifikation und -einstufung)
2. Prüfungsstufe: Feststellung der Erforderlichkeit der Datenverarbeitung zum Erreichen des verfolgten Interesses (Erforderlichkeitsprüfung)
3. Prüfungsstufe: Abwägung mit den Interessen/Grundrechten und Grundfreiheiten der betroffenen Personen (Interessenabwägung)

Darüber hinaus sind Informations- und Widerspruchsrechte der Betroffenen zu berücksichtigen. Die DSGVO sieht spezifische Informationspflichten bei Verarbeitungen auf Basis der Interessenabwägung vor. Die vernünftigen Erwartungen des Betroffenen können durch eine umfassende Transparenz im Rahmen der Erfüllung der Informationspflichten zu-

sätzlich geschärft werden. Es ist darauf zu achten, dass in diesen Fällen den Betroffenen ein ausdrückliches Widerspruchsrecht einzuräumen ist.

Beispiele: Nach EG 48 DSGVO können auch Konzerninteressen in die Interessenabwägung einbezogen werden: „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind[,] können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt." Dieser EG stellt jedoch keine „Konzernklausel" zur generell zulässigen Übermittlung von Kunden- und Beschäftigtendaten zwischen konzernangehörigen Unternehmen dar. Immer sind auch die Interessen der betroffenen Personen zu berücksichtigen, zum Beispiel der Grundsatz der Vertraulichkeit von Personaldaten nach deutschem Arbeitsrecht.

Zur Verhinderung von Betrug ist es ein berechtigtes Interesse, personenbezogene Daten im erforderlichen Umfang zu verarbeiten (EG 47). Soweit Werbung nicht auf einer wirksamen Einwilligung der betroffenen Person beruht, wird für die Zulässigkeit von Werbung fast ausschließlich die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO maßgeblich sein. Auch kann die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine Verarbeitung betrachtet werden, die einem berechtigten Interesse dient (EG 47). Inwieweit es in Europa gelingen wird, die in Deutschland in der Vergangenheit entwickelten Maßstäbe auch unter Geltung der DSGVO aufrechtzuerhalten, wird sich zeigen. Jedenfalls gilt auch zukünftig neben der DSGVO die deutsche wettbewerbsrechtliche Norm des § 7 UWG (Unzumutbare Belästigungen), wonach weitgehend eine vorherige, ausdrückliche Einwilligung gefordert wird.

5. Zulässigkeit der Weiterverarbeitung personenbezogener Daten

Die DSGVO unterliegt dem Prinzip der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), d. h., die Verarbeitung personenbezogener Daten wird durch den festgelegten Zweck begrenzt. Eine begrenzte Weiterverarbeitung erlaubt Art. 6 Abs. 4 DSGVO für kompatible Zwecke. Der Verantwortliche muss deshalb einen sogenannten Kompatibilitätstest durchführen. Dabei sind folgende Gesichtspunkte einzubeziehen:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO verarbeitet werden,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Sind die weiteren Zwecke mit dem ursprünglichen Erhebungszweck vereinbar, bedarf es für die Rechtmäßigkeit der Weiterverarbeitung keiner gesonderten Rechtsgrundlage mehr. Ist die geplante Weiterverarbeitung nicht mit dem ursprünglichen Erhebungszweck vereinbar, soll eine Weiterverarbeitung nur dann zulässig sein, wenn hierfür eine Einwilligung der betroffenen Person oder eine spezialgesetzliche „Weiterverarbeitungsnorm" im Recht der Union oder der Mitgliedstaaten vorliegt oder die Weiterverarbeitung auf einen Erlaubnistatbestand gem. Art. 5 Abs. 1 DSGVO gestützt werden kann.

> **Beispiel:** die Anonymisierung personenbezogener Daten für weitere Zwecke, z. B. „Big Data" wird seitens einiger Aufsichtsbehörden als Zweckänderung definiert und unterliegt dann den Anforderungen des Art. 6 Abs. 4 DSGVO

5.1 Besondere Kategorien personenbezogener Daten

Hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten, die sich per se durch eine große Sensibilität kennzeichnen, trifft Art. 9 DSGVO besondere Schutzregelungen. Hierzu zählen Daten zur rassischen und ethnischen Herkunft, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben und sexueller Ausrichtung sowie genetische und biometrische Daten zur eindeutigen Personenidentifizierung. Deren Verarbeitung ist grundsätzlich untersagt.

Eine Ausnahme von dem grundsätzlichen Verarbeitungsverbot ist zunächst die explizite Einwilligung. Art. 9 Abs. 2 DSGVO legt überdies eine Vielzahl von weiteren Ausnahmen vom Verarbeitungsverbot fest, darunter zum Beispiel:

- bei Ausübung von Rechten aus dem Arbeitsrecht, der sozialen
- Sicherheit und des Sozialschutzes,
- zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit,
- bei der Verarbeitung durch einen sogenannten Tendenzbetrieb,
- bei vom Betroffenen offenkundig veröffentlichten Daten,
- zur Durchsetzung rechtlicher Ansprüche,
- zur Gesundheitsvorsorge, Arbeitsmedizin, medizinischen Diagnostik, zur Versorgung und Behandlung, Verwaltung im Gesundheits- und Sozialbereich oder
- im öffentlichen Gesundheitswesen, für Archivzwecke, zur wissenschaftlichen und historischen Forschung und für statistische Belange.

Dabei wird nicht mehr zwischen öffentlicher und privater Datenverarbeitung im Gesundheits- und Sozialbereich unterschieden.

Der deutsche Gesetzgeber hat die Zulässigkeit der Verarbeitung sensibler Daten durch § 22 BDSG konkretisiert. Damit konnten die deutschen Zulässigkeitsregelungen zur Datenverarbeitung im deutschen Sozial- und Gesundheitsrecht weitgehend beibehalten werden.

Eine zusätzliche Bedingung stellt Art. 9 Abs. 3 DSGVO auf, der die Verarbeitung von Gesundheitsdaten durch Fachpersonal, das einem besonderen

Berufsgeheimnis unterliegt, regelt. Auch diese Regelung wurde durch § 22 BDSG konkretisiert. Werden Berufsgeheimnisse nicht von den Tatbeständen erfasst, die in Art. 9 DSGVO und § 22 BDSG genannt werden, so muss im Einzelfall geprüft werden, ob die in § 203 StGB sowie in weiteren nationalen Spezialgesetzen enthaltenen Berufsgeheimnisse von nationalen Ausnahmeklauseln erfasst werden.

5.2 Daten über Straftaten

Für Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln werden in Art. 10 DSGVO spezifische Voraussetzungen für die Verarbeitung benannt: Die Verarbeitung muss „unter behördlicher Aufsicht" erfolgen; anderenfalls bedarf es angemessener gesetzlicher Garantien.

5.3 Verarbeitung von Beschäftigtendaten

Der deutsche Gesetzgeber hat von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht und mit § 26 BDSG eine Regelung zu Datenverarbeitungen für Beschäftigungsverhältnisse verabschiedet. Sie ist eine spezielle Regelung zur Verarbeitung von Beschäftigtendaten und entspricht weitgehend dem § 32 BDSG a. F. Der Kreis der erfassten Beschäftigten ist in § 26 Abs. 8 BDSG festgelegt. Neben Arbeitnehmern, Leiharbeitnehmern und Auszubildenden sind auch noch Heimarbeiter, Beamte, Richter, Soldaten, Bewerber, ehemalige Beschäftigte und weitere Personengruppen erfasst.

Für die Zulässigkeit der Verarbeitung von Daten zu Zwecken des Beschäftigungs-verhältnisses ist maßgebend, ob die Daten für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind.

Daneben enthält § 26 Abs. 1 S. 2 BDSG eine spezielle Aussage zu dem sich auch aus § 26 Abs. 1 S. 1 ergebenden Recht zur Ermittlung gegen mutmaßliche Straftäter. Es handelt sich somit nicht um eine abschließende Regelung zu den Kontrollrechten, die dem Arbeitgeber im Rahmen des Beschäftigungsverhältnisses zustehen.

Neu ist die ausdrückliche Regelung zur Einwilligung im Beschäftigungsverhältnis (§ 26 Abs. 2 BDSG). Das Gesetz normiert an dieser Stelle ausdrücklich den bisher schon bekannten Grundsatz der „Freiwilligkeit". Außerdem setzt eine wirksame Einwilligung Schriftform voraus, die grundsätzlich auch in elektronischer Form erteilt werden kann.

Art. 26 Abs. 4 BDSG stellt noch einmal klar, dass personenbezogene Daten von Beschäftigten auch auf der Grundlage von Kollektivvereinbarungen zulässig sind. Diese Möglichkeit ergibt sich bereits unmittelbar aus der DSGVO (Art. 9 und Art. 88) sowie aus „unberührt" bleibendem nationalen Recht (BetrVG, BPersVG, TVG). Demnach können spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Datenverarbeitung von Beschäftigten weiterhin auf Tarifverträge und Betriebs- oder Dienstvereinbarungen gestützt werden.

5.4 Zusätzliche besondere Voraussetzungen für die Datenübermittlung

5.4.1 Datenübermittlung in Drittländer

Während innerhalb der Europäischen Union ein freier Datenverkehr auf der Grundlage der allgemeinen Regelungen der DSGVO zur Zulässigkeit der Datenverarbeitung besteht, ergeben sich bei der Übermittlung personenbezogener Daten in Drittstaaten oder an internationale Organisationen darüber hinaus besondere rechtliche Anforderungen, die in den Art. 44 bis 50 DSGVO beschrieben werden. Durch diese Regelungen soll sichergestellt werden, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen in der EU bei der Übermittlung personenbezogener Daten an Verantwortliche, Auftragsverarbeiter, internationale Organisationen oder andere Empfänger außerhalb der EU nicht untergraben wird. Für die Zulässigkeit der Übermittlung personenbezogener Daten in ein Drittland bedeutet dies, dass der Verantwortliche eine vierstufige Prüfung vornehmen muss:

1. **Grundsätzliche Anforderungen**
   Zunächst ist zu prüfen, ob die Übermittlung auf einen der Erlaubnistatbestände der DSGVO und/oder des BDSG gestützt werden kann (Art. 6 Abs. 1 DSGVO, § 24 BDSG und im Bereich

des Beschäftigtendatenschutzes Art. 88 DSGVO i. V. m. § 26 BDSG) und ob die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten nach der DSGVO beachtet werden (s. dazu auch Kap. 4, S. 15 ff.).

2. Angemessenes Datenschutzniveau

Ist dies der Fall, ist in einem zweiten Schritt zu prüfen, ob das betreffende Land, ein Gebiet oder ein besonderer Sektor dieses Landes oder die betreffende internationale Organisation ein angemessenes Datenschutzniveau bietet. Ist diese Voraussetzung erfüllt, dürfen personenbezogene Daten ohne weitere Genehmigung in dieses Land oder an diese internationale Organisation übermittelt werden. Die positive Feststellung, dass ein Land oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet, obliegt der EU-Kommission. Für die Drittstaaten Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Republik Korea, Schweiz, Uruguay und das Vereinigte Königreich hat die EU-Kommission dies bis jetzt festgestellt.[3]

Privacy Shield für die USA

Mit seinem Urteil zum EU-US-Privacy Shield hat der EuGH im Juli 2020 diese Grundlage für den Transfer personenbezogener Daten für ungültig erklärt. Es bestand aus einer Reihe von Zusicherungen der US-amerikanischen Regierung zur Einhaltung von Verarbeitungsregeln für personenbezogene Daten, die den europäischen Datenschutzgrundsätzen entsprechen, einer Klagemöglichkeit für EU-Bürger in den USA und einem Beschluss der EU-Kommission zur Angemessenheit des Datenschutzes, wonach die Garantien für die Übermittlung von Daten auf der Grundlage des Privacy Shields den Datenschutzstandards in der EU entsprechen. Wollten US-amerikanische Unternehmen am Privacy Shield teilnehmen, mussten sie sich in eine vom US-Handelsministerium geführte Liste eintragen lassen. Damit verpflichteten sie sich, die datenschutzrechtlichen Regelungen des Privacy Shield einzuhalten.

3 s. hierzu auch: Europäische Kommission (Hg.): Angemessenheitsentscheidungen der EU-Kommission gemäß Art. 45 DSGVO. o. D. Online: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (abgerufen am 11.05.2022).

Der EuGH hält diese Regelung für unzureichend und definierte in seinem Urteil („Schrems II“) die Anforderungen, dass außer bei einem Angemessenheitsbeschluss zusätzlich zu den geeigneten Garantien (vgl. unten Ziffer 3.) auch geprüft werden muss, ob durch zusätzliche Maßnahmen ein vergleichbares Datenschutzniveau erreicht werden könne.

Dies betrifft aber nicht nur Datentransfers in die USA. Welche konkreten Maßnahmen tatsächlich die Anforderungen des EuGH-Urteils erfüllen, ist aktuell noch nicht rechtssicher zu sagen. Verschlüsselungstechniken, bei denen der Empfänger keinen Zugriff auf den Schlüssel hat, werden dazugehören.

Trans-Atlantic Data Privacy Framework
Mit Pressemeldungen[4] verkündeten die USA und die EU-Kommission im März 2022, dass sie die wesentlichen Punkte[5] ausverhandelt hätten, um ein neues Abkommen zu einem DSGVO-konformen Datentransfer in die USA abzuschließen. Bisher liegt der Text noch nicht ausformuliert vor. Mit einem Abschluss ist frühestens Ende 2022 zu rechnen. Sobald ein neues Abkommen im Europäischen Amtsblatt veröffentlicht ist, kann es dann zu dem dort festgelegten Zeitpunkt angewandt werden. Für alle anderen Drittstaaten wird es bei den Vorgaben aus Schrems II bleiben.

3. Geeignete Garantien
Wenn es nach Meinung der EU-Kommission an einem angemessenem Datenschutzniveau in dem betreffenden Land, der Organisation oder dem entsprechenden Unternehmen fehlt, ist in einem dritten Schritt zu prüfen, ob als Ausgleich für den bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorgesehen werden können. Diese Garantien können sich ergeben aus:

- verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules – BCRs), Art. 47, Art. 46 Abs. 2 lit. b DSGVO,

4 vgl. Europäische Kommission (Hg.): Pressemitteilung „European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework“ vom 25.03.2022. Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087 (abgerufen am 11.05.2022).

5 vgl. Europäische Kommission (Hg.): Factsheet „Trans-Atlantic Data Privacy Framework“ vom 25.03.2022. Online: https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (abgerufen am 11.05.2022).

- von der Kommission erlassene Standarddatenschutzklauseln, Art. 46 Abs. 2 lit. c DSGVO,
- von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln, die von der Kommission genehmigt wurden, Art. 46 Abs. 2 lit. d DSGVO,
- von einer Aufsichtsbehörde genehmigten Verhaltensregeln gem. Art. 40 DSGVO, wenn diese mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen versehen sind, Art. 46 Abs. 2 lit. e DSGVO,
- von einer Aufsichtsbehörde genehmigten einzeln ausgehandelten individuellen Vertragsklauseln, Art. 46 Abs. 3 lit. a DSGVO, oder
- einem genehmigten Zertifizierungsmechanismus, Art. 46 Abs. 2 lit. f, Art. 42 DSGVO.

In all diesen Fällen müssen den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Standarddatenschutzklauseln
Die EU-Kommission hat im Juni 2021 neue Standarddatenschutzklauseln erlassen, die als Zulässigkeitsgrundlage für den Drittstaatentransfer dienen können. Zwar nennt die EU-Kommission diese Vertragsvorlagen immer noch wie in der abgelösten Richtlinie von 1995 „Standard-Vertrags-Klausel" („Standard Contractual Clauses") und kürzt sie daher SCC ab, inhaltlich berücksichtigen sie aber die Anforderungen der DSGVO.[6]

Binding Corporate Rules
Global tätige Unternehmen können selbst interne Regelungen für die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe festlegen und von der zuständigen Aufsichtsbehörde genehmigen lassen. Voraussetzung für eine Genehmigung ist, dass die Regelungen für alle Mitglieder der Unternehmensgruppe rechtlich bindend sind und die Regelungen

6 s. hierzu auch: Europäische Kommission (Hg.): Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates. Juni 2021. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=EN (abgerufen am 11.05.2022).

die allgemeinen Datenschutzgrundsätze der DSGVO beachten, Art. 47 Abs. 1 und 2 DSGVO.

Verhaltensregeln (Code of Conduct)

Erstmalig ist in Art. 40 DSGVO die Schaffung von sektorspezifischen Verhaltensregeln für den Datenschutz vorgesehen. Wirtschaftsverbände können Verhaltensregeln ausarbeiten, mit denen die Anwendung der DSGVO in dem betreffenden Wirtschaftszweig präzisiert wird. Solchen genehmigten Verhaltensregeln können sich auch Unternehmen aus Drittländern ohne ein angemessenes Datenschutzniveau unterwerfen, d. h., sie müssen rechtsverbindlich zusichern, die in den Verhaltensregeln enthaltenen Pflichten zu erfüllen. Auf dieser Grundlage ist dann eine Übermittlung personenbezogener Daten an die betreffenden Unternehmen im Drittland zulässig, ohne dass es einer zusätzlichen Genehmigung bedarf.

Zertifizierungen

Unternehmen aus Drittländern ohne angemessenes Datenschutzniveau haben gem. Art. 42 Abs. 2 DSGVO die Möglichkeit, die Einhaltung der Regelungen der DSGVO durch ein datenschutzrechtliches Zertifizierungsverfahren nachzuweisen. Aus der EU können auf dieser Grundlage personenbezogene Daten an die entsprechenden Unternehmen im Drittland übermittelt werden, ohne dass es einer zusätzlichen Genehmigung bedarf.

4. Individuelle Erlaubnistatbestände

Wenn weder ein Angemessenheitsbeschluss der Kommission noch geeignete Garantien vorliegen ist in einem vierten Schritt zu prüfen, ob einer der individuellen Erlaubnistatbestände der DSGVO für den Datentransfer in Drittländer vorliegt. Nach Art. 49 DSGVO sind Datenübermittlungen in Drittstaaten ohne angemessenes Datenschutzniveau und ohne geeignete Garantien in Ausnahmefällen unter folgenden Bedingungen zulässig:

- mit Einwilligung des Betroffenen, der über die Risiken unterrichtet werden muss, Art. 49 Abs. 1 lit. a DSGVO,
- wenn sie zur Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von

vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich sind, Art. 49 Abs. 1 lit. b DSGVO,
- wenn sie zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen Personen geschlossenen Vertrages erforderlich sind, Art. 49 Abs. 1 lit. c DSGVO,
- wenn sie aus Gründen des öffentlichen Interesses notwendig sind, Art. 49 Abs. 1 lit. d DSGVO,
- wenn sie zur Verfolgung von Rechtsansprüchen erforderlich sind, Art. 49 Abs. 1 lit. e DSGVO,
- wenn sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist und die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage ist, ihre Einwilligung zu geben, Art. 49 Abs. 1 lit. f DSGVO,
- wenn sie zur Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich sind und die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Anzahl von Personen betrifft und keine überwiegenden schutzwürdigen Interessen oder Rechte und Freiheiten der betroffenen Person entgegenstehen, Art. 49 Abs. 1 lit. g S. 2 DSGVO.

5.4.2 Videoüberwachung

5.4.2.1 Einsatzbereiche

Videoüberwachung ist bis Mai 2018 in § 6b Abs. 1 BDSG a. F. definiert als „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen". Angesichts der zunehmenden Verbreitung und Einsatzgebiete von Videokameras gilt es zunächst, verschiedene Fallgruppen abzugrenzen. Üblicherweise wird Videoüberwachung im Unternehmen eingesetzt, um Eingangsbereiche von Bürogebäuden, Werksgelände, Lagerstätten oder Parkplätze zu überwachen. Im öffentlichen Raum wird Videoüberwachung bspw. an Bahnhöfen oder Flughäfen, in Einkaufszentren, Verkaufsräumen, Bankfilialen oder öffentlichen Plätzen eingesetzt. Gelegentlich werden Videokameras auch innerbetrieblich zur Überwachung am Arbeitsplatz eingesetzt.

Der Regelfall ist die offene Videoüberwachung; eine verdeckte Videoüberwachung ist nur in besonderen Ausnahmefällen zulässig. Zunehmend wer-

den neben stationären Kameras auch mobile Kameras eingesetzt, sei es in Form von Dashcams im Auto, Bodycams bei Polizei und Sicherheitspersonal oder Drohnen zur Beobachtung des Baustellenfortschritts. Insbesondere Bodycams ermöglichen einen zielgerichteten, situativen Einsatz, dort wo bspw. eine dauerhafte, statische Videoüberwachung nicht erforderlich ist. Bei Drohnen zur Beobachtung des Baufortschritts steht wiederum das Bauwerk oder Gelände im Vordergrund. Hier richtet sich der Einsatz gerade nicht danach, Personen oder Handlungen aufzuzeichnen. Anders ist es, wenn Drohnen eingesetzt werden, um das Verhalten einzelner Personen zu beobachten. Weitere Einsatzgebiete sind Versuche von Einzelhändlern, mithilfe von Videobildern auf das Alter und Geschlecht der Kunden zu schließen, um diesen zielgruppenspezifische Werbung anzeigen zu können. Inzwischen sind viele Überwachungskameras auch in der Lage, Tonaufnahmen anzufertigen.

Die folgenden Ausführungen behandeln im Schwerpunkt die klassische Videoüberwachung durch nicht öffentliche Stellen, die eingesetzt wird, um Beschädigungen oder Straftaten zu verhindern oder Beweise für eine spätere Rechtsverfolgung zu sichern. Sonderfälle wie Dashcams oder Actioncams, die von Privatpersonen eingesetzt werden, werden hier ebenso wenig betrachtet wie Kameras im Front- oder Heckbereich von Fahrzeugen oder Maschinen, die lediglich – gleichsam wie ein „verlängertes Auge“ – flüchtige Bilder an den Fahrer übermitteln. Auch hier steht nicht die Beobachtung von Personen oder ihres Verhaltens im Vordergrund, sondern die Abbildung des Umfeldes zur Erkennung von Hindernissen.

Ebenso wenig wird hier die Videoüberwachung durch die Landespolizeien oder die Bundespolizei betrachtet, die den jeweiligen Polizeigesetzen unterliegt, so z. B. § 27 Gesetz über die Bundespolizei (BPolG).

5.4.2.2 Rechtsgrundlagen

Anders als das BDSG a. F. enthält die DSGVO keine spezielle Norm zur Videoüberwachung. Die Videoüberwachung wird im EG 91 erwähnt, aber auch bei einer systematisch umfangreichen Überwachung öffentlich zugänglicher Bereiche, wie in Art. 35 Abs. 3 lit. c DSGVO genannt. Dadurch lassen sich zwar bestimmte Formen der Videoüberwachung zuordnen, es lässt sich aber der DSGVO keine explizit auf diese Verarbeitung gerichtete Rechtgrundlage entnehmen.

Die bisherigen Regelungen zur Videoüberwachung, § 6b BDSG a. F., wurden im Videoüberwachungsverbesserungsgesetz vom März 2017 überarbeitet und in dieser Form in § 4 BDSG übernommen. Danach soll bei der Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs, der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse gelten.

Nach § 4 Abs. 4 BDSG gelten die Informationspflichten nach Art. 13 und 14 DSGVO dann, wenn die erhobenen Daten einer bestimmten Person zugeordnet werden. Im Übrigen sind nach § 4 Abs. 2 BDSG die Videoüberwachung und die Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt visuell, z. B. durch gut sichtbare Beschreibungen und Piktogramme, kenntlich zu machen.

Teilweise wird vertreten, dass für eine Regelung der Videoüberwachung im nationalen Recht keine Öffnungsklausel vorliege, mithin die Regelung des § 4 BDSG europarechtswidrig sei. Auch das Bundesverwaltungsgericht hält § 4 BDSG aufgrund formaler Anforderungen für rechtswidrig[7], dies sollte berücksichtigt werden, wenn ein Unternehmen allein darauf seine Videoüberwachung stützen möchte.

In der Praxis richtet sich die Zulässigkeit nach Art. 6 Abs. 1 lit. f. DSGVO. Eine Interessenabwägung ist für die Videoüberwachung vorgesehen (s. auch Kap. 4.2–4.6, S. 18–22).

Der Verantwortliche hat zunächst die Zwecke festzulegen. Typische Zwecke sind die Wahrnehmung des Hausrechts, der Schutz vor Vandalismus, Diebstahl oder Einbrüchen und die Sicherung von Beweisen, wenn es letztlich zu Straftaten gekommen ist. Aus den Zwecken ergibt sich das berechtigte Interesse des Verantwortlichen Der Verantwortliche hat anschließend abzuwägen, ob seinen berechtigten Interessen die schutzwürdigen Belange der Betroffenen entgegenstehen. Die schutzwürdigen Belange des Betroffenen schließen beispielsweise eine Überwachung von Umkleide- oder Sanitärräumen aus, weil solche Aufnahmen den höchstpersönlichen

7 BVerwG Urteil vom 27.03.2019 Az: 6 C 2.18.

Lebensbereich oder gar Intimbereich tangieren. Ebenso ist zu berücksichtigen, dass der Beobachtungsraum nur den eigenen Verantwortungsbereich umfassen darf, also nur soweit reichen darf wie bspw. das Hausrecht oder das Eigentum reicht. So ist sicherzustellen, dass bei der Überwachung des Eingangsbereichs oder der Außenwände eines Gebäudes nicht zugleich auch der Fußweg oder die Straße überwacht wird. Zudem ist im Rahmen der Interessenabwägung zu prüfen, inwieweit tatsächlich schwenkbare Kameras zum Einsatz kommen, ob eine dauerhafte Aufzeichnung erforderlich oder diese nur in bestimmten Fällen aktiviert wird oder ob hochauflösende Bilder benötigt werden.

Sofern Arbeitsplätze überwacht werden, sind die Mitbestimmungsrechte des Betriebsrats zu beachten insb. nach § 87 Abs. 1 Nr. 6 BetrVG. Typischerweise werden die Rahmenbedingungen der Videoüberwachung im Betrieb in einer Betriebsvereinbarung vereinbArt. Gerade bei der Videoüberwachung am Arbeitsplatz ist darauf zu achten, dass neben den schon genannten Umkleide- oder Sanitärräumen auch Pausen- und Ruheräume nicht überwacht werden dürfen. Ebenso gilt im Beschäftigungsverhältnis nach wie vor, dass eine verdeckte Videoüberwachung nach einer Abwägung der Interessen grundsätzlich unzulässig sein wird und allenfalls in begründeten Ausnahmefällen in Betracht kommen wird.

Sonderfälle Gesichtserkennung und Tonaufnahmen
Sofern bei der Videoüberwachung Verfahren zur Gesichtserkennung zum Einsatz kommen, sind zusätzlich die Voraussetzungen zur Verarbeitung biometrischer Daten zu beachten (Art. 9 Abs. 1 DSGVO). Danach ist die Verwendung biometrischer Daten grundsätzlich verboten, es sei denn, eine der Ausnahmen nach Art. 9 Abs. 2 DSGVO läge vor. Hier kommt insbesondere im Kundenverhältnis die Einwilligung in Betracht. Diese muss jedoch den Anforderungen des Art. 7 DSGVO entsprechen, insbesondere ausdrücklich erklärt werden. Ein schlichtes Betreten des Beobachtungsbereichs soll nach Auffassung der Aufsichtsbehörden nicht ausreichen.

Bei Tonaufnahmen ist neben den Vorschriften der DSGVO und des BDSG noch § 201 StGB zu beachten. Dieser stellt die unbefugte Aufnahme des nicht öffentlich gesprochenen Wortes unter Strafe. Die Befugnis zur Aufnahme kann sich in aller Regel nur durch eine ausdrückliche gesetzliche Grundlage ergeben oder aus der Einwilligung des Betroffenen. Diese wird jedoch in den Situationen, in denen die Videokameras zur Überwachung

eingesetzt werden, in aller Regel nicht freiwillig erteilt werden. Zudem gilt auch hier, dass die Einwilligung ausdrücklich und informiert zu erteilen ist. Auch hier reicht also ein schlichtes Betreten oder Verweilen im Beobachtungsbereich nicht aus. Aus diesen Gründen ist in der betrieblichen Praxis von Tonaufnahmen regelmäßig abzuraten.

Speicherfrist
Grundsätzlich sind die aufgezeichneten Daten zu löschen, wenn sie nicht mehr benötigt werden. Für den klassischen Fall der Überwachung, wo es um die Beweissicherung geht, ist darauf abzustellen, wann normalerweise festgestellt werden kann, dass die Aufnahmen benötigt werden. Die Aufsichtsbehörden gehen davon aus, dass dies in aller Regel nach ein bis zwei Tagen der Fall sein wird. Eine darüberhinausgehende Speicherfrist wäre jedenfalls zu begründen. Dies kann der Fall sein bei Abstellanlagen oder Lagerflächen, die nicht jeden Tag aufgesucht werden. Dort werden zum einen etwaige Beschädigungen oder Diebstähle nicht am nächsten Werktag festgestellt, herrscht aber zum anderen aufgrund der Lage kein Publikumsverkehr, so dass im Regelfall keine Menschen gefilmt werden.

Transparenz
Nach § 4 Abs. 4 BDSG gelten die Informationspflichten nach Art. 13 und 14 DSGVO dann, wenn die erhobenen Daten einer bestimmten Person zugeordnet werden. Im Übrigen sind nach § 4 Abs. 2 BDSG die Videoüberwachung und die Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt kenntlich zu machen. Demnach würden in einem ersten Schritt wie bisher Piktogramme mit den Kontaktdaten des Verantwortlichen am Eingangsbereich eines Einkaufszentrums oder in der Einfahrt eines Parkhauses ausreichen. Sofern Bodycams zum Einsatz kommen, sollten die Träger der Kameras mit entsprechenden Kennzeichnungen an der Dienstkleidung oder Warnweste versehen werden.

Allerdings fordern die Datenschutzaufsichtsbehörden in ihrem Kurzpapier Nr. 15[8], dass daneben mindestens folgenden Angaben zu machen sind:

- Kontaktdaten des Datenschutzbeauftragten,
- Verarbeitungszwecke und Rechtsgrundlagen in Schlagworten,

8 s. hierzu auch: Datenschutzkonferenz (Hg.): Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutz-Grundverordnung. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf (abgerufen am 11.05.2022).

- Angabe des berechtigten Interesses,
- Dauer der Speicherung und
- Hinweis, wo die vollständigen Informationen abrufbar sind.

Die weiteren Informationen sind danach für den Betroffenen zur Einsicht bereitzuhalten oder auszuhängen. Demnach gehen auch die Aufsichtsbehörden davon aus, dass die Informationen nicht im ersten Schritt in aller Ausführlichkeit zur Verfügung gestellt werden können. Dies ist unter Praxiserwägungen zu begrüßen. Allerdings ist jedenfalls für bestimmte Situationen zu erwägen, ob insbesondere in Ansehung des § 4 Abs. 4 BDSG für den Betroffenen nicht ein großes Piktogramm nur mit Angabe der verantwortlichen Stelle leichter wahrnehmbar und übersichtlicher ist als ein ausführlicher Text, der in der konkreten Situation gar nicht gelesen werden kann. So ist bei einem Parkplatz oder in einem Einkaufszentrum anzunehmen, dass es dem Betroffenen in allererster Linie wichtig ist zu erkennen, dass überwacht wird und wer für die Überwachung verantwortlich ist, nicht aber die Detailinformationen zu den Kontaktdaten des Datenschutzbeauftragten oder die Angabe des berechtigten Interesses. Mit der Kennzeichnung der verantwortlichen Stelle und den Kontaktdaten ist der Betroffene ohne weiteres in der Lage, seine weitergehenden Rechte geltend zu machen. Sobald Videobilder einer konkreten natürlichen Person zugeordnet werden, greifen ohnehin die vollständigen Informationspflichten nach Art. 13 DSGVO. Eine verdeckte Videoüberwachung ist grundsätzlich unzulässig.

Datenschutz-Folgenabschätzung
Art. 35 DSGVO sieht vor, dass bei einer systematischen und umfangreichen Überwachung öffentlich zugänglicher Räume eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist. Nach Art. 35 Abs. 1 S. 2 DSGVO kann der Verantwortliche für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken eine einzige Abschätzung vornehmen. So ist es in der Praxis üblich, dass eine Supermarktkette die Videoüberwachung ihre Filialen und Parkplätze nach standardisierten Grundsätzen durchführt, so dass in diesen Fällen eine DSFA ausreichen würde.

Die Mindestinhalte einer DSFA sind in Art. 35 Abs. 7 DSGVO normiert. Der Europäische Datenschutzausschuss hat das Working Paper 248 der Art. 29 Gruppe mit den Aussagen zur Datenschutz-Folgenabschätzung

übernommen.[9] (Ergänzende Informationen zur DSFA sind im Kapitel 7.2.4 ab S. 71 zu finden.)

Checkliste Videoüberwachung:

- Zwecke festlegen (z. B. Hausrecht, Schutz vor Vandalismus, Diebstahl, Sicherheit der Beschäftigten und Kunden)
- beobachteten Bereich beschränken (z. B. auf das eigene Grundstück, Gebäude etc.)
- Keine Beobachtung von Sozial- und Sanitärraumen oder Umkleidekabinen
- Speicherfristen festlegen und nicht benötigte Aufnahmen löschen
- Zugriffsberechtigungen und Auswertungsprozess festlegen
- Prüfung, ob Datenschutz-Folgenabschätzung erforderlich ist und gegebenenfalls durchführen
- Ggf. Mitbestimmung durch Betriebsrat berücksichtigen
- Kenntlichmachung und Informationen nach Art. 13 und 14, ggf. abgestuft mit Erstinformation auf Piktogramm und vollständigen Informationen auf der Homepage oder im Ladenlokal
- Regelmäßige Überprüfung der Erforderlichkeit und Geeignetheit der Maßnahme (nicht mehr benötigte Kameras zurückbauen oder zusätzliche Kamerafunktionen durch Updates datenschutzrechtlich bewerten)

9 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP248rev.01. Oktober 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_de (abgerufen am 11.05.2022); Europäischer Datenschutzausschuss (Hg.): Empfehlung 01/2019 zu der vom Europäischen Datenschutzbeauftragten entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725). Juli 2019. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendation_201901_edps_39.4_dpia_list_de.pdf (abgerufen am 11.05.2022).

5.5 Automatisierte Entscheidungsfindung im Einzelfall einschließlich Profiling

Gemäß Art. 22 Abs. 1 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf eine automatisierte Verarbeitung gestützten Entscheidung oder Maßnahme unterworfen zu werden, die für ihr Gegenüber rechtliche Wirkung oder eine erhebliche Beeinträchtigung zur Folge hat. Als Beispiel hierfür nennt EG 71 die Ablehnung eines Online-Kreditantrags sowie Online-Einstellungs- oder Ablehnungsverfahren ohne menschliches Eingreifen. Eine automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO liegt somit immer dann vor, wenn die Entscheidung eine rechtliche Auswirkung für die betroffene Person hat oder diese sie sonst in erheblicher Weise beeinträchtigt und keine inhaltliche Bewertung und Entscheidung durch eine natürliche Person stattgefunden hat. Insbesondere aus der zweiten Variante wird unterdessen abgeleitet, dass (automatisierte) positive Entscheidungen nicht dem Verbot nach Art. 22 DSGVO unterliegen. Der nationale Gesetzgeber hatte diese bis zum Wirksamwerden der DSGVO in § 6a BDSG a. F. umgesetzt. Art. 2 Abs. 2 DSGVO regelt Ausnahmen vom vorgenannten Verbot automatisierter – negativer – Entscheidungen. Demnach gilt Art. 22 Abs. 1 DSGVO nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedsstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Ist eine automatisierte Entscheidungsfindung danach zulässig, muss der Verantwortliche in den Fällen a) und c) geeignete Maßnahmen treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Dies umfasst mindestens das Recht auf Erwirkung des Eingreifens einer Person des Verantwortlichen, auf Darlegung des eigenen Standpunkts und Anfechtung der Entscheidung.

Soll die Verarbeitung auf eine Einwilligung gestützt werden, sind die Anforderungen an die Wirksamkeit der Einwilligung zu beachten, vgl. Art. 7 DSGVO.

Zudem darf die Einbeziehung besonderer Kategorien personenbezogener Daten in eine automatisierte Entscheidungsfindung nicht ohne eine ausdrückliche Einwilligung der betroffenen Person oder eine entsprechende Erlaubnisnorm im nationalen Recht (s. auch Kap. 5.5.3, S. 40) erfolgen.

Profiling wird in Art. 4 Nr. 4 DSGVO definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten". Dies umfasst die Analyse oder Vorhersage von Aspekten bezüglich der Arbeitsleistung, wirtschaftlichen Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort und Ortswechsel.

Profilingmaßnahmen werden (nur) von Art. 22 DSGVO erfasst, wenn deren Verarbeitung in eine automatisierte Entscheidungsfindung mündet.

Die Verarbeitung personenbezogener Daten im Rahmen des Profilings richtet sich nach den allgemeinen Zulässigkeitsvoraussetzungen des Art. 6 DSGVO. Ist die Verarbeitung eines personenbezogenen Datums zulässig, steht einer Verarbeitung dieses Datums auch im Rahmen des Profilings grundsätzlich nichts entgegen. Es gilt im Rahmen der Zulässigkeit jedoch insgesamt zu berücksichtigen, dass die eingesetzten Verfahren wissenschaftlichen Grundsätzen genügen und mathematisch-statistisch valide sein müssen. Wird etwa ein kreditorisches Risiko begründet, rechtfertigt dies grundsätzlich die Durchführung eines Profilings, sowohl im vorvertraglichen Stadium als auch während der Vertragsdurchführung.

Findet Profiling auf Grundlage von Art. 6 Abs. 1 lit. e und f DSGVO statt, hat die betroffene Person nach Art. 21 Abs. 1 S. 1 DSGVO unter engen Voraussetzungen (besondere persönliche Situation) ein Widerspruchsrecht gegen die Verarbeitung. Darüber hinaus ist beim Profiling regelmäßig zu prüfen, ob gemäß Art. 35 Abs. 3 lit. a DSGVO eine Datenschutzfolgeabschätzung durch den Verantwortlichen vorzunehmen ist.

5.5.1 Scoring

Beim Scoring handelt es sich um einen Unterfall des Profilings. Mit Hilfe von Scoring kann unter Einsatz eines mathematisch-statistischen Verfahrens, auf Basis von Erfahrungen aus der Vergangenheit, die Wahrscheinlichkeit berechnet werden, mit der eine bestimmte Person ein bestimmtes Verhalten zeigen wird. Scoring kann eine Grundlage bzw. ein Bestandteil für eine automatisierte Entscheidungsfindung sein. Ist es dies nicht oder erfolgt die Entscheidung nicht (voll-)automatisiert, ist der Regelungsbereich des Art. 22 DSGVO für das Profiling selbst nicht eröffnet. Es gelten dann die allgemeinen Verarbeitungsgrundsätze nach Art. 6 Abs. 1 DSGVO sowie zusätzlich § 31 BDSG (s. ggf. auch Kap. 5.5.3, S. 40), sofern Wahrscheinlichkeitswerte für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses verwendet werden. Das VG Wiesbaden hat dem EuGH im Oktober 2021 im Rahmen eines Vorlageverfahrens auch die Tätigkeit von Wirtschaftsauskunfteien und damit die Einbeziehung von Art. 22 DSGVO und des § 31 BDSG vorgelegt (VG Wiesbaden (1.10.21, 6 K 788/20.WI). Eine entsprechende Entscheidung wird auch hier Rechtssicherheit bringen.

5.5.2 Informationspflichten und Auskunftsrecht

Im Falle einer automatisierten Entscheidungsfindung bestehen Informations- und Auskunftspflichten für den Verantwortlichen hinsichtlich der involvierten Logik, der Tragweite und angestrebten Auswirkungen der Verarbeitung. Denkbar erscheint hier die Verwendung von generischen Texten, die das eingesetzte Verfahren und die Methodik sowie die möglichen Folgen der automatisierten Entscheidungsfindung nachvollziehbar erläutern (z. B. Merkblätter). Besondere Auskunftspflichten bei Profilingmaßnahmen, die nicht Bestandteil einer automatisierten Entscheidungsfindung sind, sehen die DSGVO sowie das BDSG hingegen nicht vor. Es gelten daher – soweit anwendbar – die allgemeinen Grundsätze zur Auskunftserteilung nach Art. 15 Abs. 1 S. 1 DSGVO.

5.5.3 Nationale Regelungen zum Profiling

Mit § 31 BDSG schreibt der nationale Gesetzgeber erkennbar die bisher aus den § 28a und § 28b BDSG a. F. bekannten Grundsätze fort. Hierfür übernimmt § 31 Abs. 1 BDSG die bereits aus § 28b BDSG a. F. bekannten An-

forderungen an das Scoreverfahren. In § 31 Abs. 2 BDSG werden ferner die Voraussetzungen für eine Einbeziehung von Daten über rückständige Forderungen (§ 31 Abs. 2 S. 1 BDSG) sowie die Zulässigkeit der Verwendung von weiteren Daten nach allgemeinem Datenschutzrecht (§ 31 Abs. 2 S. 2 BDSG) geregelt. Die Vorschrift in § 31 Abs. 2 S. 1 BDSG konkretisiert die im Rahmen von Art. 6 Abs. 1 lit. f DSGVO vorzunehmende Interessenabwägung dahingehend, unter welchen Voraussetzungen Wahrscheinlichkeitswerte über ein bestimmtes zukünftiges Verhalten einer betroffenen Person, die Informationen zu rückständigen Forderungen enthalten, zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses verwendet werden dürfen. Der nationale Gesetzgeber hat gemäß Art. 22 Abs. 2 lit. b DSGVO mit § 37 BDSG zudem eine mitgliedsstaatliche Regelung für den Bereich der Versicherungswirtschaft geschaffen. Dieser erlaubt eine automatisierte Entscheidungsfindung auch unter Einbeziehung von Gesundheitsdaten, wenn diese im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht.

5.6 Besondere Datenkategorien

Besondere Datenkategorien spielen in der betrieblichen Praxis vor allem in der Arbeitsmedizin und Arbeitsschutz oder beim betrieblichen Gesundheitsmanagement eine Rolle. Aber auch Daten zum Sexualleben werden verarbeitet, wenn im Rahmen der Personaldatenverarbeitung Daten zur eingetragenen Lebenspartnerschaft bspw. für Zwecke der Hinterbliebenenversorgung verarbeitet werden. Biometrische Daten wie Fingerabdruck-, Venen- oder Irisscanner werden ebenso wie Gesichtserkennung gelegentlich für die Zugangskontrolle zu besonders sensiblen Bereichen genutzt.

Art. 9 Abs. 1 DSGVO untersagt zunächst die Verarbeitung dieser Daten grundsätzlich. Die zulässigen Ausnahmen sind in Abs. eregelt. Die in der betrieblichen Praxis wichtigsten Erlaubnistatbestände sind die Einwilligung, die sich ausdrücklich auf die beschriebenen Zwecke beziehen muss (Art. 9 Abs. 2 lit. a DSGVO), und die Verarbeitung zur Erfüllung von Pflichten aus dem Arbeits- oder Sozialrecht bzw. des Sozialschutzes, soweit dies nach dem Unionsrecht, dem nationalen Recht oder aufgrund einer Kollektivvereinbarung zulässig ist (Art. 9 Abs. 2 lit. b DSGVO). Auch zu Zwecken der Arbeitsmedizin und der Beurteilung der Arbeitsfähigkeit dürfen Gesundheitsdaten in der betrieblichen Praxis verarbeitet werden, ebenso, wenn dies für

Diagnose, Behandlung und Therapie erforderlich ist, ebenso wie für die Versorgung im Gesundheits- oder Sozialbereich (Art. 9 Abs. 2 lit. h DSGVO).

Sofern die Daten auf der Grundlage von Art. 9 Abs. 2 lit. h DSGVO verarbeitet werden dürfen sie gem. Art. 9 Abs. 3 DSGVO nur durch Fachpersonal verarbeiten werden, wenn dieses einem Berufsgeheimnis unterliegt. § 22 Abs. 1 BDSG regelt die Zulässigkeitsvoraussetzungen für den nicht öffentlichen und den öffentlichen Bereich, § 22 Abs. 2 BDSG regelt die Zulässigkeitsvoraussetzungen für den öffentlichen Bereich. § 22 Abs. 2 BDSG sieht vor, dass zum Schutz der besonderen personenbezogenen Daten geeignete Schutzmaßnahmen zu treffen sind wie insb. Verschlüsselung der Daten und Unterweisung der mit der Verarbeitung Beschäftigten.

Sofern besondere personenbezogene Daten in erheblichem Umfang verarbeitet werden, ist eine DSFA nach Art. 35 DSGVO durchzuführen. Zudem ist zu prüfen, ob bei der Einführung von Verfahren zur Verarbeitung von besonderen personenbezogenen Daten im Beschäftigungsverhältnis Mitbestimmungstatbestände des BetrVG greifen.

6. Rechte und Pflichten

6.1 Rechte der Betroffenen

Ziel der DSGVO ist es, die Rechte der Betroffenen zu stärken und ihnen so die Kontrolle über ihre eigenen Daten (zurück) zu geben (EG 7). Diesem Ziel widmet die DSGVO das Kapitel III, in dem die Rechte der Betroffenen geregelt werden. Abschnitt 1 enthält die Vorschriften zu „Transparenz und Modalitäten" (Art. 12 DSGVO), während Abschnitt 2 die Informationspflicht des Datenverarbeiters und das Recht auf Auskunft zu personenbezogenen Daten enthält (Art. 13–15 DSGVO). Abschnitt 3 regelt die Berichtigung und Löschung (Art. 16–20 DSGVO), Abschnitt 4 das Widerspruchsrecht und die automatisierte Entscheidungsfindung im Einzelfall (Art. 21, 22 DSGVO). Im Mai 2017 wurde mit dem Datenschutzanpassungs- und Umsetzungsgesetz (DSAnpUG) das BDSG neu gefasst, das einzelne Ausnahmen von den Informationspflichten vorsieht.

6.1.1 Information und Transparenz

Art. 12 DSGVO formuliert zunächst die Verpflichtung des für die Datenverarbeitung Verantwortlichen, geeignete Maßnahmen zu treffen, um die Rechte des Betroffenen auf Transparenz und Auskunft zu erfüllen. Neu ist, dass nach Art. 12 Abs. 3 DSGVO der Verantwortliche die Anträge auf Auskunft und weitergehende Informationen nach Art. 15–22 DSGVO unverzüglich, spätestens aber innerhalb eines Monats nach Eingang des Antrags zu beantworten hat. Diese Frist kann im Ausnahmefall auf zwei Monate verlängert werden. Aber auch dann ist der Betroffene innerhalb eines Monats über die Fristverlängerung zu informieren.

Alle Betroffenenrechte sind grundsätzlich unentgeltlich zu erfüllen. Nur bei offenkundig unbegründeten und exzessiv häufigen Anträgen kann der Verantwortliche ein Entgelt verlangen oder sich weigern, die Auskunft zu erteilen. Der Verantwortliche ist in diesen Fällen nachweispflichtig. Angesichts der Bedeutung der Betroffenenrechte für Transparenz und Kontrolle über die Daten sind hohe Maßstäbe an diesen Ausnahmentatbestand anzulegen.

Art. 12 DSGVO ist gleichsam wie ein Rahmen für die Erfüllung der Betroffenenrechte auf Information, Auskunft, Berichtigung und Sperrung zu lesen und bei der Auslegung der nachfolgenden Normen heranzuziehen.

Die Transparenzpflichten unterscheiden sodann, ob die Daten beim Betroffenen erhoben wurden (Art. 13 DSGVO) oder bei Dritten (Art. 14 DSGVO). Schon die EU-Datenschutzrichtlinie und das BDSG a. F. kannten den Grundsatz der Transparenz, so dass eine Informationspflicht nicht grundsätzlich neu ist. So sah das BDSG in § 4 Abs. 3 BDSG a. F. schon bislang vor, dass der Betroffene bei der Erhebung der Daten über die Identität der verantwortlichen Stelle, die Zweckbestimmung und die Empfänger bzw. die Kategorien von Empfängern informiert wird. Wurden die Daten nicht beim Betroffenen erhoben, so war er nach §§ 19a, 33 BDSG a. F. entsprechend zu informieren. Neu ist allerdings der Umfang der Informationspflicht. Neben den vorerwähnten Informationspflichten ist der Betroffene in beiden Fällen insbesondere auch über eine beabsichtigte Datenübermittlung in Drittstaaten zu informieren sowie über das Vorhandensein eines Angemessenheitsbeschlusses oder soweit einschlägig über die geeigneten oder angemessenen Garantien sowie die Möglichkeit, eine Kopie dieser zu erhalten (Art. 13 Abs. 1f, 14 Abs. 1f DSGVO). Weitere Informationspflichten betreffen die Speicherdauer, das Recht auf Auskunft, Berichtigung oder Löschung, das Recht auf Widerruf der Einwilligung sowie das Recht, Beschwerde bei der Aufsichtsbehörde einzulegen. Auch auf eine automatisierte Entscheidungsfindung nach Art. 22 DSGVO ist der Betroffene unaufgefordert hinzuweisen. Es ist also erforderlich, die bisher bereitgehaltenen Informationen im Internet oder auf Formularen zu ergänzen und zu aktualisieren. Ggf. ist schon bei der Dokumentation der betroffenen IT-Systeme und Prozesse darauf zu achten, die Informationen bereitstellen zu können. So kann es erforderlich sein, die Dokumentation um ein Löschkonzept zu ergänzen, um über die Speicherfristen respektive die Kriterien zur Ermittlung der Speicherfristen informieren zu können.

Etwas versteckt findet sich in Art. 21 DSGVO die Verpflichtung, den Betroffenen, spätestens bei der ersten Kommunikation mit ihm, auf sein Widerspruchsrecht hinzuweisen. Der Betroffene kann der Verarbeitung der ihn betreffenden personenbezogenen Daten an sich widersprechen (Art. 21 Abs. 1 DSGVO), wenn diese auf der Basis einer Interessenab-

wägung (Art. 6 Abs. 1 f DSGVO) oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erfolgt (Art. 6 Abs. 1 e DSGVO), und zum anderen bei Verwendung seiner Daten zu Werbezwecken (Art. 6 Abs. 2 DSGVO).[10]

> **Wichtig:** Die Informationspflichten gelten immer, wenn Daten nicht nur zu ausschließlich privaten Zwecken verarbeitet werden. Also müssen auch kleinere Unternehmen, selbständige Freiberufler, Behörden oder auch Vereine die Informationspflichten erfüllen. Und die Informationspflichten gelten nicht nur für den Onlinebereich, sondern auch für den Offlinebereich. Bestehende Datenschutzhinweise auf Webseiten sind daher zu ergänzen.

6.1.1.1 Direkterhebung beim Betroffenen

Nach Art. 13 DSGVO muss bei einer Direkterhebung beim Betroffenen über folgende Inhalte informiert werden (Mindestumfang):

- Namen und Kontaktdaten des Verantwortlichen,
- ggf. Kontaktdaten des Datenschutzbeauftragten,
- Art und Umfang der Datenverarbeitung,
- Zwecke der Datenverarbeitung (vollständig, spätere Zweckänderung nur schwer möglich),
- Rechtsgrundlage der Datenverarbeitung (berechtigtes Interesse, Einwilligung, sonstige),
- ggf. Empfänger bzw. Kategorien von Empfänger (Diensteanbieter),
- ggf. Absicht der Datenübermittlung ins Ausland,
- Information über das Datenschutzniveau im Ausland,
- Information über Maßnahmen zur Sicherstellung des Datenschutzniveaus,
- ggf. Garantien (z. B. Standarddatenschutzklauseln) zur Verfügung stellen,
- Angabe des Stands der Datenschutzerklärung,
- Dauer der Datenspeicherung bzw. die zugrundliegenden Kriterien,

10 s. hierzu auch: Landesbeauftragte für Datenschutz- und Informationsfreiheit Nordrhein-Westfalen (Hg.): Information über die Erhebung von personenbezogenen Daten nach Art. 13, 14 und 21 Datenschutz-Grundverordnung Umsetzungshilfe zu den Datenschutzhinweisen. Januar 2022. Online: https://www.ldi.nrw.de/system/files/media/document/file/ldi_nrw_-_umsetzungshilfe_datenschutzinformation_2022-01.pdf (abgerufen am 11.05.2022); Europäischer Datenschutzausschuss (Hg.): Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP260rev.01. April 2018. Online: https://ec.europa.eu/newsroom/article29/items/622227 (abgerufen am 11.05.2022).

- Betroffenenrechte (allgemein),
- Recht auf Datenübertragbarkeit,
- Widerspruchsrecht insbesondere bei Datenverarbeitung aufgrund berechtigten Interesses,
- Widerspruchrecht nach Art. 21 DSGVO, insbesondere bei Direktwerbung,
- Recht zum Widerruf einer Einwilligung,
- Beschwerderecht bei Aufsichtsbehörden,
- Erforderlichkeit der Datenverarbeitung und Information über die Folgen einer Nicht-Bereitstellung,
- Information über das Bestehen einer automatisierten Einzelentscheidung inkl. Profiling und die Logik und Tragweite der Datenverarbeitung.

> **Hinweis:** Bei einer Zweckänderung besteht eine Informationspflicht vor der weiteren Verwertung der Daten.

6.1.1.2 Dritterhebung

Nach Art. 14 DSGVO muss bei einer Datenerhebung durch Dritte über folgende Inhalte informiert werden (Mindestumfang):

- Punkte, die unter Art. 13 DSGVO Direkterhebung beim Betroffenen genannt wurden,
- Quelle der Daten.

> **Hinweis:** Bei einer Zweckänderung besteht eine Informationspflicht vor der weiteren Verwertung der Daten.

1. **Einleitung, u. U. mit Glossar, Begriffsbestimmungen**

   Beschreibung der wichtigsten Prozesse (Kernprozesse Vertrieb, Vertragsabwicklung, Beschäftigungsverhältnis)

2. **Verantwortlicher für die Datenverarbeitung und Datenschutzbeauftragter (falls vorhanden) und Vertreter in der Union (bei außereuropäischen Anbietern ohne Niederlassung in der EU, vgl. Art. 27 DSGVO)**

   Kontaktdaten Verantwortlicher/Datenschutzbeauftragter

3. **Wann erhebt und verarbeitet [der Verantwortliche] personenbezogene Daten?**

   - Art und Umfang der Datenverarbeitung
   - Zwecke und Rechtsgrundlagen der Datenverarbeitung
   - Erforderlichkeit der Datenverarbeitung und Information über die Folgen einer Nicht-Bereitstellung
   - Information über das Bestehen einer automatisierten Einzelentscheidung inkl. Profiling und die Logik und Tragweite der Datenverarbeitung

4. **Wann werden Ihre Daten gelöscht?**

   Dauer der Speicherung respektive Kriterien zur Ermittlung der Speicherfrist (können unterschiedlich sein von wenigen Tagen bis zu 30 Jahren und mehr)

5. Welche Rechte haben Kunden/Beschäftigte?

Hinweis auf Betroffenenrechte:

- Recht auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung (Sperrung)
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht bei Datenverarbeitung aufgrund berechtigen Interesses
- Widerspruchsrecht bei Direktwerbung
- Recht auf Widerruf der Einwilligung
- Beschwerderecht bei Aufsichtsbehörde (ggf. Hinweis auf die für das Unternehmen zuständige Aufsichtsbehörde)

6. Werden Daten weitergegeben?

- Empfänger bzw. Kategorien von Empfängern (nicht nur Dritte, auch Dienstleister wie Druck- und IT-Dienstleister, interne Dienstleister, insb. Shared Services im Konzern)
- ggf. Absicht der Datenübermittlung ins Ausland
- Information über Datenschutzniveau im Ausland
- Information über Maßnahmen zur Sicherstellung des Datenschutzniveaus
- ggf. Verweis auf Garantien z. B. Standarddatenschutzklauseln

7. Wann werden Cookies eingesetzt?

Welche Cookies werden zu welchem Zweck eingesetzt?

8. Stand der Datenschutzhinweise

Angabe des Stands der Datenschutzerklärung

6.1.1.4 Ausnahmen nach DSGVO und BDSG

Die DSGVO formuliert bei der Direkterhebung nur eine Ausnahme: Die Informationspflicht entfällt, wenn und soweit der Betroffene über die Informationen verfügt (Art. 13 Abs. 4 DSGVO).

Bei der Erhebung bei Dritten kommen zu dieser Ausnahme noch weitere, folgende Ausnahmetatbestände hinzu (Art. 14 Abs. 5 DSGVO):

- wenn sich die Erteilung der Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde (als Beispiele werden genannt Archiv- oder Forschungszwecke oder statistische Zwecke),
- die Erlangung oder Offenlegung der Daten durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, geregelt sind und die berechtigten Interessen der Betroffenen durch geeignete Maßnahmen gewahrt sind,
- die personenbezogenen Daten einem Berufsgeheimnis oder anderen Geheimhaltungspflicht unterliegen und vertraulich behandelt werden müssen.

Weitere Ausnahmen formuliert das Bundesdatenschutzgesetz in § 29 Abs. 1 und 2 sowie §§ 32, und 33 BDSG. § 29 BDSG regelt die Rechte des Betroffenen bei besonderen Geheimhaltungspflichten, insbesondere bei Berufsgeheimnisträgern. Nach § 29 Abs. 1 BDSG besteht die Informationspflicht bei der Datenerhebung bei Dritten nicht, wenn dadurch Informationen, die ihrem Wesen nach geheim gehalten werden müssen, offenbart würden. Für den Fall der Direkterhebung sieht § 29 Abs. 2 BDSG vor, dass die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Art. 13 Abs. 3 DSGVO (Information über Weiterverarbeitung) nicht besteht, wenn die Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt werden, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt. § 32 BDSG regelt die Ausnahmen bei der Direkterhebung, während § 33 BDSG die Ausnahmen bei der Erhebung bei Dritten regelt. Allerdings regeln diese Vorschriften nur die Ausnahmen hinsichtlich der Informationspflicht bei der Weiterverarbeitung nach Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 DSGVO. Hinsichtlich der Eingangsinformation für die ursprünglichen Zwecke sind keine weiteren Ausnahmen vorgesehen. Wenn sich der Verantwortliche auf die Ausnahmen nach § 32 oder 33 BDSG beruft, so hat er geeignete Maß-

nahmen zum Schutz der berechtigten Interessen der betroffenen Person zu ergreifen. Dies schließt ein, die in Art. 13 Abs. 1 und 2 DSGVO genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Der Verantwortliche hat zudem schriftlich festzuhalten, aus welchen Gründen er von einer Information abgesehen hat. Im Ergebnis sind die Ausnahmetatbestände im Regelfall nicht einschlägig und sollen daher in dieser Broschüre nicht betrachtet werden.

6.1.1.5 Umsetzungshinweise

Für die Umsetzung ist zunächst zu prüfen, an welchen Kundenschnittstellen personenbezogene Daten erhoben werden und wie dort die Informationspflichten umgesetzt werden können. Inzwischen unterhält jedes Unternehmen oder jede Behörde eine eigene Webseite zur Information der Öffentlichkeit. Auf Webseiten haben sich schon heute Datenschutzhinweise nach § 13 Abs. 1 TMG etabliert. Dort können auch die vollständigen Hinweise nach Art. 13, 14 DSGVO hinterlegt werden. Aber auch in den Verkaufsstellen können Informationsblätter bereitgehalten werden oder gut sichtbare Hinweise auf die Informationen auf der Internetseite angebracht werden (QR-Code, URL etc.). Schwieriger scheint die Umsetzung bei telefonischen oder mobilen Angeboten, bei denen der Kundenkontakt entweder nur mündlich stattfindet oder aber die Möglichkeit der Kenntnisnahme durch ein kleines Smartphone-Display eingeschränkt ist. In diesen Fällen ist es auch mit Blick auf das Working Paper 260 zu den Anforderungen der Transparenz in der DSGVO der Art. 29 Gruppe, die durch den Europäischen Datenschutzausschuss übernommen wurde, jedoch vertretbar, zwischen denjenigen Informationen zu unterscheiden, die im Moment der Datenerhebung unmittelbar erforderlich sind für die Entscheidung, ob und welche Daten preisgegeben werden sollen, und denjenigen Informationen, die für den Betroffenen aller Voraussicht nach zu einem späteren Zeitpunkt relevant werden.[11] Dieser Medienbruch wird seitens der Datenschutzaufsichtsbehörden als vertretbar erachtet. So wird die Information über die Kontaktdaten des Datenschutzbeauftragten sowie der Hinweise auf die Betroffenenrechte regelmäßig erst dann erforderlich sein, wenn der Betroffene auch tatsächlich seine Rechte ausüben möchte. In der Praxis also könnten die unmittelbar wesentlichen Informationen in aller Kürze mitgeteilt werden und die ergänzenden

11 s. Europäischer Datenschutzausschuss (Hg.): Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP260rev.01. April 2018. Online: https://ec.europa.eu/newsroom/article29/items/622227 (abgerufen am 11.05.2022).

Informationen auf einer öffentlich zugänglichen Webseite bereitgestellt werden. Mit einem solchen abgestuften Verfahren könnte einerseits die notwendige Transparenz im Moment der Entscheidung über die Datenpreisgabe hergestellt werden. Andererseits würde der Betroffene nicht mit einer Flut von Informationen „überschüttet", die er jedenfalls in dem Moment aller Voraussicht nach gar nicht benötigt. Schon heute werden Datenschutzhinweise häufig als zu lang und zu unübersichtlich empfunden, so dass eine Vielzahl gerade von online- und mobile-Nutzern die Datenschutzhinweise schlicht „wegklickt", weil Schnelligkeit und Komfort im Vordergrund stehen. Dem Anliegen dieser Kunden könnte ein abgestuftes Verfahren durchaus gerecht werden, ohne denjenigen Kunden, die an einer vollständigen Information interessiert sind, die weiter gehenden gesetzlichen Informationen vorzuenthalten. Die Informationspflichten gelten auch für den Offline-Kontakt, müssen also auch in der konkreten Situation erfüllt werden können, in der z. B. im Laden oder an einem Serviceschalter personenbezogene Daten erhoben werden. Daher empfiehlt es sich, für solche Situationen Merkblätter mit den Informationen bereit zu halten.

6.1.2 Auskunft

Das Recht auf Auskunft gehört schon im geltenden Recht zu den unabdingbaren Betroffenenrechten und dient dem Betroffenen insbesondere dazu, seine weitergehenden Rechte auf Berichtigung und Löschung geltend zu machen (§§ 34, 35 BDSG). Neu ist mit Blick auf den Auskunftsanspruch, dass der Betroffene einen Anspruch auf eine Kopie seiner personenbezogenen Daten hat (Art. 15 Abs. 3 DSGVO), wobei das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf (Art. 15 Abs. 4 DSGVO). Der Begriff der Kopie ist weder in den EG noch im Text der DSGVO näher definiert, so dass nach allgemeinem Sprachgebrauch davon auszugehen ist, dass eine Abschrift ausreicht. Nicht erforderlich wäre nach diesem Verständnis ein vollständiger Datenbankabzug. IT-Systeme sind demzufolge dahingehend zu prüfen, ob die Herausgabe einer Kopie der personenbezogenen Daten möglich ist, ohne die Rechte anderer zu beeinträchtigen. Allerdings ist die Rechtsprechung dazu nicht einheitlich, so dass derzeit mehrere Vorlageverfahren bei dem EuGH anhängig sind, wie weit der Auskunftsanspruch an sich und insbesondere hinsichtlich der Kopie der personenbezogenen Daten zu fassen ist.

Beispiel: In einem CRM-System sind die Daten des Kunden ebenso wie die Daten der bearbeitenden Mitarbeiter enthalten. Eine Kopie aus dem CRM-System könnte die Rechte der Mitarbeiter beeinträchtigen. In diesem Fall könnte die Kopie in einer Abschrift der nur den Kunden betreffenden Daten bestehen. Ebenso ist zu prüfen, welche Maßnahmen erforderlich sind, um die Auskunft elektronisch erteilen zu können. Dabei wird es wichtig sein, auch in der elektronischen Kommunikation den Betroffenen eindeutig zu identifizieren und einen unbefugten Zugriff auf die Kommunikation zu vermeiden.

Zusammen mit der Auskunft sind dem Betroffenen zudem noch folgende Informationen zur Verfügung zu stellen:

- Verarbeitungszwecke,
- Kategorien der verarbeiteten Daten,
- Empfänger oder Kategorien von Empfängern, insb. bei Empfängern in Drittländern,
- geplante Speicherdauer,
- Recht auf Berichtigung, Löschung, Sperrung (Einschränkung der Verarbeitung) und Widerspruch,
- Recht zur Beschwerde bei einer Aufsichtsbehörde,
- Herkunft der Daten, sofern sie nicht beim Betroffenen erhoben wurden,
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling.

Sofern Daten in ein Drittland transferiert werden, hat der Betroffene das Recht, über die geeigneten Garantien nach Art. 46 DSGVO unterrichtet zu werden (Art. 15 Abs. 2 DSGVO). Nach Art. 15 Abs. 3 DSGVO kann der Betroffene eine Kopie der gespeicherten Daten verlangen, wobei die erste Kopie kostenlos ist. Für weitere Kopien kann der Verantwortliche ein angemessenes Entgelt auf der Basis der Verwaltungskosten verlangen. Unter Praxis- und Wirtschaftlichkeitsgesichtspunkten ist zu prüfen, in welchem Verhältnis der Aufwand zur Geltendmachung des Entgelts zum Entgelt selbst steht. Form und Frist zur Auskunftserteilung sind in Art. 12 DSGVO geregelt. Danach sind die Auskünfte schriftlich, elektronisch oder auf Wunsch des Betroffenen mündlich zu erteilen, letzteres jedoch nur, wenn die Identität des Betroffenen auf andere Weise nachgewiesen wurde (Art. 12 Abs. 1 DSGVO).

Da nunmehr ausdrücklich eine verbindliche Frist zur Beantwortung von Datenschutzanliegen formuliert ist (1 Monat, § 12 Abs. 3 DSGVO), sind die Prozesse im Kundenservice daraufhin zu prüfen, ob die eingehenden Kundenanliegen fristgerecht beantwortet werden können. Hierzu empfiehlt es sich je nach Anzahl der Kundenanliegen, Experten oder Expertenteams zu benennen, die Auskunftsersuchen fachgerecht beantworten. In größeren, verzweigten Unternehmen kann hierzu auch die Recherche gehören, in welchen Unternehmensteilen personenbezogene Daten gespeichert werden.[12]

Ähnliche Prozesse sollten in der Personalabteilung etabliert werden, da auch die Beschäftigten eines Unternehmens Anspruch auf Auskunft haben.

Die Konferenz der Datenschutzaufsichtsbehörden hat unterdessen ein Kurzpapier zu den Auskunftsrechten veröffentlicht. Darin weisen sie darauf hin, dass auch eine Negativauskunft zu erteilen ist, wenn keine Daten zu dem Betroffenen gespeichert sind.[13]

Art. 15 DSGVO sieht keine Ausnahmen von der Auskunftspflicht vor. Dagegen sieht das BDSG Ausnahmen vor für die Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (§ 27 BDSG), für Verarbeitungen zu im öffentlichen Interesse liegenden Archivzwecken (§ 28 BDSG) sowie für bestimmte Geheimhaltungspflichten und Berufsgeheimnisträger (§ 29 BSDG). Diese sind im Regelfall für die typische Geschäftstätigkeit eines Unternehmens nicht relevant und sollen hier nicht weiter betrachtet werden.[14]

Demgegenüber ist die Ausnahmeregelung des § 34 Abs. 1 Nr. 2 BDSG durchaus relevant. Denn danach entfällt die Auskunftspflicht, wenn die Daten ausschließlich für gesetzliche oder satzungsmäßige Aufbewahrungsfristen oder zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert werden und die Auskunftserteilung einen unverhältnismäßig hohen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische oder organisatorische Maßnahmen

12 Vgl. aber hierzu die Ausführungen des Hessischen Beauftragten für den Datenschutz und die Informationsfreiheit: Auskunftsersuchen müssen grundsätzlich an die verantwortliche Stelle gerichtet werden und nicht pauschal an den Konzerndatenschutzbeauftragten, wenn in der Konzernleitung typischerweise keine Daten gespeichert werden.

13 s. hierzu auch, u. a. für ergänzende Hinweise zum Auskunftsrecht der betroffenen Person: Datenschutzkonferenz (Hg.): Kurzpapier Nr. 6. Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf (abgerufen am 11.05.2022).

14 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP260rev.01. April 2018. Online: https://ec.europa.eu/newsroom/article29/items/622227 (abgerufen am 11.05.2022).

ausgeschlossen ist. In jedem Fall sind die Gründe der Auskunftsverweigerung zu dokumentieren und gegenüber dem Betroffenen zu begründen.

6.1.3 Datenübertragbarkeit

Tatsächlich neu ist das Recht auf Datenübertragbarkeit (Art. 20 DSGVO), wonach der Betroffene verlangen kann, die von ihm auf der Basis einer Einwilligung oder eines Vertrags zur Verfügung gestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Insoweit betrifft das Recht auf Datenübertragbarkeit anders als das Auskunftsrecht nicht alle Daten einer natürlichen Person sondern nur diejenigen, die auf der Basis einer Einwilligung oder zur Erfüllung eines Vertrages verarbeitet werden. Ziel dieser Regelung ist es, insbesondere bei der Nutzung sozialer Netzwerke so genannte Lock In-Effekte zu vermeiden, also den Wechsel von einem sozialen Netzwerk zum anderen zu erleichtern. In den anderen Fällen, insbesondere in den Fällen, in denen die Datenverarbeitung auf der Basis der Interessenabwägung erfolgt, besteht der Anspruch nicht.

Der Betroffene kann verlangen, die Daten direkt von einem zum anderen Verantwortlichen zu übermitteln, soweit dies technisch machbar ist (Art. 20 Abs. 2 DSGVO).

Gemäß EG 68 sollen Anbieter aber nicht verpflichtet sein, zum Zwecke der Datenportabilität kompatible Systeme zu unterhalten. Daraus folgt auch, dass der neue Anbieter als potenzieller Datenempfänger nicht verpflichtet ist, die Daten entgegenzunehmen und in seine Systeme zu übernehmen.

Auch dieses Recht auf Datenübertragbarkeit darf Rechte und Freiheiten anderer Personen nicht beeinträchtigen (Art. 20 Abs. 4 DSGVO).

Der Anspruch auf Datenübertragbarkeit richtet sich erkennbar an die Anbieter sozialer Netzwerke, um den Wechsel von einem zum anderen Netzwerk zu erleichtern. Dem Wortlaut nach gilt es aber für alle Anbieter und sowohl mit Blick auf Kundendaten als auch auf Beschäftigtendaten. Im Rahmen des Beschäftigungsverhältnisses sind aber nur wenige praktisch relevante Anwendungsfälle denkbar. Daher erscheint es vertretbar, insbesondere dort zunächst auf vollautomatische Schnittstellen zu verzichten und die Portabilitätswünsche in einem manuellen Prozess zu erfüllen.

Gleichwohl sollten diejenigen Prozesse identifiziert und geprüft werden, die in den Anwendungsbereich fallen könnten (Bonusprogramme, Bewerbungsprozesse etc.), um entsprechende Anliegen von Kunden oder Beschäftigten innerhalb der Frist von einem Monat beantworten zu können.

6.1.4 Weitere Betroffenenrechte

Das Recht auf Löschung wurde in der Überschrift ergänzt um den Zusatz „Recht auf Vergessenwerden". Diese Ergänzung bezieht sich auf Art. 17 Abs. 2 DSGVO, wonach der Verantwortliche, der die Daten öffentlich gemacht hat, angemessene Maßnahmen zu treffen hat, um die Empfänger über das Löschungsbegehren zu informieren. Diese Regelung ist erkennbar auf soziale Netzwerke und vergleichbare Internetdienste gerichtet, deren Geschäftsmodell die Veröffentlichung personenbezogener Daten ist. Dennoch war eine solche Benachrichtigung der Empfänger bei Berichtigung, Löschung oder Sperrung schon nach bisherigem Recht vorgesehen (§§ 20 Abs. 8, 35 Abs. 7 BDSG a. F.).

Das Widerspruchsrecht (Art. 21 Abs. 1 DSGVO) gibt dem Betroffenen das Recht, der weiteren Verarbeitung seiner Daten zu widersprechen, wenn die Datenverarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist oder in Ausübung einer dem Verantwortlichen übertragenen öffentlichen Gewalt erfolgt (Art. 6e) oder auf einem berechtigten Interesse des Verarbeiters beruht (Art. 6 Abs. 1 lit. f DSGVO). Auch dieses Instrument ist grundsätzlich nicht neu (§§ 20 Abs. 5, 35 Abs. 5 BDSG a. F.). Allerdings ist neu, dass der Verantwortliche künftig „zwingende Gründe" nachweisen muss, die die Interessen des Betroffenen überwiegen. Insofern empfiehlt es sich, insbesondere bei einer auf die Interessenabwägung gestützten Verarbeitung die Gründe bereits zu Beginn der Datenverarbeitung nachvollziehbar zu dokumentieren, ggf. im Zeitverlauf zu aktualisieren und zum Nachweis bereitzuhalten. Neu ist auch, dass der Betroffene auf sein Widerspruchsrecht hinzuweisen ist und der Hinweis verständlich und von anderen Informationen getrennt zu erfolgen hat (Art. 20 Abs. 4 DSGVO).

Art. 22 DSGVO regelt die automatisierte Entscheidungsfindung. Die Regelung erinnert im Kern an § 6a BDSG a. F., der schon bisher ein Verbot der automatisierten Einzelentscheidung beinhaltete. Wie schon bis-

her muss sichergestellt sein, dass der Betroffene seinen Standpunkt geltend machen kann und ein manuelles Eingreifen möglich ist (Art. 22 Abs. 3 DSGVO). Die Transparenzpflichten nach Art. 13 und 14 DSGVO sowie die Auskunftspflicht nach Art. 15 DSGVO sehen entsprechende Informationspflichten im Hinblick auf die involvierte Logik und Tragweite und die angestrebten Auswirkungen einer automatisierten Entscheidungsfindung vor.

6.1.5 Fazit

Schon heute gelten Informationspflichten und Auskunftsrechte. Neu ist allerdings der Umfang der unaufgeforderten Information an den Betroffenen, so dass die bestehenden Informationsmedien auf ihre Vollständigkeit hin zu prüfen sind. Neu ist auch, dass der Verantwortliche im Rahmen seines Datenschutzmanagements nachweisen muss, dass er geeignete Maßnahmen getroffen hat, um die Rechte der Betroffenen zu gewährleisten. Daher empfiehlt es sich, im Rahmen einer Richtlinie oder eines Handbuchs beispielsweise für den Kundenkontakt oder die Personaldatenverarbeitung Prozesse und Ansprechpartner zu definieren. Ferner kann es sinnvoll sein, die nach Art. 13 und 14 DSGVO erforderlichen Informationen gut verständlich in den eigenen Internetauftritt zu integrieren. Für die Kundenkontakte im Laden oder an einem Serviceschalter sollten ebenfalls für etwaige Nachfragen Informationsblätter bereitgehalten werden. Und nicht zuletzt kann es erforderlich sein, die Dokumentation der IT-Systeme und die Prozesse zur Bearbeitung von Kundenanliegen dahingehend zu prüfen und ggf. zu ergänzen, dass die erforderlichen Auskünfte fristgerecht und vollständig erteilt werden können.

6.2 Pflichten der Datenverarbeiter

Die EU-DSGVO erlegt den für die Datenverarbeitung Verantwortlichen eine Vielzahl von Pflichten auf, die teilweise schon nach altem Recht zu beachten waren, zum Teil aber durch die DSGVO auch erst neu geschaffen wurden. Dazu zählen in erster Linie die in Abschnitt 2 der DSGVO kodifizierten Informationspflichten des Datenverarbeiters (Art. 13 und 14 DSGVO). Darüber hinaus gibt es aber eine ganze Reihe weiterer Pflichten, die von den Verantwortlichen zu erfüllen sind. Als für die Praxis relevant

sind in diesem Zusammenhang u. a. zu nennen die Vorschriften zur Auftragsverarbeitung (Art. 28 DSGVO, s. auch Kap. 6.2.3, S. 60), zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (s. auch Kap. 6.2.4.3, S. 62), zur Durchführung von Datenschutz-Folgeabschätzungen (s. auch Kap. 6.2.4.6, S. 64 f.) und zur Bestellung von betrieblichen Datenschutzbeauftragten (s. auch Kap. 6.2.4.7, S. 65).[15]

6.2.1 Informationspflichten

Die neuen Informationspflichten, die in Kapitel 6.1.1 „Information und Transparenz" erläutert wurden, richten sich danach, ob die Daten beim Betroffenen selbst (Art. 13 DSGVO) oder bei einem Dritten (Art. 14 DSGVO) erhoben werden. Die dem Betroffenen zu gebenden Informationen sind zwar in beiden Fällen größtenteils identisch, unterscheiden sich aber in Nuancen, die sich aus der jeweils zugrundeliegenden Situation ergeben. So besteht etwa bei der Erhebung von Daten über den Betroffenen bei Dritten die Pflicht, ihn über die Quellen der Daten zu informieren. Eine solche Informationspflicht kann es bei der Ersterhebung von Daten beim Betroffenen selbst naturgemäß gar nicht geben, so dass die entsprechende Pflicht zwar im Katalog des Art. 14 DSGVO, nicht aber in demjenigen des Art. 13 DSGVO aufgeführt ist.

Schließlich schreibt die DSGVO dem Datenverantwortlichen ausdrücklich vor, wie die Informationen dem Betroffenen zu übermitteln sind: Danach sind die Informationspflichten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfüllen. Für die Übermittlung der verschiedenen Information und Auskünfte gelten unterschiedliche Zeitpunkte und Fristen. Der Informationspflicht nach Art. 13 DSGVO (Erhebung beim Betroffenen) muss der Datenverarbeiter grundsätzlich zum Zeitpunkt der Erhebung der Daten nachkommen. Die Informationen nach Art. 14 DSGVO (Erhebung bei Dritten) müssen dagegen innerhalb eines Monats nach Erlangung der Daten, spätestens jedoch zum Zeitpunkt der ersten Offenlegung gegeben werden (Art. 14 Abs. 3 a–c DSGVO).

15 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), WP243rev.01. April 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_de (abgerufen am 11.05.2022).

Besondere Schwierigkeiten ergeben sich bei der durch die DSGVO neu eingeführten Informationspflicht im Falle mündlicher oder telefonischer Datenerhebung. Bei einem Gespräch mit einem potenziellen Kunden, in dessen Verlauf naturgemäß Name und ggf. Anschrift notiert werden, müsste grundsätzlich noch während dieses Gesprächs auf die Pflicht zur Erteilung bestimmter Informationen hingewiesen und dem Gesprächspartner mündlich zur Kenntnis gebracht werden. Es liegt auf der Hand, dass dies regelmäßig zu Unverständnis bzw. problematischen Situationen führen dürfte und in der Praxis nicht handhabbar ist. In solchen Fällen reicht es daher aus, wenn dem Gesprächspartner/Angerufenen angeboten wird, ihm im Anschluss an das Gespräch/Telefonat den Informationstext per Post, Fax oder E-Mail zu übermitteln oder sich den Text auf der jeweiligen Internetseite anzusehen. Natürlich kann der Informationsempfänger auch erklären, dass er auf die Informationen, zu deren Erteilung der Datenverarbeiter verpflichtet ist, verzichtet.

Wichtig ist in jedem Fall, dass die Erfüllung dieser Informationspflicht im System des für die Datenverarbeitung Verantwortlichen dokumentiert wird. Diese Dokumentation ist notwendig, damit der Datenverarbeiter im Falle einer Datenschutzprüfung durch die Aufsichtsbehörden jederzeit nachweisen kann, was wann von wem wie gemacht wurde.

Die Informationspflicht bei der Erhebung von Daten über den Betroffenen bei Dritten ist dagegen grundsätzlich nicht neu; sie entspricht im Wesentlichen der bisherigen Benachrichtigungspflicht nach § 33 BDSG a. F. Geändert hat sich lediglich der Umfang der zu gebenden Informationen.

Stellt der Betroffene einen Antrag auf Erteilung einer Auskunft über die zu seiner Person gespeicherten Daten elektronisch, so sind ihm die Informationen grundsätzlich ebenfalls in einem gängigen elektronischen Format zur Verfügung zu stellen. Da die elektronische Übermittlung von derartigen Auskünften an Betroffene aus Sicht der Aufsichtsbehörden allerdings in bestimmten Situationen – etwa im Falle fehlender Verschlüsselung – unsicher ist, muss jeweils geprüft werden, ob diese Verpflichtung im konkreten Fall tatsächlich eingehalten werden kann.

Ausnahmen von den Informationspflichten ergeben sich wiederum zum einen aus den Bestimmungen der DSGVO selbst, zum anderen aber auch aus §§ 32 und 33 BDSG.

6.2.2 Löschpflichten

Beim Recht auf Löschung (Art. 17, 21 DSGVO) handelt es sich um die in den letzten Jahren vielfach unter dem Schlagwort „Recht auf Vergessenwerden" diskutierte Regelung. Inhaltlich entspricht die Bestimmung dem in den Grundzügen auch schon im BDSG a. F. verankerten Löschungsanspruch.

Hinzu gekommen ist durch die DSGVO jedoch die Möglichkeit des Betroffenen, allein aufgrund eines gegen die Verarbeitung seiner Daten eingelegten Widerspruchs die Löschung seiner Daten verlangen zu können, so dass der Widerspruch nach dem Konzept der DSGVO grundsätzlich zu einer Löschverpflichtung des Datenverarbeiters führen soll. Der Löschungsanspruch aufgrund eines Widerspruchs greift allerdings nur dann, wenn der Betroffene sich in einer besonderen persönlichen Situation befindet und der Verantwortliche keine zwingenden schutzwürdigen Gründe für die Verarbeitung der Daten nachweisen kann, welche die Interessen, Rechte und Freiheiten des Betroffenen überwiegen. In einem solchen Fall findet also wie schon nach dem BDSG a. F. eine Interessenabwägung statt, deren Ergebnis in der Regel gegen eine Löschung sprechen wird.

Problematisch ist es für manche Branchen, dass die DSGVO – im Gegensatz zum BDSG a. F. – keine festen Speicher- und Löschfristen mehr vorsieht. Gespeicherte Daten sind nach der DSGVO vielmehr zukünftig dann zu löschen, „wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind". Darüber, wann dies der Fall ist, lässt sich im Einzelfall natürlich trefflich streiten.

Auf das Vorhandensein klar definierter Löschfristen sind etwa die Auskunfteien angewiesen, die im Rahmen ihrer Tätigkeit zwangsläufig eine Vielzahl von Negativmerkmalen wie fällige offene Forderungen oder Insolvenzverfahren speichern. Da es sich insoweit um ein „Massengeschäft" handelt, das sich einer Einzelfallbearbeitung entzieht, ist es für das Geschäft der Auskunfteien unabdingbar, sich bei der Verarbeitung der von ihnen gespeicherten Daten auf ein rechtssicheres Löschkonzept stützen zu können. Für eine Möglichkeit zur Festlegung von Regellöschfristen spricht auch EG 39, der bestimmt, dass der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfung der Erforderlichkeit zur weiteren Speicherung vorsehen sollte. Demgemäß hat der Verband „Die

Wirtschaftsauskunfteien“ einen „Code of Conduct“ (CoC) im Sinne des Art. 40 DSGVO verabschiedet, der im Sinne einer praxisgerechten Handhabung der Löschverpflichtung im Wesentlichen eine Fortschreibung der bisherigen Speicher- und Löschpraxis des BDSG a. F. beinhaltet. Die zuständige Datenschutzaufsichtsbehörde NRW hat den CoC durch Bescheid vom 25.05.2018 genehmigt, so dass in diesem Bereich die notwendige Rechtssicherheit in Bezug auf die Löschpflichten hergestellt ist. Allerdings ist dabei zu beachten, dass auch Festlegungen in Verhaltensregeln einer gerichtlichen Kontrolle unterworfen sind.

6.2.3 Auftragsverarbeitung

Das Rechtsinstitut der Auftragsdatenverarbeitung, das nach der DSGVO zukünftig nur noch als „Auftragsverarbeitung“ betitelt wird, bleibt weiterhin erhalten. Wie schon bisher sind Auftraggeber und Auftragnehmer im Falle des Vorliegens eines Auftragsverarbeitungsverhältnisses verpflichtet, einen schriftlichen Vertrag abzuschließen, der bestimmte gesetzliche Voraussetzungen erfüllen muss. Diese Voraussetzungen werden in Art. 28 DSGVO aufgelistet und entsprechen im Wesentlichen dem, was auch schon im BDSG a. F. gefordert worden war. Da die DSGVO aber davon abweichende gesetzliche Anforderungen enthält, waren Altverträge zu überprüfen und ggf. anzupassen.

Eine der maßgeblichen Pflichten des Auftraggebers ist es zu überprüfen, dass der Auftragnehmer seine vertraglich übernommenen Pflichten einhält. Eine entsprechende Überprüfung des Auftragnehmers ist sinnvoll und sollte dokumentiert werden, damit dies ggf. bei einer aufsichtsbehördlichen Prüfung nachgewiesen werden kann (s. auch Kap. 7, S. 67 ff.).[16]

16 s. hierzu auch: Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hg.): Mustervertragsanlage. Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO). Mai 2017 (in Überarbeitung). Online: https://www.bitkom.org/sites/main/files/2022-03/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf (abgerufen am 11.05.2022); Europäische Kommission (Hg.): Durchführungsbeschluss (EU) 2021/915 Der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates. Juni 2021. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=EN (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO. Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO. Juni 2021. Online: https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-mustervertrag-zur-auftragsverarbeitung-gemaess-art-28-ds-gvo (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): Template Processing in accordance with Article 28 General Data Protection Regulation (GDPR). Juni 2021. Online: https://www.gdd.de/downloads/praxishilfen/ph-iv-mustervertrag_zur_auftragsverarbeitung_ds-gvo_english (abgerufen am 11.05.2022).

6.2.4 Neue Dokumentationspflichten

6.2.4.1 Datenschutzgrundsätze und Rechenschaftspflicht

Ausgangspunkt sind die in Art. 5 Abs. 1 DSGVO neu definierten Datenschutzgrundsätze:

- Rechtmäßigkeit und Treu und Glauben,
- Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit sowie
- Rechenschaftspflicht.

Die Datenverarbeiter sind verpflichtet, die vorgenannten Grundsätze einzuhalten. Die Beachtung dieser Prinzipien kann insbesondere von den Datenschutzaufsichtsbehörden kontrolliert werden. Auf Anforderung muss der Verantwortliche die Einhaltung dieser Grundsätze nachweisen können (sog. Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO). Um diese Rechenschaftspflicht erfüllen zu können, ist es unerlässlich, die Einhaltung der vorgenannten Grundsätze und die dazu getroffenen Maßnahmen zu dokumentieren.

6.2.4.2 Datenschutzmanagementsystem

Um den Nachweis über die Einhaltung der voraufgeführten Datenschutzgrundsätze gegenüber Datenschutzaufsichtsbehörden oder z. B. auch nachfragenden Kunden erbringen und belegen zu können, dass der Verantwortliche die Datenverarbeitung entsprechend den Vorgaben der DSGVO, insbesondere auch den Datenschutzgrundsätzen aus Art. 5 Abs. 1 DSGVO organisiert hat, ist es sinnvoll, ein professionelles Datenschutzmanagementsystem (DSMS) zu etablieren. Auf diese Weise lässt sich am besten dokumentieren, dass die einzelnen, zur Gewährleistung angemessener Datenschutzstandards erforderlichen Maßnahmen systematisch, vollständig, gewissenhaft und nachprüfbar umgesetzt werden.

Ein DSMS ist durch eine auf kontinuierliche Verbesserung ausgerichtete, systematische und gesteuerte Organisation definiert, die dazu dient, die Anforderungen des Datenschutzes angemessen und erfolgreich mittels geeigneter Maßnahmen umzusetzen. Es sind also zunächst bestimmte,

im Unternehmen geltende Datenschutzrichtlinien festzulegen. In einem Handbuch ist dann zu dokumentieren, durch welche Maßnahmen diese strategischen Vorgaben in der Praxis im Unternehmen umgesetzt werden.

Das Datenschutzhandbuch sollte zentral die strategischen und operativen Vorgaben dokumentieren und zugleich Nachschlagwerk bezüglich der Anwendung des DSMS für die Verantwortlichen der Datenschutzorganisation sein. Darüber hinaus soll das Datenschutzhandbuch etwa als Prüfungsgrundlage für die Durchführung von Audits etc. dienen (s. auch Kap. 8, S. 77 ff.).

6.2.4.3 Verzeichnis der Verarbeitungstätigkeiten

Jeder Datenverarbeiter ist verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, zu führen. Eine entsprechende Verpflichtung enthielt auch das BDSG a. F. Das Verzeichnis muss gem. Art. 30 Abs. 1 DSGVO u. a. folgende Angaben aufweisen:

- Name und Kontaktdaten des Verantwortlichen,
- Zweck der Verarbeitung,
- Beschreibung der Kategorien betroffener Personen und personenbezogener Daten,
- Kategorien von Empfängern,
- Übermittlung personenbezogener Daten in ein
- Drittland,
- Fristen für die Löschung,
- Beschreibung der technischen und organisatorischen Maßnahmen usw.

Die Erstellung kann auch mittels einer tabellarischen Auflistung erfolgen, es gibt aber auch proprietäre Tools, die dabei unterstützen. Aufsichtsbehörden haben auch einfache Muster für Verzeichnisse der Verarbeitungsübersicht für verschiedene Verantwortliche veröffentlicht, wie beispielsweise das Bayerische Landesamt für Datenschutzaufsicht.[17]

17 s. hierzu auch: Bayerisches Landesamt für Datenschutzaufsicht (Hg.): Muster 9. Online-Shop – Verzeichnis von Verarbeitungstätigkeiten. o. D. Online: https://www.lda.bayern.de/media/muster_9_online-shop_verzeichnis.pdf (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e. V. (Hg.): GDD-Praxishilfe Verzeichnis von Verarbeitungstätigkeiten – Verantwortlicher, Version 2.1. April 2022. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfeDSGVOVerzeichnisvonVerarbeitungsttigkeiten.pdf (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e. V. (Hg.): GDD-Praxishilfe DS-GVO Vb. Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter. Januar 2020. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_5bVVTAuftragsverarbeiter.pdf (abgerufen am 11.05.2022).

6.2.4.4 Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik und vor allem der Eintrittswahrscheinlichkeit sowie der Schwere des Risikos für Rechte und Freiheiten der Betroffenen ist der Datenverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Dazu gehören z. B. folgende Maßnahmen:

- Pseudonymisierung und Verschlüsselung,
- Vertraulichkeit und Integrität,
- Datenminimierung,
- Speicherfristen,
- Zugänglichkeit.

Diese Maßnahmen waren in ähnlicher Form ebenfalls bereits im früheren BDSG geregelt. Dabei kann auch auf die Maßnahmen zurückgegriffen werden, die aus eigenem Interesse zum Schutz der Informationen ergriffen werden. Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sind für jedes Unternehmen und jede Behörde unerlässlich – eignen sich aber dabei auch als Maßnahmen zum Schutz personenbezogener Daten. An diesen Datensicherheitsmaßnahmen können sich die Unternehmen auch weiterhin orientieren, die Vorgehensweise zur Skalierung orientiert sich an den Risiken für die Rechte und Freiheiten der natürlichen Person, deren Daten verarbeitet werden.[18]

6.2.4.5 Meldung von bzw. Benachrichtigung bei Schutzverletzungen – „Datenpannen“

Eine „Datenpanne“ ist jedes schädliche Ereignis bei der Verarbeitung von personenbezogenen Daten. Nach der DSGVO umfasst eine Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DSGVO).

18 s. hierzu auch: Bayerisches Landesamt für Datenschutzaufsicht (Hg.): Good Practice bei technischen und organisatorischen Maßnahmen Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit (Checkliste TOM: technische und organisatorische Maßnahmen). Oktober 2020. Online: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf (abgerufen am 11.05.2022).

Dies liegt etwa dann vor, wenn im Unternehmen gespeicherte Kunden- oder Beschäftigtendaten verloren gehen, gehackt werden oder auf sonstige Weise in falsche Hände geraten. In allen diesen Fällen handelt es sich um eine Verletzung des Schutzes personenbezogener Daten, die nach Art. 33 DSGVO zu einer Meldepflicht des betroffenen Unternehmens gegenüber der für diese Gesellschaft zuständigen Aufsichtsbehörde führt. Die Meldung hat unverzüglich nach Bekanntwerden und möglichst binnen 72 Stunden zu erfolgen.

Diese Meldepflicht besteht nach der DSGVO grundsätzlich bei sämtlichen personenbezogenen Daten. Allerdings erfährt diese Verpflichtung insoweit eine Einschränkung, als jedenfalls dann keine Meldung erforderlich ist, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Letzteres gilt etwa dann, wenn lediglich Bagatellverletzungen im Raum stehen oder der zu erwartende Schaden unmittelbar begrenzt und behoben wird. Nicht jede einzelne Datenpanne ist damit automatisch meldepflichtig, sondern eine Meldepflicht entsteht erst dann, wenn die Datenschutzverletzung zu einem messbaren Risiko führt.

Hat die Datenpanne nicht nur ein „normales", sondern darüber hinaus ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, müssen zudem die davon betroffenen Personen benachrichtigt werden (Art. 34 DSGVO). Ist dies mit einem unverhältnismäßigen Aufwand verbunden, etwa weil die Zahl der betroffenen Personen zu groß ist, dann entfällt die persönliche Benachrichtigungspflicht. Stattdessen hat in derartigen Fällen eine öffentliche Bekanntmachung zu erfolgen, etwa durch entsprechende Informationen auf der Webseite des Unternehmens oder durch eine Veröffentlichung in den Medien.[19]

6.2.4.6 Datenschutz-Folgenabschätzung

Hat eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche vorab eine Abschätzung der Folgen des Verarbeitungsvorganges durchführen und sicherstellen, dass das Risiko durch angemessene Maßnahmen so gering wie möglich gehalten wird (Art. 35 DSGVO). Die Anforderungen an die

19 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250rev.01. Februar 2018. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_de (abgerufen am 11.05.2022).

DSFA sind umfangreich und vor allem müssen die getroffenen Maßnahmen und die vorgenommenen Prüfungen ausführlich dokumentiert werden, um auf diese Weise die durchgeführte DSFA ggf. gegenüber der zuständigen Datenschutzaufsichtsbehörde belegen zu können.

Zunächst ist zu prüfen, für welche Verfahren eine gesonderte DSFA vorzunehmen ist. Erforderlich ist dies nur bei Verfahren, die ein besonders hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben können. Die Datenschutzaufsichtsbehörden haben inzwischen verschiedene Listen veröffentlicht, in denen entsprechende Verfahren beschrieben bzw. Branchen genannt werden, bei denen eine DSFA in jedem Falle durchzuführen ist.[20]

6.2.4.7 Benennung eines Datenschutzbeauftragten

Die DSGVO verpflichtet die datenverarbeitenden Unternehmen unter bestimmten Voraussetzungen, die Bestellung eines betrieblichen Datenschutzbeauftragten vorzunehmen (Art. 37 DSGVO). Die Aufgaben des Datenschutzbeauftragten ergeben sich aus Art. 39 DSGVO, dazu gehören insbesondere die

- Beratung des Verantwortlichen in datenschutzrechtlicher Hinsicht,
- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften,
- Schulung der Mitarbeiter,
- Beratung des Verantwortlichen bei der Datenschutz-Folgenabschätzung.

6.2.5 Zusammenfassung

Die Pflichten der Datenverarbeiter sind mit Einführung der DSGVO deutlich erhöht worden. Der Umfang der zur Verfügung zu stellendenim Rahmen der Informationspflichten gemäß Art. 13 und 14 DSGVO zu geben-

20 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP248rev.01. Oktober 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_de (abgerufen am 11.05.2022); Europäischer Datenschutzausschuss (Hg.): Empfehlung 01/2019 zu der vom Europäischen Datenschutzbeauftragten entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725). Juli 2019. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendation_201901_edps_39.4_dpia_list_de.pdf. (abgerufen am 11.05.2022).

den Informationen ist um ein Vielfaches angestiegen. Eine ganz wesentliche Veränderung bringt die DSGVO für die Datenverarbeiter auch in Bezug auf die Dokumentationspflichten mit sich. Die Ausweitung des Inhalts der Verfahrensverzeichnisse und die Durchführung einer DSFA bedeuten erhebliche Mehraufgaben für die Datenschutzverantwortlichen. Ob die Erfüllung der durch die DSGVO eingeführten bzw. erhöhten Pflichten der Datenverarbeiter zu der vom europäischen Gesetzgeber gewünschten Verbesserung des Datenschutzes in der EU führt, wird sich in der Praxis noch zeigen müssen.

7. Auftragsverarbeitung

Es gibt kaum ein Unternehmen oder eine öffentliche Einrichtung, die keinen Dienstleister einsetzt, um dessen Spezialisierung in Anspruch zu nehmen. Werden dabei personenbezogene Daten verarbeitet, sind für den Auftraggeber und den Auftragnehmer in aller Regel die Vorgaben der DSGVO zur Auftragsverarbeitung nach Art. 28 DSGVO zu beachten. Dies betrifft beispielsweise die Beauftragung von Call-Centern, Lettershops, aber auch IT-Dienstleistern, insb., wenn deren Tätigkeit die Speicherung oder andere Verarbeitungen personenbezogener Daten beinhaltet. Dazu zählen dann auch Cloud-Dienstleister und ggf. Webhoster etc.

Der Auftraggeber bleibt in seiner Rolle als Verantwortlicher, d. h., er bestimmt Zwecke und Mittel der Verarbeitung. Der eingesetzte Auftragsverarbeiter bleibt bei der Verarbeitung strikt weisungs- und zweckgebunden. Für die Einbeziehung eines Auftragsverarbeiters und die Weitergabe der personenbezogenen Daten an diesen benötigt der Verantwortliche keine weitere Rechtmäßigkeitsgrundlage. Diese leitet sich aus der originären Grundlage ab, auf die sich der Verantwortliche zur Verarbeitung beruft, würde er die ausgelagerten Tätigkeiten selbst durchführen. Im Unterschied zu den bisherigen datenschutzrechtlichen Vorgaben werden dem Dienstleister nun eigene Verantwortlichkeiten in der DSGVO zugewiesen.

Grundsätzlich entsprechen die Begriffsbestimmungen zum Verantwortlichen und zum Auftragsverarbeiter (Art. 4 Nr. 7 und 8 DSGVO) den bisherigen aus der EU-Datenschutzrichtlinie aus dem Jahr 1995.[21] Einige Besonderheiten ergeben sich aber aus Art. 28 DSGVO, der die zentrale Norm für die Beauftragung eines Dienstleisters darstellt.

7.1 Angebotseinholung und Angebotsauswahl

Bei den Anforderungen an den Dienstleister (Auftragnehmer = Auftragsverarbeiter = AV) ist wie bisher zu beachten, dass der AV aufgrund seiner technischen und organisatorischen Maßnahmen (TOM) hinreichende Garantien bietet, dass die Verarbeitung durch ihn im Einklang mit den daten-

21 vgl. EUR-Lex: Richtlinie 95/46/EG. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31995L0046 (abgerufen am 11.05.2022).

schutzrechtlichen Anforderungen hinsichtlich des Schutzes der Rechte der betroffenen Person erfolgt (Art. 28 Abs. 1 DSGVO).

> **Wichtig:** Somit ist in der Angebots- und Auswahlphase weiterhin darauf zu achten, dass der AV die erforderlichen TOMs gewährleistet.

7.2 Der Vertrag

Gemäß Art. 28 DSGVO sind der Gegenstand und die Dauer sowie die diversen Pflichten und die Ausgestaltung von Kontrollen durch den „Verantwortlichen", also den Auftraggeber (= AG) detailliert vertraglich festzulegen. Folgende Punkte sind vertraglich zwingend zu regeln:

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten und die Kategorien betroffener Personen,
- die weisungsabhängige Verarbeitung durch den Auftragsverarbeiter, dabei auch weisungsabhängige Drittlandübermittlung (dabei Hinweispflicht bei gesetzlicher Pflicht des AV zur Übermittlung in ein Drittland sowie Hinweispflicht des AV bei seiner Ansicht nach rechtswidrigen Weisungen),
- die Verpflichtung, dass zur Verarbeitung nur Personen befugt sind, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
- dass erforderliche Schutzmaßnahmen nach Art. 32 ergriffen werden,
- dass bei der Einbindung weiterer AV die Bedingungen des Art. 28 Abs. 2 und 4 DSGVO eingehalten werden und diese nur in Abstimmung mit dem Verantwortlichen und bei Weitergabe der vertraglichen Verpflichtung einzusetzen,
- eine Regelung zum Umgang der Daten nach Abschluss der Erbringung der Verarbeitungsleistung (Löschung oder Rückgabe),
- Regelungen zur Unterstützung durch den AV zugunsten des AG bei dessen Pflichten zur Datensicherheit, Meldepflicht bei Datenpannen, Behandlung von Betroffenenrechten sowie der DSFA,

- Regelungen, wie der AG die Einhaltung der Anforderungen nach Art. 28 DSGVO beim AV überprüfen kann. Hierbei stehen ihm nicht nur Selbstauskünfte oder Zertifikate zur Verfügung, auch eine Vor-Ort-Inspektion kann in Frage kommen.

Dass der AV dem AG eine Verletzung des Schutzes personenbezogener Daten meldet, ist bereits in Art. 33 Abs. 2 DSGVO geregelt und muss nicht gesondert vereinbart werden. Zu der Vereinbarung zur Auftragsverarbeitung bestehen bereits entsprechende Muster von Vereinen und Verbänden.[22]

Auch die EU-Kommission hat von der Möglichkeit aus Art. 28 Abs. 7 DSGVO Gebrauch gemacht, Standardvertragsklauseln zur Auftragsverarbeitung zu veröffentlichen.[23] Neben der EU-Kommission können auch Datenschutzaufsichtsbehörden Standardvertragsklauseln zur Auftragsverarbeitung veröffentlichen. Diese sind aber nicht zwingend zu verwenden, sondern können eine Basis für Verhandlungen bieten. Lassen Sie sich dabei fachkundig beraten, denn diese Formulierungen müssen dem jeweiligen Einzelfall angepasst werden.

7.2.1 Form des Vertrages

Die Vereinbarungen zur Auftragsvereinbarung können nunmehr auch in einem elektronischen Format abgeschlossen werden, dies schließt z. B. auch Vereinbarungen über E-Mail-Kommunikation mit ein. Dabei sollte beachtet werden, dass hierüber ein Nachweis möglich sein muss. Ein Abschluss mittels qualifizierter elektronisch Signatur (§ 126a BGB) ist nicht erforderlich.

22 s. hierzu auch: Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO. Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO. Juni 2021. Online: https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-mustervertrag-zur-auftragsverarbeitung-gemaess-art-28-ds-gvo (abgerufen am 11.05.2022).

23 s. hierzu auch: Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hg.): Mustervertragsanlage. Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO). Mai 2017 (in Überarbeitung). Online: https://www.bitkom.org/sites/main/files/2022-03/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf (abgerufen am 11.05.2022); Europäische Kommission (Hg.): Durchführungsbeschluss (EU) 2021/915 Der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates. Juni 2021. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=EN (abgerufen am 11.05.2022).

7.2.2 Übermittlungsprivileg künftig auch für Auftragsverarbeitung in Drittländern

Die frühere Beschränkung der Auftragsverarbeitung innerhalb der EU/des EWR ist entfallen. Durch entsprechende Maßnahmen (z. B. Einwilligung der betroffenen Person, ein Angemessenheitsbeschluss der EU-Kommission, der Verwendung der EU-Standardvertragsklauseln, das Vorhandensein genehmigter Binding Corporate Rules oder eines besonderen Anforderungen unterliegenden Zertifikats beim Datenempfänger) ist ein angemessenes Datenschutzniveau beim Empfänger sicherzustellen.

7.2.3 Kontrollpflichten des Auftraggebers und des Auftragsverarbeiters

Der AG ist als Verantwortlicher zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs verpflichtet. Diese ergibt sich aus den Anforderungen des Art. 32 Abs. 1 lit. d DSGVO, denn durch die Auslagerung von bestimmten Verarbeitungstätigkeiten kann sich der AG als Verantwortlicher dieser Verpflichtung nicht entziehen. Ein Verstoß hiergegen ist bußgeldbewehrt.

Die Verpflichtung zu geeigneten Schutzmaßnahmen und deren Einhaltung trifft auch den AV selbst. Damit kann der AG seine Kontrollen auch auf die entsprechenden Dokumentationen des AV abstellen. Je nach individueller Interessenslage kann der AV hierbei Zertifikate nutzen, um dadurch die Offenlegung von Details seiner Schutzmaßnahmen gegenüber einer großen Anzahl von Kunden zu vermeiden. Um spätere Missverständnisse zu vermeiden, empfiehlt es sich, bereits bei Beauftragung zu klären, unter welchen Bedingungen Inspektionen vor Ort möglich sind, sollte die Prüfung von Schutzmaßnahmen allein über Selbstbestätigungen, Gütesiegel, genehmigte Verhaltensregeln oder Zertifikate nicht mehr ausreichen. Dabei kann auch geklärt werden, welche Anforderungen an die Anmeldung und ggf. eine aufwandsbezogene Vergütungspflicht von beiden Seiten erwartet wird.

7.2.4 Pflichten des Auftraggebers bzw. des Auftragsverarbeiters im Zusammenhang mit einer Datenschutz-Folgenabschätzung

Soweit eine Datenschutz-Folgenabschätzung durch den AG erforderlich ist (Art. 35), sind im Rahmen der nach Art. 36 evtl. erforderlichen vorherigen Konsultation der Aufsichtsbehörde ausreichende Informationen über beteiligte AV zur Verfügung zu stellen. In diesem Fall wird durch den AG neben den eigenen Schutzmaßnahmen zumindest ein ausreichendes Datenschutz- und Sicherheitskonzept des oder der AV mit vorzulegen zu sein. Nach Art. 28 Abs. 3 lit. f DSGVO ist der AV vertraglich zu verpflichten, den AG im Zusammenhang mit der DSFA zu unterstützen.

7.2.5 Vergütungsfragen frühzeitig klären

Bei einigen Unterstützungsleistungen des AV gegenüber dem AG ist für den AV schwer einzuschätzen, wie oft und in welchem Umfang er hierfür in Anspruch genommen werden kann.

> **Tipp:** Klären Sie frühzeitig, welche Unterstützungsleistung durch den AV bereits mit der Vergütung für die Hauptleistung umfasst ist und bei welchen unter Umständen weitere Kosten entstehen können. Sie reduzieren dadurch das Risiko von Missverständnissen und Zeitverlust, wenn die Unterstützung erforderlich wird.

7.2.6 Haftungserweiterung auf Auftragsverarbeiter

Der AV unterliegt nach der DSGVO mehr Pflichten und umfangreicheren Haftungsregeln als nach dem BDSG (z. B. gesamtschuldnerische Haftung gemäß Art. 82 DSGVO und den Bußgeldvorschriften nach Art. 83 DSGVO).

Ein AV im Sinne von Art. 28 DSGVO ist soweit verpflichtet:

- sein Dienstleistungsangebot, seine internen Prozesse sowie die TOMs an die Anforderungen der DSGVO anzupassen,
- ein entsprechendes Datensicherheitskonzept und ein IT-Sicherheitsmanagement zu etablieren,

- seine Infrastruktur und TOMs permanent zu überprüfen, um den „Stand der Technik“ zu gewährleisten,
- auch die auftragsbezogenen Verarbeitungen in einem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren (Art. 30 Abs. 2) und
- seine bestehenden und künftigen Verträge mit seinem AG entsprechend den Anforderungen der DSGVO zu gestalten.

7.2.7 Beauftragung von Dienstleistungen, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann

Hierzu gab es eine eigene Regung in § 11 Abs. 5 BDSG a. F., die eine entsprechende Anwendung der Vorgaben zur Auftragsverarbeitung vorsah. Die DSGVO enthält keine entsprechende Regelung. Dennoch kommen die deutschen Aufsichtsbehörden in ihrem Kurzpapier Nr. 13 vom Januar 2018 zu der Aussage, dass auch hier die Vorgaben des Art. 28 DSGVO anzuwenden sind.[24] Nur bei einer rein technischen Wartung, wie bei der Stromzufuhr, reiche eine Verschwiegenheitsvereinbarung. Diese Einschätzung zur Fernwartung stand allerdings unter dem Vorbehalt, dass auf europäischer Ebene durchaus eine andere Einschätzung denkbar ist. In ihrem Leitfaden 07/2020 zum Verantwortlichen und Auftragsverarbeiter[25] bringt der Europäische Datenschutzausschuss hierzu einige Beispiele.[26]

7.2.8 Regelung zum Einsatz von Unterauftragnehmern

Der Einsatz weiterer Auftragsverarbeiter (Unter-Auftragnehmer) unterliegt der gesonderten oder allgemeinen Zustimmungspflicht des Verantwortlichen (Art. 28 Abs. 2 DSGVO). „Weitere Auftragnehmer“ dürften nicht solche AV sein, die allgemeine Hilfs- und Nebentätigkeiten erbringen, die nicht unmittelbar der Erfüllung des Ursprungsauftrags dienen (z. B. Soft-

24 s. hierzu auch: Datenschutzkonferenz (Hg.): Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DSGVO. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf (abgerufen am 11.05.2022).

25 European Data Protection Board (Hg.): Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Juli 2021. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (abgerufen am 11.05.2022).

26 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO. Juli 2021. Online: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf (abgerufen am 11.05.2022).

ware-Wartung oder Datenvernichtung). Die Verpflichtung zum Abschluss einer Vereinbarung über eine Auftragsverarbeitung zwischen dem AV und dem die allgemeinen Hilfs- und Nebentätigkeiten erbringenden Dienstleister nach Art. 28 Abs. 1 bleibt davon unberührt.

Soweit es sich um einen weiteren AV handelt, weil eine Hauptleistung oder ein Teil davon an einen weiteren Auftragsverarbeiter ausgelagert wird, muss der AV

- seinen AG über jede vorgesehene Änderung in Bezug auf die Hinzufügung oder die Ersetzung anderer weiterer AV informieren und dem AG ein Einspruchsrecht einräumen,
- mit dem weiteren AV einen Vertrag (schriftlich oder elektronisch) abschließen, der dieselben Gesetzesanforderungen erfüllt wie der Vertrag zwischen AG und AV.

7.2.9 Abgrenzung Auftragsverarbeitung zur „Funktionsübertragung“

Der Begriff der „Funktionsübertragung“ grenzte vor Anwendbarkeit der DSGVO eine weisungsabhängige, primär technische Dienstleistung (Auftragsverarbeitung) zu einer (weitgehend) weisungsfreien, dabei eigene Aufgaben erfüllenden Leistungserbringung ab. Wegen dieser übertragenen Funktion und der damit (auch) verfolgten eigenen Zwecke wird der Dienstleister zur verantwortlichen Stelle.

> **Beispiel:** externer Betriebsarzt, Rechtsanwalt, Steuerberater, Wirtschaftsprüfer, Reisebüro

Die Datenschutzkonferenz lehnt den Begriff der „Funktionsübertragung“ unter der DSGVO ab. Bei der Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DSGVO gegeben sein muss, liegt aber weiterhin keine Auftragsverarbeitung vor.[27]

27 s. hierzu auch: Datenschutzkonferenz (Hg.): Kurzpapier Nr. 13. Auftragsverarbeitung, Art. 28 DSGVO. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf (abgerufen am 11.05.2022).

Weitere Beispiele: neben Berufsgeheimnisträgern, Inkassobüros mit Forderungsübertragung, Bankinstitute für den Geldtransfer und Postdienste für den Brieftransport

Die Rechtsgrundlage für die Weitergabe der personenbezogenen Daten an solche Empfänger ist in Art. 6 DSGVO zu suchen, meist wird die Wahrung berechtigter Interessen heranzuziehen sein (vgl. Art. 6 Abs. 1 lit. f DSGVO). Ergänzend wird dies auch im DSK-Kurzpapier Nr. 16 behandelt, in dem es heißt: „Verarbeitungen, die bislang in Deutschland als sogenannte Funktionsübertragung bewertet wurden, können unter der DSGVO – je nach Fall – als Auftragsverarbeitung (Art. 28 DSGVO), als gemeinsame Verantwortlichkeit (Art. 26 DSGVO) oder aber als „normale" Übermittlung an einen anderen Verantwortlichen (ohne gemeinsame Verantwortlichkeit) eingestuft werden. Welcher Fall jeweils vorliegt, beurteilt sich allein danach, wer über die Zwecke und (zumindest wesentlichen Elemente der) Mittel der Datenverarbeitung entscheidet."[28]

In die Diskussion kam durch die DSGVO auch wieder die Mandatierung eines Steuerberaters. Hierzu gab es durch deutsche Aufsichtsbehörden unterschiedliche Aussagen hinsichtlich der Lohnbuchhaltung durch Steuerberater. Der deutsche Gesetzgeber hat hier durch eine Änderung des § 11 Steuerberatungsgesetz für Rechtssicherheit gesorgt. Demnach handelt ein Steuerberater für alle Tätigkeiten, die er im Rahmen des Steuerberatungsgesetzes ausführt, als Verantwortlicher nach Art. 4 Nr. 7 DSGVO, davon werden auch alle Tätigkeiten im Rahmen der Lohnbuchhaltung umfasst. Neben dem (meist formlosen) Mandatsvertrag wird daher mit dem Steuerberater keine Vereinbarung zur Auftragsverarbeitung benötigt.

7.2.10 Gemeinsame Verantwortlichkeit

Durch die DSGVO gibt es nun auch ein neues Modell der Zusammenarbeit in datenschutzrechtlicher Hinsicht: die gemeinsame Verantwortlichkeit von mindestens zwei verantwortlichen Stellen, die sich gemeinsam zur Verarbei-

28 Datenschutzkonferenz (Hg.): Kurzpapier Nr. 16. Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, März 2018, S. 2. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf (abgerufen am 11.05.2022).

tung entscheiden, Art. 26 DSGVO. Diese müssen eine Vereinbarung abschließen, aus der hervorgeht, wer für die Umsetzung der Betroffenenrechte verantwortlich ist und diese Passagen müssen den betroffenen Personen zugänglich gemacht werden.

Auch wenn das Konstrukt der gemeinsamen Verantwortlichkeit bereits in der früheren EU-Datenschutzrichtlinie angelegt war, so existierten in Deutschland noch keine nachhaltigen Erfahrungen mit diesem Modell. Es gibt aber bereits EuGH-Entscheidungen, in denen die gemeinsame Verantwortlichkeit thematisiert wurde (gemeinsame Verantwortung von Facebook und Fanpage-Betreibern, EuGH vom 5.6.2018 (C-210/16), sowie Mitglieder der Gemeinschaft der Zeugen Jehovas im Rahmen einer Verkündigungstätigkeit sind zusammen mit der Religionsgemeinschaft gemeinsame Verantwortliche, EuGH vom 10. Juli 2018 (C-25/17)). Auch befasst sich der Europäische Datenschutzausschuss in seiner Guideline 07/2020[29] mit der Thematik und berücksichtigt dabei die EuGH-Entscheidungen.

Die gemeinsame Verantwortung wird meist wohl durch die Nutzung gemeinsamer Infrastrukturen oder anderer Umstände erkennbar sein (z. B. bei Verarbeitung von Beschäftigten- oder Kundendaten innerhalb einer Unternehmensgruppe). Aber hierfür ist weiterhin eine entsprechende Rechtmäßigkeitsgrundlage (wie Art. 6 Abs. 1 lit. f DSGVO) erforderlich.[30]

29 European Data Protection Board (Hg.): Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Juli 2021. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (abgerufen am 11.05.2022).

30 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO. Juli 2021. Online: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe XV. Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO (Joint Controllership). Dezember 2019. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_15_JointControllership_1.0.pdf (abgerufen am 11.05.2022).

8. Datenschutzmanagementsystem

Mit der DSGVO gewinnt das Thema Informationssicherheit und Datenschutz massiv an Bedeutung. Eine Pflicht zur Einführung eines Datenschutzmanagementsystems (DSMS) unter der DSGVO ergibt sich somit zwangsläufig, da die DSGVO verlangt, ein Verfahren zur Überprüfung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (TOM) einzusetzen. Um den neuen Vorgaben der DSGVO – insbesondere zur Auftragsverarbeitung im Unternehmen gerecht zu werden – empfiehlt es sich, die Vorgaben und Richtlinien zum Datenschutz in das vorhandene Informationssicherheitsmanagementsystem (ISMS) zu integrieren. Dadurch entsteht ein ganzheitliches Datenschutzmanagementsystem.

Art. 32 DSGVO legt dabei die Schutzziele fest, an denen ein für die Datenverarbeitung personenbezogener Daten Verantwortlicher, seine technischen und organisatorischen Maßnahmen zum Schutz der Daten auszurichten hat. Die oben beschriebene Pflicht des Verantwortlichen seine getroffenen technischen und organisatorischen Maßnahmen regelmäßig hinsichtlich ihrer Wirksamkeit zu überprüfen, ist in engem Zusammenhang mit einer weiteren Regelung der DSGVO zu sehen. Hierzu zählt z. B. die in Art. 5 Abs. 2 DSGVO geführte Rechenschaftspflicht. Die in Art. 32 DSGVO beschriebenen Ziele weichen etwas von den derzeit im BDSG genannten Zielsetzungen ab. Etwas grundlegend Neues wurde mit der DSGVO jedoch nicht eingeführt. Wirklich neu ist jedoch die letztgenannte Maßnahme mit der Forderung nach „einem Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“. Die Konsequenzen, die sich aus dieser gesetzlichen Regelung für die Verantwortlichen ergeben, sollen im Folgenden näher beleuchtet werden. Die für das Datenschutzmanagement relevanten Normen finden sich in der Verordnung an vielen unterschiedlichen Stellen, beispielsweise:

- Art. 5 DSGVO stellt die Grundsätze für die Verarbeitung personenbezogener Daten dar,
- Art. 30 DSGVO legt dem Verantwortlichen auf, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen,

- Art. 32 DSGVO regelt, dass der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen umzusetzen haben, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung von personenbezogenen Daten gemäß der DSGVO erfolgt,
- Art. 35 DSGVO verpflichtet den Verantwortlichen bei Verarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchzuführen.

8.1 Vorteile eines Datenschutzmanagementsystems

Zu den Vorteilen eines DSMS zählen insbesondere die

- nachhaltige, ganzheitliche Risikominimierung,
- Absicherung der Unternehmenswerte,
- Überprüfbarkeit durch revisionssichere Dokumentation der Aktivitäten und
- Compliance gegenüber Geschäftspartnern, Kunden, Interessenten etc.

In einem dergestalt etablierten DSMS lassen sich schützenswerte Informationen und Geschäftsprozesse nahtlos integrieren. Das heißt, es werden dadurch alle Anforderungen des Datenschutzes und der Informationssicherheit erfüllt. Außerdem kann man mit der Etablierung eines Datenschutzkonzeptes nach der DSGVO den Anforderungen an die Rechenschaftspflichten der Grundverordnung gegenüber Datenschutzbeauftragten und Aufsichtsbehörden am ehesten gerecht werden.

8.2 Datenschutzmanagement und Informationssicherheit

Die Berücksichtigung von Datenschutz und Informationssicherheit in Form eines Datenschutzmanagementsystems ist empfehlenswert, da das gesamte Vorgehen zur Umsetzung der neuen EU-DSGVO-Anforderungen viele Gemeinsamkeiten mit der Struktur eines ISMS aufweist.

8.3 Datenschutzmanagementsystem-Prozess

Ein DSMS auf Basis der DSGVO und der ISO 27001 oder/und IT-Grundschutz etabliert anerkannte Verfahren, mit welchen Prozesse und Richtlinien in einem Unternehmen methodisch eingeführt werden. Diese Richtlinien ermöglichen es, Risiken für Datenschutzverstöße zu erkennen und einschließlich aller technischen und organisatorischen Maßnahmen zu steuern, zu kontrollieren und permanent zu verbessern.

Durch die ISO 27701 wird dies zusammengeführt und auf Basis eines bestehenden ISO 27001-Zertifikats ein erweiterter Schutz für personenbezogene Daten berücksichtigt. Die nachfolgenden Schritte – angelehnt an den Plan-Do-Check-Act-Zyklus – können für die Einführung oder Anpassung eines Datenschutzmanagementsystems hilfreich sein:

1. **Analyse** der gegebenen IT-Situation mit (datenschutz-)rechtlicher Bewertung, Identifizieren und Bewerten von Risiken
2. **Agieren** mit Handlungsanweisungen und zu etablierenden Maßnahmen
3. **Kontrolle** der Gegebenheiten mit Überwachungsprozessen
4. **Bewertungen vornehmen und Folgendefinition** im Rahmen der gegebenen Situation im DSMS-Kreislaufsystem

Die Vorgaben der DSGVO hinsichtlich des DSMS müssen demnach erfüllt werden und nachweisbar sein. Das heißt, Unternehmen müssen beweisen können, dass sie geeignete Datenschutzrichtlinien und -vorkehrungen getroffen haben und umsetzen. Andernfalls drohen Bußgelder, Schadenersatzansprüche und weitere Nachteile.

8.4 Inhalte einer Datenschutzrichtlinie

8.4.1 Datenschutzorganisation und Verantwortlichkeiten

Die beste Datenschutzrichtlinie ist sinnlos, wenn sie nicht durchgängig auch gelebt wird. Die Datenschutzrichtlinie muss also nicht nur von der Geschäftsführung/Unternehmensleitung, sondern gerade auch von den Mitarbeitern im Unternehmen ernst genommen und umgesetzt werden. Je nach Größe des Unternehmens kann es sich empfehlen – zusätzlich zu

dem Datenschutzbeauftragten des Unternehmens – in den verschiedenen Abteilungen einen Verantwortlichen für den Datenschutz (Datenschutz-Koordinator oder -Delegierten) zu benennen, der als Koordinierungsstelle zwischen dem Datenschutzbeauftragten und den Mitarbeitern in seiner Abteilung dient. Dieser Verantwortliche (z. B. der Abteilungsleiter) hat dafür zu sorgen, dass alle datenschutzrechtlich relevanten Sachverhalte aus seiner Abteilung an den Datenschutzbeauftragten weitergeleitet werden. Die Schulung und Sensibilisierung der Mitarbeiter sollte aber der Datenschutzbeauftragte selbst übernehmen.[31]

8.4.2 Einbindung des Datenschutzbeauftragten

In der Datenschutzrichtlinie sind die Fälle zu definieren, in denen die Mitarbeiter den Datenschutzbeauftragten anzusprechen und einzubinden haben. Hat das Unternehmen sich dafür entschieden, dass die Mitarbeiter sich zunächst an den Datenschutz-Koordinator wenden sollen, dann gelten diese Fälle auch für diesen. Ausgenommen sind vertrauliche Anfragen, in denen die Rechte des Mitarbeiters selbst betroffen sind. Als „meldepflichtige" Fälle gelten insbesondere:

- Beschwerden von Betroffenen (Mitarbeitern, Kunden),
- Einführung eines neuen Systems/Tools,
- Einsatz eines neuen Dienstleisters/ggf. auch Subunternehmers im Rahmen genutzter AV,
- Werbemaßnahmen (z. B. Versand von Newsletter, Onlinemarketing-Aktionen, insbesondere Conversion Tracking etc.).

In jedem Unternehmen hat der Datenschutzbeauftragte die datenschutzrechtlich relevanten Sachverhalte zu definieren und in die Datenschutzrichtlinie aufzunehmen. Diese Liste kann und muss nicht abschließend sein, sondern sollte vor allem als Handlungshilfe für die Mitarbeiter dienen und nachträglich ergänzt werden können.

31 s. hierzu auch: Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO. Die Datenschutz-Richtlinie. Grundlagen, Grundstrukturen und typische Regelungsbereiche. November 2021. Online: https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/PraxishilfeDSGVODieDatenschutzRichtlinie.pdf (abgerufen am 11.05.2022).

8.4.3 Verzeichnis von Verarbeitungstätigkeiten

Um personenbezogene Daten nach Maßgaben der DSGVO schützen zu können, muss das verantwortliche Unternehmen zunächst ermitteln, in welchen Fällen personenbezogene Daten – z. B. von Kunden, Lieferanten oder Beschäftigten – erhoben und verarbeitet werden. Als erster Anhaltspunkt bietet sich an, alle Systeme bzw. Tools im Unternehmen aufzulisten, in denen personenbezogene Daten gespeichert werden (z. B. Zeiterfassungssystem, CRM-System, Bewerbertool, HR-Managementtool etc.). Eine solche Vorgehensweise erscheint doppelt sinnvoll: Zum einen können die Datenflüsse im Unternehmen entsprechend erkannt und beschrieben werden. Ferner ist damit auch ein erster Schritt für die Erstellung der Übersicht über die Verarbeitungstätigkeiten getan (zu den Inhalten eines Verzeichnisses von Verarbeitungstätigkeiten s. Kap. 6.2.4.3, S. 62 f.).[32]

8.4.4 Datenschutz-Folgenabschätzung

Daneben sind Unternehmen in bestimmten Fällen verpflichtet, eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen. Diese sind durchzuführen, wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko für personenbezogenen Daten verursacht, insbesondere bei neuen Technologien oder aufgrund ihres Wesens, ihres Umfangs, ihres Kontexts oder ihrer Zwecke (s. auch Kap. 7, v. a. Kap. 7.2.4, S. 71 ff.). Die Aufsichtsbehörden für den Datenschutz sind gehalten, Listen von Verarbeitungsvorgängen zu erstellen, bei denen typischerweise Folgenabschätzungen nach Art. 35 DSGVO vorgeschrieben sind (sog. Positivlisten). Ebenso erstellen die Datenschutz-Aufsichtsbehörden Listen von Vorgängen, bei denen Folgenabschätzungen entbehrlich sind (sog. Negativlisten).[33]

32 s. hierzu auch: Bayerisches Landesamt für Datenschutzaufsicht (Hg.): Muster 9. Online-Shop – Verzeichnis von Verarbeitungstätigkeiten. o. D. Online: https://www.lda.bayern.de/media/muster_9_online-shop_verzeichnis.pdf (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e. V. (Hg.): GDD-Praxishilfe Verzeichnis von Verarbeitungstätigkeiten – Verantwortlicher, Version 2.1. April 2022. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfeDSGVOVerzeichnisvonVerarbeitungsttigkeiten.pdf (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e. V. (Hg.): GDD-Praxishilfe DS-GVO Vb. Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter. Januar 2020. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_5bVVTAuftragsverarbeiter.pdf (abgerufen am 11.05.2022).

33 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP248rev.01. Oktober 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_de (abgerufen am 11.05.2022); Europäischer Datenschutzausschuss (Hg.): Empfehlung 01/2019 zu der vom Europäischen Datenschutzbeauftragten entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725). Juli 2019. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendation_201901_edps_39.4_dpia_list_de.pdf (abgerufen am 11.05.2022).

8.4.5 Vertragsmanagement

Im Rahmen des Vertragsmanagements empfiehlt es sich, alle von einem Unternehmen eingesetzten Dienstleister in einer gesonderten Dokumentation zusammenzufassen – im ersten Schritt auch zunächst unabhängig davon, ob dabei personenbezogenen Daten verarbeitet werden oder nicht. Danach ist seitens des Datenschutzbeauftragten zu prüfen, ob durch den Dienstleister personenbezogene Daten erhoben, genutzt, übermittelt oder verarbeitet bzw. anderweitig verwendet werden. Ferner ist zu prüfen, ob und in welcher Form eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO erforderlich ist und ob diese bereits abgeschlossen wurde, dabei ist auch zu untersuchen, ob nicht eine Anpassung oder gar Neufassung aufgrund der neuen Rechtslage (Gültigkeit der DSGVO) erforderlich wird.

Empfehlung: Überprüfung abzuschließender Verträge mit Datenschutzrelevanz auf DSGVO- Konformität, darunter insbesondere

- vertragliche Regelungen im Zusammenhang mit Outsourcingverhältnissen,
- Verträge über die Übermittlung personenbezogener Daten,
- sonstige Verträge, welche die Verarbeitung personenbezogener Daten betreffen.

8.4.6 Verpflichtung auf das Datengeheimnis

Die Mitarbeiter sollten auch weiterhin auf das Datengeheimnis verpflichtet werden, auch wenn dies in der Datenschutzgrundverordnung nicht mehr ausdrücklich geregelt ist. Davon umfasst ist insbesondere die Verarbeitung ausschließlich auf Basis einer Rechtmäßigkeitsgrundlage unter Beachtung der Zweckbindung und Wahrung der Vertraulichkeit. Eine solche Verpflichtung kann als erste Maßnahme zur Sensibilisierung der Mitarbeiter angesehen werden.[34]

34 s. hierzu auch: Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO XI. Verpflichtung auf die Vertraulichkeit. Dezember 2017. Online: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf (abgerufen am 11.05.2022).

8.4.7 Datenschutz-Schulung

Die Beschäftigten sind regelmäßig zu den datenschutzrechtlichen Anforderungen und deren Umsetzung im Unternehmen zu sensibilisieren. Je nach Tätigkeit kann dies auch jährlich erforderlich sein. Die Datenschutz-Schulung und die Verpflichtung auf das Datengeheimnis sind beide als Teil der organisatorischen Maßnahmen anzusehen, die dem Schutz der personenbezogenen Daten dienen. In der Praxis werden die Schulungen häufig dem Datenschutzbeauftragten übertragen.

8.4.8 Prozess zur Wahrnehmung von Betroffenenrechten

Bevor ein Prozess zur Wahrnehmung von Betroffenenrechten implementiert werden kann, muss der Verantwortliche sich klar machen, welche Rechte die Betroffenen überhaupt haben (s. auch Kap. 6.1, S. 43 ff.).

9. Zertifizierung

Durch die Datenschutzgrundverordnung sind auf EU-Ebene erstmals auch rechtliche Rahmenbedingungen für datenschutzspezifische Zertifizierungsverfahren eingeführt worden. Hiernach können genehmigte Zertifizierungsverfahren herangezogen werden, um die Erfüllung rechtlicher Anforderungen nachzuweisen. Kleine und mittlere Unternehmen können sich dies in zweifacher Hinsicht zunutze machen: Zum einen können sie selbst ein Zertifizierungsverfahren durchlaufen und sich hierdurch einen Wettbewerbsvorteil verschaffen, zum anderen können sie insbesondere im Bereich der Auftragsverarbeitung Haftungsrisiken minimieren, indem sie auf zertifizierte Anbieter zurückgreifen.[35] Die nachfolgenden Ausführungen geben einen Überblick über die insoweit einschlägigen Regelungen der DSGVO und des BDSG und informieren über den aktuellen Sachstand bezüglich der Etablierung genehmigter Zertifizierungsverfahren.

Die Datenschutzgrundverordnung betrachtet Zertifizierungen als ein wichtiges Instrument zum Nachweis der Einhaltung datenschutzrechtlicher Pflichten. So kann ein genehmigtes Zertifizierungsverfahren als Faktor herangezogen werden, um Folgendes nachzuweisen:

- die Erfüllung der Pflichten des für einen Verarbeitungsvorgang Verantwortlichen (Art. 24 Abs. 3 DSGVO),
- die Einhaltung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutz-freundliche Voreinstellungen (Art. 25 Abs. 3 DSGVO),
- die Einhaltung rechtlicher Anforderungen an Auftragsverarbeiter (Art. 28 Abs. 5 DSGVO) sowie
- die Implementierung geeigneter technischer und organisatorischer Maßnahmen (Art. 32 Abs. 3 DSGVO).

Dementsprechend wird eine erteilte Zertifizierung bei der Entscheidung über die Verhängung einer Geldbuße und deren Betrag gebührend (positiv) berücksichtigt (Art. 83 Abs. 2 lit. j DSGVO). Eine erteilte Zertifi-

35 Auch bei der Beschaffung von Hard- und Software ist es sinnvoll, auf zertifizierte Produkte zurückzugreifen. Insoweit ist aber darauf hinzuweisen, dass Hard- und Software als solche nicht dem Anwendungsbereich von Art. 42 f. DSGVO („Verarbeitungsvorgänge") unterfallen, weshalb es sich bei entsprechenden Zertifizierungen nicht um genehmigte Zertifizierungen im Sinne der DSGVO handeln kann.

zierung mindert allerdings nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung der Bestimmungen der DSGVO und berührt auch nicht die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden (Art. 42 Abs. 4 DSGVO). Zertifiziert werden können Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern (Art. 42 Abs. 1 S. 1 DSGVO). Hierdurch soll betroffenen Personen ein rascher Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglicht werden (EG 100).

Einen Spezialfall regelt Art. 46 Abs. 2 lit. f DSGVO, wonach eine Übermittlung personenbezogener Daten in ein Drittland außerhalb des Europäischen Wirtschaftsraums durch einen genehmigten Zertifizierungsmechanismus zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland legitimiert werden kann. Neben anderen geeigneten Garantien wie Standarddatenschutzklauseln und verbindlichen internen Datenschutzvorschriften („Binding Corporate Rules“) nebst eventuell erforderlicher zusätzlicher Maßnahmen wird Unternehmen in Zukunft bei Drittstaatentransfers also auch diese Möglichkeit der Legitimation zur Verfügung stehen. Auf diesen Spezialfall wird nachfolgend allerdings nicht näher eingegangen, da viele grundsätzliche Fragestellungen hierzu derzeit noch ungeklärt sind.[36]

Eine Zertifizierung ihrer eigenen Verarbeitungsvorgänge ist für kleine und mittlere Unternehmen insbesondere dann interessant, wenn ihre Kerntätigkeit darin besteht, personenbezogene Daten im Auftrag ihrer Kunden zu verarbeiten. In einer solchen Konstellation kann ein offiziell anerkanntes Datenschutzzertifikat gerade im B2B-Kontext ein wichtiges Argument für potenzielle Kunden sein, sich für das zertifizierte Unternehmen zu entscheiden. In der Praxis war schon vor dem Geltungsbeginn der DSGVO zu beobachten, dass Datenschutzzertifizierungen im Rahmen von Ausschreibungen eine Rolle spielen – zudem sahen verschiedene Landesdatenschutzgesetze eine Verpflichtung für öffentliche Stellen vor, zertifizierte Produkte und Verfahren vorrangig einzusetzen.[37] Ein offiziell anerkanntes Zertifikat wird schließlich im Regelfall Vor-Ort-Prüfungen der Kunden beim Auftragsverarbeiter (vgl. Art. 28 Abs. 3 S. 2, lit. h DSGVO) ent-

36 Der Europäische Datenschutzausschuss arbeitet an Leitlinien zur Zertifizierung als Übermittlungstool. Diese sind bislang aber noch nicht verabschiedet worden (Stand: 01/2022).
37 vgl. auch Erwägungsgrund 78 DSGVO, letzter Satz.

behrlich machen, so dass dem zertifizierten Unternehmen keine Aufwände durch solche Prüfungen entstehen.

Die Datenschutzgrundverordnung sieht ausdrücklich vor, dass den besonderen Bedürfnissen von kleinen und mittleren Unternehmen Rechnung getragen wird (Art. 42 Abs. 1 S. 2 DSGVO).

Gemäß Art. 42 Abs. 5 S. 1 DSGVO werden Zertifizierungen nach erfolgreichem Durchlaufen eines transparenten Verfahrens (Art. 42 Abs. 3 DSGVO) durch eine Zertifizierungsstelle (vgl. Art. 43 DSGVO) oder durch die zuständige Aufsichtsbehörde erteilt. Erfolgt die Erteilung durch eine Zertifizierungsstelle, so teilt diese der zuständigen Aufsichtsbehörde die Gründe für die Erteilung der beantragten Zertifizierung mit (Art. 43 Abs. 5 DSGVO). Die Erteilung von Zertifizierungen darf nur durch Zertifizierungsstellen erfolgen, die hierfür akkreditiert worden sind. Zertifizierungsstellen sollen von einer oder beiden der folgenden Stellen akkreditiert werden: der zuständigen Aufsichtsbehörde (Art. 55 oder 56 DSGVO) oder der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 benannt wurde.

Die DSGVO gibt den EU-Mitgliedstaaten damit die Möglichkeit, sich für eine dieser Optionen zu entscheiden. Die entsprechende Entscheidung des deutschen Gesetzgebers lässt sich § 39 BDSG entnehmen: Hiernach erfolgt die Erteilung der Befugnis, als Zertifizierungsstelle tätig zu werden, durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige Aufsichtsbehörde auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle (DAkkS). Dies bedeutet, dass Datenschutzaufsichtsbehörden und DAkkS im Rahmen von Akkreditierungsverfahren eng zusammenarbeiten müssen. Einzelheiten zum Ablauf eines solchen Verfahrens lassen sich der Übersicht „Akkreditierungsprozess für den Bereich „Datenschutz" gemäß Art. 42, 43 DSGVO" der Datenschutzkonferenz (DSK) entnehmen.[38]

Die einzuhaltenden Zertifizierungskriterien müssen von der zuständigen Aufsichtsbehörde genehmigt werden (Art. 42 Abs. 5 S. 1 i. V. m. Art. 58 Abs. 3 DSGVO) und werden von dieser in leicht zugänglicher Form veröffentlicht (Art. 43 Abs. 6 S. 1 DSGVO). Werden die Kriterien vom Europäischen Datenschutzausschuss (Art. 68 ff. DSGVO) genehmigt, kann

38 vgl. Datenschutzkonferenz (Hg.): Schematische Darstellung „Akkreditierungsprozess für den Bereich ‚Datenschutz' gemäß Art. 42, 43 DS-GVO". Version 1.0 (15.03.2019). Online: https://www.datenschutzkonferenz-online.de/media/oh/20190315_oh_akk_c.pdf (abgerufen am 11.05.2022).

dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen (Art. 42 Abs. 5 S. 2 DSGVO). Eine solche gemeinsame Zertifizierung hätte für zertifizierte Unternehmen den großen Vorteil, dass die Gültigkeit eines erlangten Zertifikats nicht auf einen einzelnen EU-Mitgliedstaat beschränkt wäre.

Zertifizierungen werden für eine Höchstdauer von drei Jahren erteilt und können verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden (Art. 42 Abs. 7 S. 1 DSGVO). Eine erteilte Zertifizierung wird gegebenenfalls durch die Zertifizierungsstelle oder durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden (Art. 42 Abs. 7 S. 2 DSGVO). Alle Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen werden vom Europäischen Datenschutzausschuss in ein Register aufgenommen und in geeigneter Weise veröffentlicht (Art. 42 Abs. 8 DSGVO).

Art. 42 Abs. 1 S. 1 DSGVO fordert die Mitgliedstaaten der Europäischen Union, die EU-Kommission und die Datenschutzaufsichtsbehörden dazu auf, die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen insbesondere auf EU-Ebene zu fördern. Diese Förderpflicht spiegelt sich auch in den Aufgaben und Befugnissen der Datenschutzaufsichtsbehörden (Genehmigung von Kriterien, Mitwirkung an der Akkreditierung von Zertifizierungsstellen etc.) wider.

Trotz der soeben skizzierten Förderpflicht gibt es bislang keine genehmigten Zertifizierungsverfahren im Sinne der DSGVO. Dies gilt nicht nur für Deutschland, sondern für die gesamte Europäische Union. Gründe hierfür sind die hohe Komplexität der Materie an sich sowie die von Zertifizierungsstellen zu durchlaufenden Akkreditierungsverfahren, für deren Entwicklung zudem erst einmal eine Vielzahl von Abstimmungsprozessen auf nationaler[39] wie auch auf EU-Ebene durchlaufen werden mussten. Gegenwärtig ist davon auszugehen, dass die ersten genehmigten Zertifizierungsverfahren im Verlauf des Jahres 2022 zur Verfügung stehen werden.[40]

39 so jedenfalls in Deutschland

40 Christiane Schulzki-Haddouti: Meldung auf heise online: „Meldung vom Datenschutz: DSGVO-Zertifizierung kommt 2022“ vom 29.11.2021. Online: https://www.heise.de/news/Datenschutz-DSGVO-Zertifizierung-kommt-2022-6278967.html (abgerufen am 11.05.2022).

10. Der Datenschutzbeauftragte

10.1 Einführung

Um das Recht von Kunden, Beschäftigten etc. auf den Schutz personenbezogener Daten effektiv sicherzustellen, bedarf es der angemessenen Überwachung von solchen Stellen, die personenbezogene Informationen verarbeiten. Eine solche Kontrolle erfolgt zum einen von außen, nämlich durch die Datenschutzaufsichtsbehörden sowie Verbraucherschutzverbände. Letzteren stehen im Fall von Datenschutzverstößen Möglichkeiten der kollektiven Rechtsdurchsetzung zu. Die Einhaltung des Datenschutzes kann zum anderen aber auch von den betroffenen Personen selbst kontrolliert werden, insbesondere über die Ausübung der Betroffenenrechte nach Art. 12 ff. DSGVO. Komplettiert wird das Überwachungssystem durch den Datenschutzbeauftragten und, sofern vorhanden, den Betriebs- oder Personalrat, welche als Selbstkontrollorgane agieren. Während der Betriebs- bzw. Personalrat allerdings nur für die Verarbeitung von Beschäftigtendaten zuständig ist, bezieht sich der Überwachungsauftrag des Datenschutzbeauftragten auf alle Datenverarbeitungen mit Personenbezug.

Die Funktion des Datenschutzbeauftragten ist jedoch nicht allein auf die Überwachung des Datenschutzes beschränkt. Eine weitere Kernaufgabe liegt in der datenschutzrechtlichen Beratung und Unterstützung der benennenden Stelle sowie der dort Beschäftigten.

10.2 Voraussetzungen der Benennungspflicht

10.2.1 Benennungspflicht nach DSGVO

Nach der DSGVO ist ein Datenschutzbeauftragter in folgenden Fällen verpflichtend zu benennen (vgl. Art. 37 Abs. 1):

- Art. 37 Abs. 1 lit. a DSGVO: Personenbezogene Datenverarbeitung durch Behörde/öffentliche Stelle (Ausnahme: justizielle Tätigkeit)
- Art. 37 Abs. 1 lit. b DSGVO: Die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters besteht in Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke

eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.

- Art. 37 Abs. 1 lit. c DSGVO: Die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten (Art. 9 DSGVO) oder von Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO).

Zur „Kerntätigkeit" zählen alle Geschäftsbereiche, die entscheidend sind für die Umsetzung der Unternehmensstrategie, die ihren Ausdruck findet in Kundenservice, Marketing, Produktdesign etc. Keine Aktivitäten in diesem Sinne sind routinemäßige Verwaltungs- und Erhaltungsaufgaben. Es genügt also, wenn die die Benennungspflicht auslösende Tätigkeit einen Hauptzweck der betreffenden Stelle darstellt. „Beobachtung" meint umfangreiche regelmäßige und systematische personenbezogene Auswertungen, insbesondere die Vornahme von Profilbildungen.[41]

Beispiele für Benennungspflicht nach Art. 37 Abs. 1 lit. b DSGVO: Auskunfteien; Detekteien; Versicherungsunternehmen (Risikomanagement oder individualisierte Tarife wie „Pay as you drive"); Marketing auf Basis detaillierter Kunden- und Interessentenprofile.

Beispiele für Benennungspflicht nach Art. 37 Abs. 1 lit. c DSGVO: Gesundheitseinrichtungen, wie z. B. Krankenhäuser; mit genetischen Untersuchungen befasste Labors; Beratungsstellen wie Pro Familia; Dienstleister im biometrischen ID-Management oder Anbieter von Erotikartikeln.

41 s. hierzu auch: Datenschutzkonferenz (Hg.): Kurzpapier Nr. 13. Auftragsverarbeitung, Art. 28 DSGVO. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf (abgerufen am 11.05.2022).

10.2.2 Benennungspflicht nach BDSG

Hinweis: Nach § 38 Abs. 1 Satz 1 BDSG haben Verantwortliche und Auftragsverarbeiter ergänzend zu den Vorgaben der DSGVO einen Datenschutzbeauftragten zu benennen, *soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.* Zudem schreibt § 38 Abs. 1 Satz 2 BDSG vor, dass schwellenwertunabhängig ein Datenschutzbeauftragter zu benennen ist, sofern der Verantwortliche oder Auftragsverarbeiter Verarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO)[16] unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet.

Der 20-Personen-Schwellenwert muss in der Regel erreicht werden. Maßgeblich ist die Anzahl der normalerweise mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen. Entscheidend ist, ob der Schwellenwert über einen Zeitraum von einem Jahr erreicht wurde bzw. im Rahmen einer vorausschauenden Betrachtung erreicht werden wird. „Ständig" beschäftigt ist die Person, wenn sie die Aufgabe, die nicht ihre Hauptaufgabe zu sein braucht, regelmäßig wahrnimmt. Nicht notwendig ist insoweit, dass der Umgang mit personenbezogenen Daten den Kern der Tätigkeit des Beschäftigten bildet, wie dies z. B. bei Mitarbeitern der Personalabteilung der Fall ist. Ausreichend ist vielmehr, dass im Rahmen der konkreten Tätigkeit auch mit personenbezogenen Daten umgegangen wird. Dies ist bereits bei Anbindung an Kommunikationssysteme wie z. B. Outlook und/oder Zugriff auf unternehmenseigene Adressverzeichnisse der Fall. Solche Mitarbeiter sind im Hinblick auf die Benennungspflicht ebenso mitzuzählen wie Mitarbeiter, die keine weiteren Kompetenzen haben, als sich personenbezogene Daten anzeigen zu lassen.

10.2.3 Freiwillige Benennung

Art. 37 Abs. 4 DSGVO stellt klar, dass die freiwillige Benennung unbenommen ist. Entscheidendes Argument für eine Benennung auch ohne Pflicht ist, dass Datenschutzbeauftragte einen zentralen Beitrag zur Gewährleistung von Datenschutzkonformität und damit zur Vermeidung von Unternehmensrisiken darstellen.

10.2.4 Übersicht zur Benennungspflicht

Überblick: Wann ist ein Datenschutzbeauftragter zu benennen?

Öffentliche Stelle:

→ *immer*

Durch die Festlegung auf europäischer Ebene in Art. 37 Abs. 1 lit a DSGVO haben öffentliche Stellen immer einen Datenschutzbeauftragten zu benennen.

Nichtöffentliche Stellen:

→ *schwellenwertabhängig*

in der Regel sind mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt

→ *Unabhängig vom Erreichen des Schwellenwertes in folgenden Fällen:*

- Datenschutz-Folgenabschätzung (Art. 35 DSGVO),[42]
- Geschäftsmäßige Verarbeitung personenbezogener Daten zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung
- Kerntätigkeit, die eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich macht
- Kerntätigkeit, die in der umfangreichen Verarbeitung besonderer Kategorien von Daten (Art. 9 DSGVO) oder von Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) besteht

10.3 Aufgaben des Datenschutzbeauftragten

10.3.1 Allgemeines

Nach Art. 39 Abs. 1 und Art. 38 Abs. 4 DSGVO hat der Datenschutzbeauftragte folgende zwingende Mindestaufgaben:

- Unterrichtung und Beratung des Verantwortlichen bzw. des Auftragsverarbeiters und der Beschäftigten hinsichtlich bestehender datenschutzrechtlicher Verpflichtungen (Art. 39 Abs. 1 lit. a),

42 Von den Aufsichtsbehörden veröffentlichte sog. Blacklists (Art. 35 Abs. 4 DSGVO) haben zu einer ersten Konturierung der Voraussetzungen geführt, unter denen eine Datenschutz-Folgenabschätzung durchzuführen ist, vgl. Datenschutzkonferenz (Hg.): Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist. Version 1.1. Oktober 2018. Online: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf (abgerufen am 11.05.2022).

- Überwachung der Einhaltung des Datenschutzes (Art. 39 Abs. 1 lit. b);
- Beratung – auf verpflichtende[43] Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und Überwachung ihrer Durchführung (Art. 39 Abs. 1 lit. c),
- Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als deren Anlaufstelle (Art. 39 Abs. 1 lit. d und e),
- Ansprechpartner für die betroffenen Personen zu allen mit der Verarbeitung ihrer Daten und mit der Wahrnehmung ihrer Rechte aus der Verordnung im Zusammenhang stehenden Fragen (Art. 38 Abs. 4).

Kernaufgaben bilden die Beratung und Überwachung des Verantwortlichen bzw. Auftragsverarbeiters und der konkret mit der Datenverarbeitung beschäftigten Personen.

„Unterrichtung" ist hierbei im Sinne einer allgemeinen Information über bestehende datenschutzrechtliche Verpflichtungen zu verstehen, Beratung als Unterstützung bei der Lösung von konkreten datenschutzrechtlichen Fragestellungen, etwa der Entwicklung von Datenschutzstrategien des Verantwortlichen oder Auftragsverarbeiters.

„Überwachung" bedeutet ein Vorgehen, bei dem eventuelle Abweichungen zwischen einem Ist- und Sollzustand festgestellt werden sollen. Ausgangspunkt ist die Überprüfung der vom Verantwortlichen bzw. Auftragsverarbeiter selbst vorgegebenen Datenschutzstrategien, wie z. B. Richtlinien/Policies, Arbeits-/Dienstanweisungen oder Betriebsvereinbarungen, bezüglich ihrer Vereinbarkeit mit den datenschutzrechtlichen Vorgaben. Steht die Rechtskonformität der internen Datenschutzvorgaben und der allgemeinen datenschutzrechtlichen Rahmenbedingungen fest, kann der Abgleich der konkreten Datenverarbeitungstätigkeiten mit den Datenschutzstrategien der Einrichtung sowie den gesetzlichen Anforderungen erfolgen. Konsequenzen aus den Empfehlungen des Datenschutzbeauftragten zu ziehen, ist Aufgabe der benennenden Stelle. Dem Datenschutzbeauftragten fehlen die diesbezüglichen Weisungs- und Entscheidungsbefugnisse.

43 Vgl. Art. 35 Abs. 2 DSGVO.

Hinweis: *Der Datenschutzbeauftragte ist nicht für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich!* Die Verantwortung für den Datenschutz kann dem Datenschutzbeauftragten auch nicht übertragen werden, da sich dieser dann selbst überwachen müsste und es ihm insofern als internem Überwachungsorgan an der nötigen Unabhängigkeit fehlen würde.[44]

Nach Art. 39 Abs. 1 DSGVO arbeitet der Datenschutzbeauftragte mit der Datenschutzaufsichtsbehörde zusammen und fungiert als deren „Anlaufstelle" beim für die Verarbeitung Verantwortlichen, d. h., er ist erster Ansprechpartner für die Behörde und koordiniert den Kontakt mit der datenschutzrechtlich verantwortlichen Leitung und der zuständigen Fachabteilung. Zudem berät er sich mit der zuständigen Behörde „zu allen sonstigen Fragen". Wichtig im Verhältnis zwischen Aufsichtsbehörde und Datenschutzbeauftragtem ist, dass es sich um voneinander unabhängige Überwachungsorgane handelt. Der Datenschutzbeauftragte ist nicht verlängerter Arm der Behörde, sondern zur eigenständigen Meinungsbildung berechtigt und verpflichtet.

Im Rahmen der Funktion als Ansprechpartner der betroffenen Personen (Art. 38 Abs. 4 DSGVO) ist der Datenschutzbeauftragte verpflichtet, Datenschutzbeschwerden zu prüfen und die betroffenen Personen über das Ergebnis der Prüfung zu informieren. Stellt er Datenschutzverletzungen fest, z. B. die Missachtung von Betroffenenrechten, hat er darauf hinzuwirken, dass diese vom Verantwortlichen abgestellt werden. Mit dieser Aufgabe hängt die Verpflichtung des Datenschutzbeauftragten zur Wahrung der Vertraulichkeit eng zusammen.[45]

44 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), WP243rev.01. April 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_de (abgerufen am 11.05.2022).

45 s. hierzu auch: Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO I. Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung. Juli 2019. Online: https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0 (abgerufen am 11.05.2022); Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (Hg.): Das berufliche Leitbild der Datenschutzbeauftragten/Code of Practice for Data Protection Officers. April 2018. Online: https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf (abgerufen am 11.05.2022).

10.3.2 Übertragung weiterer Aufgaben an den Datenschutzbeauftragten

Gemäß Art. 38 Abs. 6 DSGVO ist es dem Datenschutzbeauftragten ausdrücklich gestattet, auch andere Aufgaben und Pflichten wahrzunehmen (sog. nebenamtlicher Datenschutzbeauftragter oder Teilzeit-Datenschutzbeauftragter). Die Zulässigkeit der Wahrnehmung anderer Aufgaben und Pflichten steht allerdings unter dem Vorbehalt, dass diese nicht zu einem Interessenkonflikt mit der Tätigkeit als DSB führen dürfen.

So ist es unzulässig, das Amt Personen der Leitungs-, Chef- und Inhaberebene zu übertragen. Nachgeordnete Personen mit Führungsaufgaben und Entscheidungskompetenz über die Festlegung von Zwecken und Mitteln der Datenverarbeitung, wie etwa IT-, Marketing- oder HR-Leitern, dürfen ebenfalls nicht benannt werden.[46]

10.3.3 Pflicht zur risikoorientierten Tätigkeit

Gemäß Art. 39 Abs. 2 DSGVO hat der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung zu tragen, wobei ausschlaggebend für die Risikobewertung insbesondere Art, Umfang, Umstände und Zwecke der Verarbeitung sind.

Die Verpflichtung des Datenschutzbeauftragten zur risikoorientierten Tätigkeit entspricht dem risikobasierten Ansatz, welcher die DSGVO insgesamt durchzieht. Der Datenschutzbeauftragte hat seine Tätigkeiten nach Priorität zu ordnen und seine Anstrengungen auf Sachverhalte zu konzentrieren, von denen besondere Bedrohungen für die betroffenen Personen ausgehen. Insbesondere mit Verarbeitungen, die aufgrund des hohen Risikos für die Rechte und Freiheiten der betroffenen Personen einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) bedürfen, wird der Datenschutzbeauftragte sich regelmäßig zeitnah befassen müssen.

46 Vgl. LfDI BW (Hg.): Praxisratgeber: Die/der Beauftragte für den Datenschutz. Teil II: Persönliche Voraussetzungen Durchführung der Benennung Stellung und Aufgaben Beendigung der Benennung. November 2019. Abschnitt I.3. Online: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/11/Praxisratgeber-LfDI-BW-Der-Beauftragte-f%C3%BCr-den-Datenschutz-Teil-II.pdf (abgerufen am 11.05.2022).

10.4 Rechtsstellung des Datenschutzbeauftragten

10.4.1 Unabhängigkeit und organisatorische Einordnung

Die Unabhängigkeit ist Kern der Rechtsstellung des Datenschutzbeauftragten. Als übergeordnete Gewährleistung wird diese in EG 97 der DSGVO angesprochen. Konkrete Einzelausprägungen der Unabhängigkeit finden sich in Art. 38 Abs. 3 DSGVO: „Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters."

In der Datenschutzliteratur ist umstritten, ob der letzte Satz ausschließlich als Vorgabe eines Berichtswegs zu verstehen ist oder zugleich auch als organisatorische Anforderung, die es verbietet, den Datenschutzbeauftragten einer anderen Stelle als unmittelbar der Leitung des Unternehmens bzw. der öffentlichen Stelle zu unterstellen. Hierfür spricht, dass die Verortung unmittelbar unter der Leitung die konsequente organisatorische Umsetzung der in EG 97 Satz 4 DSGVO vorgesehenen vollständigen Unabhängigkeit des Datenschutzbeauftragten ist.

10.4.2 Abberufungsschutz, Kündigungsschutz und Benachteiligungsverbot

Zum Schutz des Datenschutzbeauftragten gewährleistet die DSGVO Abberufungsschutz sowie ein Benachteiligungsverbot (Art. 38 Abs. 3 Satz 2 DSGVO). Der Datenschutzbeauftragte darf vom Verantwortlichen oder Auftragsverarbeiter wegen der Erfüllung der Aufgaben nicht abberufen oder benachteiligt werden. Möglich ist jedoch nach der DSGVO ein betriebsbedingter Wegfall der Benennung.

Restriktiver als der europäische Gesetzgeber hat der bundesdeutsche Gesetzgeber die Zulässigkeit der Abberufung geregelt. Nach § 6 Abs. 4 S. 1 BDSG soll die Abberufung nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs, d. h. „aus wichtigem Grund" zulässig sein. Zweck dieses erweiterten nationalen Abberufungsschutzes ist es, dass einem unbequemen

Datenschutzbeauftragten nicht einfach das Amt entzogen werden können soll, da dies die effektive Amtsausübung gefährden würde. Allein der Abberufungsschutz nach DSGVO bietet insofern keinen ausreichenden Schutz.

Einen arbeitsrechtlichen Schutz des Datenschutzbeauftragten sieht die DSGVO nicht vor. Der nationale Gesetzgeber hat sich jedoch entschieden, verpflichtend zu benennenden internen Datenschutzbeauftragten nicht nur erweiterten Abberufungsschutz, sondern auch arbeitsrechtlichen Kündigungsschutz einzuräumen (§ 6 Abs. 4 S. 2 und 3 BDSG, für nichtöffentliche Stellen i. V. m. § 38 Abs. 2 BDSG). Danach ist die Kündigung des Arbeitsverhältnisses eines Datenschutzbeauftragten unzulässig, es sei denn, dass Tatsachen vorliegen, welche zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen, also zu einer außerordentlichen Kündigung. Es besteht damit ein Gleichlauf zwischen den Voraussetzungen an die Abberufung und denjenigen an die Kündigung des Datenschutzbeauftragten.

10.4.3 Anspruch auf Einbindung, Unterstützung und Fortbildung

Eine erfolgreiche Tätigkeit als Datenschutzbeauftragter hängt wesentlich von der Unterstützung seitens der benennenden Stelle ab. Dem trägt die DSGVO Rechnung, indem sie einen Anspruch des Datenschutzbeauftragten auf Einbindung und Unterstützung vorsieht (Art. 38 Abs. 1 und 2 DSGVO), der im Einzelnen Folgendes umfasst:

- ordnungsgemäße und frühzeitige Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen,
- Unterstützung bei der Aufgabenerfüllung,
- Ressourcen zur Aufgabenwahrnehmung/Erhaltung des Fachwissens sowie
- Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen.

Zur notwendigen Unterstützung gehört insbesondere, dass dem Datenschutzbeauftragten die notwendigen zeitlichen Ressourcen zur Wahrnehmung der Aufgabe zur Verfügung gestellt werden. Das konkrete Maß der erforderlichen Unterstützung ist im Einzelfall zu bestimmen.[47]

47 Zu den insoweit maßgeblichen Kriterien vgl. Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO I. Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung. Juli 2019, S. 11. Online:

10.4.4 Verpflichtung zur Wahrung der Vertraulichkeit

Die Wahrung der Vertraulichkeit ist essenziell für eine effektive Ausübung der Tätigkeit als Datenschutzbeauftragter. Art. 38 Abs. 5 DSGVO verpflichtet den Datenschutzbeauftragten insofern zur Wahrung der Geheimhaltung bzw. Vertraulichkeit bei der Aufgabenerfüllung, überlässt allerdings die nähere Ausgestaltung dieser Verpflichtung dem Unionsrecht bzw. dem Recht der Mitgliedstaaten. Auf Art. 38 Abs. 5 DSGVO beruht § 6 Abs. 5 Satz 2 i. V. m. § 38 Abs. 2 BDSG, wonach der Datenschutzbeauftragte zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf diese zulassen, verpflichtet ist, soweit er nicht von dieser befreit wird. Datenschutzbeauftragte, die für einen Berufsgeheimnisträger tätig sind, können sich bei Verletzung der Vertraulichkeit strafbar machen (§ 203 Abs. 4 Satz 1 StGB). Solchen Datenschutzbeauftragten steht zur Absicherung der Verschwiegenheit ein Zeugnisverweigerungsrecht zu (§ 6 Abs. 6 i. V. m. § 38 Abs. 2 BDSG).

10.5 Anforderungen an den Datenschutzbeauftragten

Der Düsseldorfer Kreis, der frühere Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich, hat 2010 Mindestanforderungen an Fachkunde und Unabhängigkeit der betrieblichen Beauftragten für den Datenschutz aufgestellt,[48] die sinngemäß auch heute noch herangezogen werden können.[49] Nach dem Beschluss soll die zu benennende Person mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der benennenden Stelle:

- Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten,
- umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die Verantwortlichen einschlägigen Regelungen, auch technischer und organisatorischer Art,

https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0 (abgerufen am 11.05.2022).

48 Düsseldorfer Kreis, Beschluss vom 24./25.11.2010 zu den Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 BDSG.

49 vgl. LfDI BW (Hg.): Vgl. LfDI BW (Hg.): Praxisratgeber: Die/der Beauftragte für den Datenschutz. Teil II: Persönliche Voraussetzungen Durchführung der Benennung Stellung und Aufgaben Beendigung der Benennung. November ²2019. S. 6. Online: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/11/Praxisratgeber-LfDI-BW-Der-Beauftragte-f%C3%BCr-den-Datenschutz-Teil-II.pdf (abgerufen am 11.05.2022)

- Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen.

Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur des Verantwortlichen und der Sensibilität der zu verarbeitenden Daten:

- Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
- Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen etc.),
- betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),
- Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung beim zu betreuenden Verantwortlichen (Aufbau- und Ablaufstruktur bzw. Organisation beim Verantwortlichen) und
- Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Die Anforderungen an das notwendige Fachwissen sind nicht fix, sondern orientieren sich am Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten (EG 97). Je komplexer die Datenverarbeitung der benennenden Stelle und je sensibler die Daten, desto höhere Anforderungen sind auch an die Qualifikation zu stellen.[50]

Nach der DSGVO muss der Datenschutzbeauftragte grundsätzlich bereits bei Benennung über ausreichendes Fachwissen verfügen. Zu Beginn der Benennung eventuell noch bestehende Informationsdefizite sind zeitnah auszugleichen.

50 s. hierzu auch: Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (Hg.): Das berufliche Leitbild der Datenschutzbeauftragten/Code of Practice for Data Protection Officers. April 2018. Online: https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf (abgerufen am 11.05.2022).

10.6 Anforderungen an die Benennung

10.6.1 Optionen bei Benennung

Nach Art. 37 Abs. 6 DSGVO kann Datenschutzbeauftragte Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein (sog. interner Datenschutzbeauftragter) oder die Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen (sog. externer Datenschutzbeauftragter).

Der Einsatz eines externen Datenschutzbeauftragten kann insbesondere bei kleinen und mittleren Unternehmen sinnvoll sein. Für die Entscheidung zugunsten einer externen Person spricht, dass deren Expertise und Erfahrungen sofort in Anspruch genommen werden können und der initiale Aufwand für die Ausbildung eines eigenen Mitarbeiters entfällt. Vorteile eines internen Datenschutzbeauftragten sind demgegenüber die regelmäßig bessere Kenntnis der Prozesse und Spezifika des Verantwortlichen bzw. Auftragsverarbeiters.

In Konzernen und Unternehmensgruppen mit mehreren juristisch selbstständigen Unternehmen kann sich die Benennung eines „Konzerndatenschutzbeauftragten" – in der Terminologie der DSGVO: „gemeinsamer Datenschutzbeauftragter", Art. 37 Abs. 2 DSGVO – empfehlen, um eine konzernweite Datenschutzpolitik/-strategie sowie einheitliche Empfehlungen, Vorgaben und Prozesse in Form von Mindeststandards zu etablieren.[51] Bei denjenigen Konzernunternehmen, für die er zwar benannt, bei denen er jedoch nicht beschäftigt ist, ist der Konzerndatenschutzbeauftragte externer Datenschutzbeauftragter.

10.6.2 Zeitpunkt, Form und arbeitsrechtliche Aspekte der Benennung

Sofern die Voraussetzungen der Benennungspflicht erfüllt sind (vgl. Kap. 10.2.4, S. 92), muss ein Datenschutzbeauftragter unverzüglich benannt werden. Eine Karenzzeit für die Benennung ist nicht vorgesehen. Die Benennung

51 Vgl. hierzu Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO. Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung. August 2021. S. 14. Online: https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-verantwortlichkeiten-und-aufgaben-nach-der-ds-gvo-inkl-synopse (abgerufen am 11.05.2022).

erfolgt durch einseitige empfangsbedürftige Erklärung der Leitung der benennenden Stelle. Besondere Formanforderungen bestehen nicht, allerdings ist der Verantwortliche bzw. Auftragsverarbeiter nachweispflichtig im Hinblick auf die Benennung.

Nach dem Bundesarbeitsgericht[52] ist mit der Benennung zum internen Datenschutzbeauftragten regelmäßig eine Änderung des Arbeitsvertrags verbunden. Die Benennung kann damit vom Arbeitgeber nicht einseitig im Rahmen des Direktionsrechtes vorgenommen werden.[53]

10.6.3 Dauer der Benennung

Ob eine Befristung der Benennung zulässig ist, ist umstritten. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist der Auffassung, dass eine zeitliche Begrenzung des Amtes den Datenschutz erheblich gefährden würde und die Benennung interner Datenschutzbeauftragter damit grundsätzlich als unbefristet anzusehen ist.[54] Vor demselben Hintergrund sollen nach Auffassung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Verträge mit externen Datenschutzbeauftragten Verträge mit externen DSB regelmäßig eine Mindestvertragslaufzeit von vier Jahren haben. Lediglich bei Erstverträgen soll wegen der Notwendigkeit der Überprüfung der Eignung eine Vertragslaufzeit von ein bis zwei Jahren reichen.

10.6.4 Kontaktdaten des Datenschutzbeauftragten

Die DSGVO erleichtert die Kontaktaufnahme mit dem Datenschutzbeauftragten, indem sie vorschreibt, dass dessen „Kontaktdaten" zu veröffentlichen und der Aufsichtsbehörde mitzuteilen sind (Art. 37 Abs. 7 DSGVO).

52 BAG, Urt. v. 13.03.2007 – 9 AZR 612/05, NJW 2007, 2507, NZA 2007, 563, BB 2007, 1115, DB 2007, 1198.

53 s. hierzu auch: Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): Muster Benennung eines/einer Datenschutzbeauftragten. o. D. Online: https://www.gdd.de/der-datenschutzbeauftragte/copy_of_zertifizierung/benennung-dsb (abgerufen am 11.05.2022); Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): Muster Stellenbeschreibung für eine/n Datenschutzbeauftragte/n. o. D. Online: https://www.gdd.de/der-datenschutzbeauftragte/copy_of_zertifizierung/stellenbeschreibung-dsb (abgerufen am 11.05.2022).

54 LfDI BW (Hg.): Praxisratgeber: Die/der Beauftragte für den Datenschutz. Teil II: Persönliche Voraussetzungen Durchführung der Benennung Stellung und Aufgaben Beendigung der Benennung. November ²2019. S. 14 f. Online: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/11/Praxisratgeber-LfDI-BW-Der-Beauftragte-f%C3%BCr-den-Datenschutz-Teil-II.pdf (abgerufen am 11.05.2022).

Hinweis: Wie ein Vergleich mit Art. 13 Abs. 1 lit. a DSGVO zeigt, wo von „Name und Kontaktdaten" die Rede ist, setzt die Angabe der bloßen Kontaktdaten, z. B. auf der Homepage, nicht zwingend voraus, dass auch der Name des Datenschutzbeauftragten genannt wird. Im Verhältnis zur Aufsichtsbehörde ist die namentliche Nennung gleichwohl sinnvoll (vgl. auch Art. 30 Abs. 1 lit. a i. V. m. Abs. 4 DSGVO).

10.7 Fazit

Als fachkundiges internes Beratungs- und Überwachungsorgan leistet der Datenschutzbeauftragte einen zentralen Beitrag zum Schutz des Rechts auf informationelle Selbstbestimmung sowie zur Reduzierung von Unternehmensrisiken. Wichtig ist, dass allein der Umstand, dass eine Stelle nicht zur Benennung verpflichtet ist, nicht dazu führt, dass diese sich nicht an datenschutzrechtliche Vorgaben zu halten hat. Auch in Stellen mit Benennungspflicht trägt nicht der Datenschutzbeauftragte die Verantwortung für die Einhaltung des Datenschutzes, sondern die Leitung bzw. in abgeleiteter Verantwortung die jeweilige Fachabteilung.[55]

55 s. hierzu auch, insb. zu weiteren gesetzlich nicht geregelten Rollen mit Bezug zum Datenschutz, insbesondere Datenschutzmanagern, -koordinatoren und -referenten: Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO I. Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung. Juli 2019. Online: https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0 (abgerufen am 11.05.2022).

11. Die Datenschutzaufsichtsbehörden – externe Kontrolle

Die Einhaltung der Regelungen der DSGVO durch Wirtschaftsunternehmen, Selbständige, Verbände und Vereine sowie im Internet wird von unabhängigen Aufsichtsbehörden kontrolliert, die von den Bundesländern bestimmt werden. In den meisten Bundesländern wird diese Aufgabe von den Landesdatenschutzbeauftragten wahrgenommen, in Bayern durch das Landesamt für Datenschutzaufsicht, im Saarland durch das Unabhängige Datenschutzzentrum und in Schleswig-Holstein durch das Unabhängige Landeszentrum für Datenschutz. Für die Überwachung der Telekommunikations- und Postdienstunternehmen sowie für alle Finanzbehörden im Anwendungsbereich der Abgabenordnung ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig.[56] Die örtliche Zuständigkeit richtet sich nach dem Sitz der verantwortlichen Stelle; bei Unternehmen, die Niederlassungen in mehreren Bundesländern haben, ist dies der Hauptsitz.

11.1 Aufgaben der Aufsichtsbehörden

Grundsätzlich muss jede Aufsichtsbehörde die Anwendung der DSGVO überwachen und durchsetzen. Zu den Aufgaben der Aufsichtsbehörden gehört dabei gem. Art. 57 DSGVO und § 40 BDSG vor allem

- die Beratung der Verantwortlichen und der betrieblichen Datenschutzbeauftragten,
- die Bearbeitung von Beschwerden Betroffener,
- die Durchführung von Datenschutzkontrollen,
- die Information Betroffener über ihre Rechte und der Öffentlichkeit über Risiken der Datenverarbeitung,
- die Erstellung und Führung einer Liste der Verarbeitungsarten, für die gem. Art. 35 Abs. 2 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen ist,

56 s. hierzu auch: Die Kontaktdaten der Datenschutzbeauftragten der Länder, der Aufsichtsbehörden für den nicht-öffentlichen Bereich, des Rundfunks, der Kirchen, in Europa und im übrigen Ausland finden Sie auf der Internetseite des Bundesbeauftragten für Datenschutz und Informationsfreiheit unter folgendem Link: https://www.bfdi.bund.de/DE/Service/Anschriften/anschriften_node.html;jsessionid=7D639968D96543526BFDC0A4BE76D55B.intranet241(abgerufen am 11.05.2022).

- die Förderung der Ausarbeitung von Verhaltensregeln gem. Art. 40 DSGVO durch Stellungnahmen und ggf. deren Billigung,
- die Genehmigung verbindlicher interner Vorschriften gem. Art. 47 DSGVO.

11.2 Prüfungs- und Informationsbefugnisse der Aufsichtsbehörden

Die Aufsichtsbehörden haben das Recht

- die zur Durchführung ihrer Aufgaben erforderlichen Auskünfte von den verantwortlichen Stellen unverzüglich zu erhalten,
- Datenverarbeitungen von verantwortlichen Stellen zu prüfen,
- im Rahmen von Datenschutzprüfungen Einsicht in geschäftliche Unterlagen zu nehmen,
- im Rahmen von Datenschutzprüfungen die Geschäftsräume der verantwortlichen Stelle zu betreten,
- Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten,
- betroffene Personen über Verstöße gegen die Vorschriften über den Datenschutz zu unterrichten,
- bei schwerwiegenden Verstößen die Gewerbeaufsicht zu unterrichten,
- die Abberufung des Datenschutzbeauftragten zu verlangen, wenn die zur Erfüllung seiner Aufgaben erforderliche Sachkunde fehlt oder ein schwerwiegender Interessenkonflikt vorliegt,
- von der verantwortlichen Stelle die Aushändigung des gem. Art. 30 DSGVO zu führenden Verzeichnisses der Verarbeitungstätigkeiten zu verlangen. Stellen mit weniger als 250 Beschäftigten müssen ein solches Verzeichnis nicht führen, es sei denn es handelt sich um die Verarbeitung besonderer Datenkategorien wie Gesundheitsdaten.

11.3 Durchsetzungsbefugnisse der Datenschutzaufsichtsbehörden

Um die Einhaltung der Regeln der DSGVO durchzusetzen, stehen den Aufsichtsbehörden unterschiedliche Maßnahmen zur Verfügung. Sie können

- die verantwortliche Stelle verwarnen, wenn sie mit Datenverarbeitungsvorgängen gegen die DSGVO verstoßen hat,
- die verantwortliche Stelle anweisen, diese Verarbeitungsvorgänge auf bestimmte Weise und in bestimmter Zeit in Übereinstimmung mit der DSGVO zu bringen,
- die verantwortliche Stelle anweisen, den Anträgen Betroffener auf Ausübung ihrer Rechte zu entsprechen,
- die verantwortliche Stelle anweisen, den von einer Verletzung des Schutzes seiner personenbezogenen Daten Betroffenen darüber zu informieren,
- die Berichtigung oder Löschung und die Einschränkung der Verarbeitung von personenbezogenen Daten anordnen,
- die Unterrichtung der Empfänger dieser Daten über diese Maßnahmen anordnen,
- eine Zertifizierung widerrufen oder die Zertifizierungsstelle anweisen, dies zu tun,
- die Aussetzung der Übermittlung von personenbezogenen Daten in ein Drittland anordnen,
- eine Geldbuße gem. Art. 83 DSGVO verhängen, und zwar zusätzlich zu einer der genannten Maßnahmen oder anstelle davon (s. auch Kap. 13, S. 111 ff.).

12. Datensicherheit

Aussagen zur Datensicherheit finden sich in der DSGVO an verschiedenen Stellen. Die zentralen Regelungen zur Datensicherheit sind in Art. 32 DSGVO zusammengefasst. Orientiert am klassischen Risikobegriff wird hier ein dem Risiko für die Betroffenen angemessenes Schutzniveau gefordert. Zur Gewährleistung dieses Schutzniveaus sind die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen. Bei Verletzungen des festgelegten Schutzniveaus resultieren daraus verschiedene Pflichten des Verarbeiters:

- Meldepflichten gegenüber der zuständigen Aufsichtsbehörde binnen 72 Stunden (s. Art. 33 DSGVO),
- Benachrichtigung der Betroffenen (s. Art. 34 DSGVO). Dies wird in § 29 BDSG weiter präzisiert.

Der Kern der Regelungen entspricht den bisherigen Maßnahmen des alten BDSG. Die geforderten konkreten Maßnahmen gehen jedoch deutlich über die bisherigen Regelungen hinaus. So sind detailliert Meldefristen und Meldeinhalte festgelegt. Weitere Präzisierungen lassen sich primär aus Art. 24 DSGVO (Verantwortung des für die Verarbeitung Verantwortlichen), Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) und aus Art. 35 DSGVO (Datenschutz-Folgenabschätzung) ableiten. Ergänzend sind hier die Nachweis- und Rechenschaftspflichten zu erwähnen, die die Beweislast den Verantwortlichen übertragen und zu einem entsprechenden Kontrollsystem und regelmäßigen Überprüfungen zwingen. Offen ist hier noch die Frage, inwieweit die Rechenschaftspflicht von der Selbstbelastung abzugrenzen ist. Dies wird aktuell in der Literatur diskutiert. Grundlage ist eine entsprechende Risikoabschätzung. Dies erlaubt auch die notwendige Skalierung der DSGVO und eine Anpassung an die reale Risikosituation. Wichtig ist jedoch, die Einschätzung zu begründen und zu dokumentieren. Ein Mittel hierzu ist die DSFA, die in einem ersten Schritt zu einer ersten Abschätzung der grundsätzlichen Risiken führen sollte und damit den weiteren Umfang einer DSFA bestimmt.

12.1 Zum Risikobegriff der DSGVO

Die DSGVO verwendet einen klassischen Risikobegriff, der das Risiko auf Basis der Eintrittswahrscheinlichkeit und der möglichen Folgewirkungen einordnet. Das potenzielle Maximalrisiko wird durch entsprechende Gegenmaßnahme begrenzt, so dass im Ergebnis eine Risikopositionierung des tatsächlich entstehenden Restrisikos vorgenommen wird. Als Maßstab sind die Auswirkungen auf die Grundrechte und Freiheiten von natürlichen Personen anzuwenden. Bemerkenswert ist dabei, dass der Art. 32 DSGVO nicht nur die Auswirkungen auf die Betroffenen der Verarbeitung betrachtet, sondern auf die resultierenden Risiken für alle natürlichen Personen abzielt.[57]

Die Auswirkungen sind insbesondere an den folgenden Schutzzielen zu prüfen:

- **Vertraulichkeit:** Daten dürfen nur von Berechtigten verarbeitet werden (Vermeidung unautorisierter Informationsgewinnung). Dies schließt insbesondere auch die Datenübertragung und den Einblick in die Daten ein und erzwingt letztlich ein dem Risiko entsprechendes Berechtigungssystem.
- **Integrität:** Daten dürfen nicht unbemerkt verändert werden können. Jede Änderung muss nachvollzogen werden können. Auch wenn nicht jeder Zugriff dokumentiert werden muss, muss doch zwingend der Verursacher einer Änderung nachvollzogen werden können.
- **Verfügbarkeit:** Der Zugriff auf die Daten muss innerhalb der definierten Grenzen möglich sein und korrekte Ergebnisse liefern.

In der Regel erfolgt eine Bewertung auf Basis von Schutzklassen der zugrundeliegenden Datenarten. Hierzu finden sich entsprechende methodische Hinweise in den BSI-Standards 200-1 „Managementsysteme für Informationssicherheit“, 200-2 „IT-Grundschutzmethodik“ und 200-3 „Risikomanagement“.[58]

57 s. hierzu auch: Europäischer Datenschutzausschuss (Hg.): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP248rev.01. Oktober 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_de (abgerufen am 11.05.2022).

58 s. hierzu auch: Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standards. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html;jsessionid=80CA0A1A0981C5F43CDD4A5B51CAE522.internet462 (abgerufen am 11.05.2022).

Die DSGVO unterscheidet hier im Wesentlichen die folgenden Arten bzw. Schutzklassen personenbezogener Daten:

- **Personenbezogene Daten:** gemäß Art. 4 Nr. 1 DSGVO.
- **Besonders schutzwürdige Daten:** gemäß Art. 9 DSGVO. Dies beinhaltet insbesondere Gesundheitsdaten, biometrische und genetische Informationen.
- **Personenbezogen Angaben über Straftaten und strafrechtliche Verurteilungen:** gemäß Art. 10 DSGVO.

Gegebenenfalls sind noch Verarbeitungen und besondere Restriktionen für nationale Kennziffern (s. Art. 87 DSGVO) zu beachten.

Die DSGVO definiert einige weitere Schutzziele. Hier führt insbesondere der Begriff der „Belastbarkeit" zu Verständnisproblemen. Unter Belastbarkeit ist nicht die Verarbeitungsmöglichkeit großer Datenmengen zu verstehen, sondern die Resilienz von Systemen, wie es in zutreffender Weise in der englischen Fassung steht. Resilienz bezeichnet dabei die Fähigkeit eines Systems, den ordnungsgemäßen Betriebszustand der gesetzeskonformen Datenverarbeitung nach einer Störung schnellstmöglich wieder zu erreichen. Dies greift insbesondere die Aspekte der Betriebssicherheit (Safety) auf, die den Begriff IT-Sicherheit (Security) ergänzt. Letztlich kann der so zwischen Datenschutz, Safety und Security durch am Risiko orientierte technischen und organisatorischen Maßnahmen aufgespannte Sicherheitsraum abgedeckt werden.

12.2 Technische und organisatorische Maßnahmen

Die dem Risiko adäquaten technischen und organisatorischen Maßnahmen müssen sich am Stand der Technik, den Implementierungskosten und der Art, des Umfangs, der Umstände und dem Zweck der Verarbeitung orientieren. Dabei müssen TOM die beiden konträren Ziele der DSGVO „Wahrung der Grundrechte und Freiheiten der Bürger der EU" und „die Gewährleistung eines freien Verkehrs personenbezogener Daten in der EU" ausbalancieren.[59]

59 s. hierzu auch: Bayerisches Landesamt für Datenschutzaufsicht (Hg.): Good Practice bei technischen und organisatorischen Maßnahmen Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit (Checkliste TOM: technische und organisatorische Maßnahmen). Oktober 2020. Online: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf (abgerufen am 11.05.2022).

12.3 Stand der Technik

Die Begrifflichkeit „Stand der Technik“[60] ist von den häufig verwendeten „anerkannten Regeln der Technik“ abzugrenzen. Während die anerkannten Regeln der Technik eher dem BDSG a. F. zu Grunde lagen, fordert der Stand der Technik mehr, insbesondere in Richtung einer regelmäßigen Prüfung und dem Bestreben, die bestmöglichen Schutzmaßnahmen einzusetzen.

12.4 Restrisiko

Letztlich obliegt es dem Verantwortlichen in einem dokumentierten Prozess und nachweisbaren Ergebnis die Risikoabwägung ernsthaft vorzunehmen und angemessen zu begründen.

Praxistipp: Der gesamte Bewertungsprozess ist zu dokumentieren und für die einzelnen Projektvorhaben zu dokumentieren. In der Praxis könnte dies beispielsweise wie folgt umgesetzt werden:

1. Eine geplante Verarbeitung personenbezogener Daten wird in einem ersten Schritt in eine Risikoklasse eingeordnet, beispielsweise über einen Fragenkatalog, der die einzelnen Aspekte der DSGVO abdeckt und insbesondere die Kriterien für eine Datenschutz-Folgenabschätzung abfragt.

2. Je nach Ergebnis sind weitere Maßnahmen erforderlich und festzulegen. So kann beispielsweise eine einfache Risikoabwägung durchgeführt oder eine Stellungnahme des Datenschutzbeauftragten angefordert werden.

3. Durchführung einer Datenschutz-Folgenabschätzung.

60 s. hierzu auch TeleTrusT – Bundesverband IT-Sicherheit e.V. (Hg.): IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen, revidierte und erweiterte Ausgabe 2018.

13. Bußgelder und Sanktionen bei Datenschutzverstößen

Mit Inkrafttreten der DSGVO besteht für die Datenschutzaufsichtsbehörden die Möglichkeit, deutlich höhere Bußgelder zu verhängen als es bisher der Fall war. Während nach dem bisherigen BDSG Bußgelder von bis zu 300.000 Euro möglich waren, beträgt die maximale Geldbuße im Rahmen von Art. 83 DSGVO 20 Mio. Euro oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Wert der höhere ist.

13.1 Bußgelder bei Verstößen gegen die DSGVO

Geldbußen sind Strafen, die von den Verwaltungsbehörden im Ordnungswidrigkeitenverfahren erlassen werden können (§ 43 BDSG) und werden konkret gem. Art. 83 DSGVO festgelegt. Die Aufsichtsbehörde hat bei festgestellten Verstößen Geldbußen zu verhängen, die in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sind. Dabei sind die Umstände des Einzelfalls nach Art, Schwere, Dauer, Anzahl der betroffenen Personen und Ausmaß des erlittenen Schadens zu berücksichtigen. Nach Art. 83 Abs. 3 DSGVO bemisst sich die Höhe des Betrags am schwerwiegendsten Verstoß und übersteigt den Gesamtbetrag der Geldbuße nicht.

Die Höhe der Geldbußen hat durch die Neuregelung eine enorme Änderung erfahren. Bei Verstößen gegen die Grundsätze der DSGVO (Art. 5, 7, 9 DSGVO), die Regelungen zur Rechtmäßigkeit der Datenverarbeitung (Art. 6 DSGVO), die Rechte des Betroffenen (Art. 12–22 DSGVO) sowie bei Missachtung einer Anweisung einer Datenschutzaufsichtsbehörde (Art. 58 Abs. 2 DSGVO) betragen diese bis zu 20 Mio. Euro oder 4 % des Jahresumsatzes des vorangegangenen Geschäftsjahres (gem. Art. 83 Abs. 5 und 6 DSGVO). Bei Verstößen gegen organisatorische Regelungen betragen diese (gem. Art. 83 Abs. 4 DSGVO) bis zu 10 Mio. Euro bzw. 2 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres. Solche organisatorischen Regelungen wären:

- Verstöße gegen die Pflichten der für die Verarbeitung, Verantwortlichen und der Auftragsverarbeiter, Art. 8, 11, 25–39, 42, 43 DSGVO,

- Verstöße gegen die Pflichten der Zertifizierungsstelle, Art. 42, 43 DSGVO,
- Verstöße gegen die Pflichten der Überwachungsstelle, Art. 41 Abs. 4 DSGVO.

Es gibt in Deutschland aufgrund unterschiedlicher Bewertungen durch Gerichte derzeit die Diskussion, inwieweit die Vorgaben des § 130 OWiG bei einem Bußgeld nach der DSGVO gegen ein Unternehmen zu berücksichtigen sind. Hierzu wurde im Rahmen eines Vorlagebeschlusses im Dezember 2021 der EuGH angerufen.[61]

13.2 Sanktionen bei Verstößen gegen die DSGVO

Sanktionen sind Strafen i.S.d. Strafrechts (§ 42 BDSG). Die EU hat keine generelle Kompetenz für das Strafrecht. Sie kann lediglich im Rahmen der DSGVO vorgeben, dass für den genannten Fall des Art. 84 DSGVO in den Mitgliedstaaten Straftatbestände normiert werden sollen. Die Mitgliedstaaten werden daher verpflichtet, Vorschriften über andere Sanktionen für Verstöße gegen die DSGVO, die keiner Geldbuße gem. Art. 83 DSGVO unterliegen, festzulegen. Diese müssen gem. Art. 84 DSGVO ebenso wirksam, verhältnismäßig und abschreckend sein. Diese Vorgabe hat die Bundesrepublik Deutschland im Rahmen des neuen Bundesdatenschutzgesetzes umgesetzt. Nachfolgend finden Sie einen Überblick der neuen BDSG Normen.

13.3 Sanktionen des BDSG

Das BDSG ist am 25. Mai 2018 gemeinsam mit der DSGVO in Kraft getreten. Das Gesetz wurde als Teil des Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) beschlossen und löste das bisher geltende Bundesdatenschutzgesetz vollständig ab.

Kapitel 5 des BDSG „Sanktionen" enthält ergänzende und flankierende Regelungen hinsichtlich datenschutzrechtlicher Verstöße.

61 KG Berlin: 3 Ws 250/21 vom 06.12.2021. Online: https://rewis.io/urteile/urteil/en2-06-12-2021-3-ws-25021/ (abgerufen am 11.05.2022).

Nach § 42 BDSG Abs. 1 BDSG wird jemand, der gewerbsmäßig, wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, einem Dritten übermittelt oder auf andere Art und Weise zugänglich macht, ohne hierzu berechtigt zu sein, mit bis zu 3 Jahren Freiheitsstrafe oder Geldstrafe bestraft.

Nach § 42 Abs. 2 BDSG wird jemand mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft, wenn er personenbezogene Daten, die nicht allgemein zugänglich sind, ohne hierzu berechtigt zu sein, verarbeitet oder durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Diese Taten werden gem. § 42 Abs. 3 BDSG jedoch nur auf Antrag verfolgt.

§ 43 BDSG setzt ergänzende Bußgeldvorschriften bei Verstößen gegen § 30 BDSG fest und richtet sich gegen Stellen, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung verarbeiten. Die Vorschrift entspricht den Bußgeldtatbeständen des § 43 Abs. 1 Nr. 7a und b BDSG a. F., die der Umsetzung des Art. 9 der Verbraucherkreditrichtlinie 2008/48/EG dienen. Der bisherige Bußgeldrahmen von bis zu 50.000 Euro wird in § 43 Abs. 2 BDSG beibehalten.

Die DSGVO selbst regelt das Straf- und Bußgeldverfahren nicht. Sie sieht in Art. 83 Abs. 8 DSGVO vor, dass die Mitgliedstaaten angemessene Verfahrensgarantien festlegen. § 41 BDSG legt den verfahrensrechtlichen Rahmen von Bußgeld- und Strafverfahren fest. Nach § 41 Abs. 1 BDSG ist bei Verstößen gegen Art. 83 Abs. 4 bis 6 DSGVO grundsätzlich das Gesetz über Ordnungswidrigkeiten (OWiG) anwendbar (soweit gesetzlich nichts anderes bestimmt wird). Für Verfahren wegen eines Verstoßes nach Art. 83 Abs. 4 bis 6 der Verordnung gelten (soweit gesetzlich nichts anderes bestimmt) nach § 41 Abs. 2 BDSG die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren entsprechend.

In Deutschland sind für die Verhängung von Sanktionen in der Regel die Gerichte zuständig, für die Verfolgung Polizei und Staatsanwaltschaft. Insoweit ergibt sich hier aus der DSGVO keine Neuregelung.

14. Öffentliche Stellen

Bis zur Reform des europäischen Datenschutzrechts hat das deutsche Recht bereits stark zwischen öffentlichen und nichtöffentlichen datenverarbeitenden oder verantwortlichen Stellen unterschieden. Das bis zur DSGVO geltende BDSG befasste sich gleichwohl in nur einer Norm mit den öffentlichen Stellen des Bundes und der Gesamtheit der nichtöffentlichen Stellen. Für den weitaus größeren Bereich der öffentlichen Stellen der Länder und damit auch der Kommunen und ihrer Rechtsbereiche wurden die Regelungen in den betreffenden Landesdatenschutzgesetzen getroffen. Zudem umfasst auch das spezifische Bereichsrecht des Bundes und der Länder an einigen Stellen Vorgaben und Normen zum Datenschutz für den öffentlichen Bereich (wie z. B. das Sozialgesetzbuch). An dieser auch dem Föderalismus geschuldeten Struktur hat sich im Wesentlichen nichts geändert, eine der weiteren Rechtsvereinfachung dienende Föderalismusreform konnte im Rahmen des neuen europäischen Rechts rechtspolitisch nicht zur Diskussion stehen.

Mit Stand des Wirksamwerdens der Grundverordnung ist auch das neue BDSG in Kraft getreten.

Die Regelungen der DSGVO gelten für öffentliche und nichtöffentliche Stellen gleichermaßen. Ausdrücklich beziehen Art. 4 Nr. 7, 8 DSGVO bei der Definition des Verantwortlichen und Auftragsverarbeiters neben den natürlichen und juristischen Personen auch die Behörden mit ein. Dies schafft ein neues, nunmehr zukünftig gleich hohes Schutzniveau gegenüber den Betroffenen unabhängig davon, welcher Rechtsnatur der Verantwortliche oder Auftragsverarbeiter nun ist, letztere gibt es auch im öffentlichen Bereich.

Unverändert bleibt das nationale Datenschutzrecht subsidiär in seiner Anwendung gegenüber spezialgesetzlichen Vorschriften, aber gleichwohl vorrangig zum Verwaltungsverfahrensrecht. Dies spielt für einige Verwaltungsbereiche eine entscheidende Rolle (Soziales und Gesundheit) sowie für die gesamte digitale Transformation im noch anhaltenden Dissens zwischen technisch Machbarem und Sinnvollem sowie dem derzeit rechtlich Erlaubten. Natürlich müssen aber alle datenschutzrechtlichen Vorschriften der neuen DSGVO folgen.

Nur wenige Normen der Grundverordnung enthalten Spezialvorschriften für die öffentlichen Stellen wie z. B. Art. 2 Abs. 2 lit. d) , der die Verarbei-

tung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung usw. aus dem Anwendungskreis der DSGVO völlig ausnimmt und in einer parallel zur Grundverordnung verabschiedeten neuen Richtlinie (Richtlinie (EU) 2016/680) regelt. Deren nationalrechtlich erforderliche Umsetzung erfolgt im Teil 3 des BDSG (neu). Dies ist der augenscheinlich größte Verwaltungsbereich mit eigenem Regelungswerk.

Neben einer ausdrücklichen Regelung innerhalb der europäischen Normen gibt es auch mit Blick auf die Öffnungsklauseln, Möglichkeiten zu besonderen nationalgesetzlichen Regelungen für den öffentlichen Bereich, wie z. B. im Art. 83 Abs. 7 DSGVO, in dem es um die Verhängung von Bußgeldern gegenüber öffentlichen Stellen geht.

Vorab sei noch erwähnt, dass das BDSG (neu) nach § 2 Abs. 5 die öffentlichen Stellen des Bundes und der Länder den nichtöffentlichen gleichstellt, wenn sie in Form öffentlich-rechtlicher Unternehmen am Wettbewerb teilnehmen und zusätzlich für die Länder, wenn die Unternehmen Bundesrecht ausführen und der Datenschutz dort nicht durch Landesrecht gewährleistet ist.

Auffällige Unterschiede zwischen öffentlichem und nichtöffentlichem Bereich bestehen u. a. nun in folgenden Punkten:

- Nach Art. 37 Abs. 1 lit. a muss die verantwortliche (öffentliche) Stelle bereits einen Datenschutzbeauftragten bestellen. In einer Wiederholung dieser Norm sehen § 5 Abs. 1 BDSG und die neuen Landesdatenschutzgesetze dasselbe vor. Hierdurch ergibt sich nun erstmals eine Verpflichtung für den gesamten öffentlichen Bereich aller Verwaltungsebenen, einen Datenschutzbeauftragten zu bestellen. Für die nichtöffentlichen Bereiche greifen die Vorgaben der DSGVO in Verbindung mit § 38 Abs. 1 BDSG zur Bestellung eines Datenschutzbeauftragten, die damit eine weitere Öffnungsklausel der DSGVO in Anspruch nehmen. Hier gab es bereits im November 2019 zur Entlastung der KMU eine Rechtsänderung durch Anhebung von 10 auf 20 Personen, die regelmäßig mit personenbezogenen Daten arbeiten und damit die Bestellung eines Datenschutzbeauftragten bedingen.

- Personenbezogene Daten besonderer Kategorien erhalten unverändert auch im neuen BDSG entsprechenden Schutz, die

Verarbeitungsbefugnisse sind in § 22 Abs. 1 Ziff. 1 BDSG geregelt und wurden gleichfalls durch Rechtsänderung im November 2019 erweitert. Unter bestimmten, abschließend aufgezählten Bedingungen ist deren Verarbeitung für öffentliche und nichtöffentliche Stellen zulässig. Für den öffentlichen Bereich sind darüber hinaus unter Ziff. 2 der Norm weitere Zulässigkeitsbedingungen genannt, die den nichtöffentlichen Verarbeitern verwehrt bleiben (Abwehr erheblicher Gefahren, Gemeinwohl, Verteidigung und Krisenbewältigung).

- Die in den §§ 23 und 24 BDSG geregelte Verarbeitung zu „anderen Zwecken" ist für den öffentlichen Bereich gleichfalls deutlich weiter gefasst. Der nichtöffentliche Bereich kann vom ursprünglichen Verarbeitungszweck nur im Rahmen der Gefahrenabwehr für die staatliche oder öffentliche Sicherheit abweichen oder zur Verfolgung und Klärung zivilrechtlicher Ansprüche. Gleichwohl gilt die Kompatibilitätsprüfung aus Art. 6 Abs. 4 DSGVO, da die Grundverordnung eben weitreichendere Regelungen ohne einengende Bestimmung unter entsprechenden Vorgaben zugunsten eines legitimen Interesses ausweislich der Regelungsöffnung der DSGVO zulässt. Der Erlaubnisvorbehalt für den öffentlichen Bereich ist deutlich umfangreicher und umfasst wiederum einige Konstellationen mehr als eine anzunehmende Zustimmung der betroffenen Person, Überprüfung von Angaben, Maßnahmen der Gefahrenabwehr, Verfolgung von Straftaten und Ordnungswidrigkeiten, Abwehr von Beeinträchtigungen der Rechte Dritter u. a. m.

- Besonderes Augenmerk finden die Bußgeldregelungen nach Art. 83 ff. DSGVO zum einen, weil das europäische Normenwerk bekanntlich drastische Höhen vorsieht, zum anderen sind die nationalen Gesetzgeber aufgefordert, die bestehende Öffnungsklausel auszukleiden sowie weitere Sanktionen festzulegen. Dies hat der Bundesgesetzgeber in den Bestimmungen der §§ 41–43 BDSG (neu) umgesetzt. Vor allem § 43 Abs. 3 BDSG fällt sofort auf, nach dem gegen Behörden und sonstige öffentliche Stellen im Sinne des BDSG keine Bußgelder verhängt werden. Das scheint auf den ersten Blick ein enormes Privileg des öffentlichen Bereichs zu sein, soll aber Zahlungen innerhalb öffentlicher Haushalte ersparen.

Zu beachten ist hier, dass die öffentlichen Stellen u. U. datenschutzrechtlich als nichtöffentliche Stellen zu sehen sind (Tätigkeit als öffentlich-rechtliche Unternehmen im Wettbewerb). In diesen Fällen greift die Befreiung des § 43 Abs. 3 BDSG (neu) dann eben nicht und sie unterliegen denselben Vorschriften wie private Leistungsanbieter auch. Dies gilt es für öffentliche Stellen unbedingt zu beachten und daraus folgt, dass bei einer Prüfung und Feststellung der Verarbeitungsbefugnis durch die öffentliche Stelle unbedingt auch schon allein aus Sicht der Straf- und Bußgeldvorschriften eine Prüfung und Festlegung des Tätigkeitscharakters stattfinden muss. Außerdem kann eine Betätigung öffentlicher Verwaltung, die in diesem Zusammenhang zur Bewertung als nichtöffentliche Stelle führt, Verarbeitungsermächtigungen wieder einschränken, die als öffentliche Stelle bestehen würden.

Unabhängig von öffentlicher und nichtöffentlicher Stelle geht es bei der Beurteilung einer Täterschaft zu. Die Bußgelder der DSGVO richten sich stets gegen die verantwortliche Stelle. Schuldhaftes Verhalten des Verantwortlichen oder seines Beauftragten selbst werden ggf. separat verfolgt, selbstverständlich auch gegen Beschäftigte des öffentlichen Dienstes.

Zusammenfassend ist festzustellen, dass die Rahmenbedingungen im Wesentlichen gleich gelagert sind, beide Bereiche haben die Verarbeitung personenbezogener Daten zu schützen, dies zu überprüfen und zu dokumentieren. An der einen oder anderen Stelle sind die Verarbeitungsermächtigungen zu Gunsten des öffentlichen Bereichs weiter gefasst, können aber nur unter Berücksichtigung der neuen Regularien genutzt werden. Für die Betroffenen der Verarbeitung personenbezogener Daten entwickelt sich nunmehr ein Zustand eines gleich hoch gelagerten Schutzniveaus und gleicher Rechte gegenüber den Verarbeitern unabhängig davon, in welcher Anwendungshemisphäre er sich nun befindet.

Sammlung weiterführender Links

Die vorliegende Publikation „Die DSGVO. Hinweise für kleine und mittlere Unternehmen“ steht als Online-Publikation zum kostenfreien Download zur Verfügung. In der PDF-Datei sind alle nachfolgend zusammengestellten Links einfach aufrufbar.

Zur Online-Version gelangen Sie hier:
www.awv-net.de/DSGVO-KMU

Bayerisches Landesamt für Datenschutzaufsicht (Hg.): Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018. o. D. Online: https://www.lda.bayern.de/media/dsgvo_fragebogen.pdf (abgerufen am 11.05.2022).

Bayerisches Landesamt für Datenschutzaufsicht (Hg.): Good Practice bei technischen und organisatorischen Maßnahmen Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit (Checkliste TOM: technische und organisatorische Maßnahmen). Oktober 2020. Online: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf (abgerufen am 11.05.2022).

Bayerisches Landesamt für Datenschutzaufsicht (Hg.): Muster 9. Online-Shop – Verzeichnis von Verarbeitungstätigkeiten. o. D. Online: https://www.lda.bayern.de/media/muster_9_online-shop_verzeichnis.pdf (abgerufen am 11.05.2022).

Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (Hg.): Das berufliche Leitbild der Datenschutzbeauftragten/Code of Practice for Data Protection Officers. April 2018. Online: https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf (abgerufen am 11.05.2022).

Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hg.): Mustervertragsanlage. Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO). Mai 2017 (in Überarbeitung). Online: https://www.bitkom.org/sites/main/files/2022-03/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf (abgerufen am 11.05.2022).

Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standards. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html;jsessionid=80CA0A1A0981C5F43CDD4A5B51CAE522.internet462 (abgerufen am 11.05.2022).

Bundesbeauftragter für Datenschutz und Informationsfreiheit: Kontaktinformationen Europäischer Datenschutzbehörden. Online: https://www.bfdi.bund.de/DE/Service/Anschriften/Europa/Europa-node.html (abgerufen am 11.05.2022).

Bundesbeauftragter für Datenschutz und Informationsfreiheit: Kontaktinformationen Kirchen und Religionsgemeinschaften. Online: https://www.bfdi.bund.de/DE/Service/Anschriften/Kirchen/Kirchen-node.html (abgerufen am 11.05.2022).

Bundesbeauftragter für Datenschutz und Informationsfreiheit: Kontaktinformationen Landesbehörden. Online: https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html (abgerufen am 11.05.2022).

Bundesbeauftragter für Datenschutz und Informationsfreiheit: Kontaktinformationen Rundfunkdatenschutzbeauftragte. Online: https://www.bfdi.bund.de/DE/Service/Anschriften/Rundfunk/Rundfunk-node.html (abgerufen am 11.05.2022).

Datenschutzkonferenz (Hg.): Kurzpapier Nr. 6. Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf (abgerufen am 11.05.2022) (abgerufen am 11.05.2022).

Datenschutzkonferenz (Hg.): Kurzpapier Nr. 13. Auftragsverarbeitung, Art. 28 DSGVO. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf (abgerufen am 11.05.2022).

Datenschutzkonferenz (Hg.): Kurzpapier Nr. 15. Videoüberwachung nach der Datenschutz-Grundverordnung. Dezember 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf (abgerufen am 11.05.2022).

Datenschutzkonferenz (Hg.): Kurzpapier Nr. 16. Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO. März 2018. Online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf (abgerufen am 11.05.2022).

Datenschutzkonferenz (Hg.): Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist. Version 1.1. Oktober 2018. Online: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf (abgerufen am 11.05.2022).

Datenschutzkonferenz (Hg.): Schematische Darstellung „Akkreditierungsprozess für den Bereich ‚Datenschutz' gemäß Art. 42, 43 DS-GVO". Version 1.0 (15.03.2019). Online: https://www.datenschutzkonferenz-online.de/media/oh/20190315_oh_akk_c.pdf (abgerufen am 11.05.2022).

Die Wirtschaftsauskunfteien e.V. (Hg.): Code of Conduct. Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien. Januar 2020. Online: https://www.die-wirtschaftsauskunfteien.de/code-of-conduct (abgerufen am 11.05.2022).

Europäische Kommission (Hg.): Angemessenheitsentscheidungen der EU-Kommission gemäß Art. 45 DSGVO. o. D. Online: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (abgerufen am 11.05.2022).

Europäische Kommission (Hg.): Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates. Juni 2021. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=EN (abgerufen am 11.05.2022).

Europäische Kommission (Hg.): Durchführungsbeschluss (EU) 2021/915 Der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates. Juni 2021. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=EN (abgerufen am 11.05.2022).

Europäische Kommission (Hg.): Factsheet „Trans-Atlantic Data Privacy Framework“ vom 25.03.2022. Online: https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (abgerufen am 11.05.2022).

Europäische Kommission (Hg.): Pressemitteilung „European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework“ vom 25.03.2022. Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087 (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Empfehlung 01/2019 zu der vom Europäischen Datenschutzbeauftragten entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725). Juli 2019. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendation_201901_edps_39.4_dpia_list_de.pdf (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250rev.01. Februar 2018. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_de (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679. Mai 2020. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen. Oktober 2019. Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP260rev.01. April 2018. Online: https://ec.europa.eu/newsroom/article29/items/622227 (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), WP243rev.01. April 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_de (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Leitlinien zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO. Juli 2021. Online: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf (abgerufen am 11.05.2022).

Europäischer Datenschutzausschuss (Hg.): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP248rev.01. Oktober 2017. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_de (abgerufen am 11.05.2022).

European Data Protection Board (Hg.): Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. Dezember 2021. Online: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf (abgerufen am 11.05.2022).

European Data Protection Board (Hg.): Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Juli 2021. Online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO. Die Datenschutz-Richtlinie Grundlagen, Grundstrukturen und typische Regelungsbereiche. November 2021. Online: https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/PraxishilfeDSGVODieDatenschutzRichtlinie.pdf (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO. Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO. Juni 2021. Online: https://www.gdd.de/downloads/praxishil-

fen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-muster-vertrag-zur-auftragsverarbeitung-gemaess-art-28-ds-gvo (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO: Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung. August 2021. Online: https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-verantwortlichkeiten-und-aufgaben-nach-der-ds-gvo-inkl-synopse (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO I. Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung. Juli 2019. Online: https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0 (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO Vb. Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter. Januar 2020. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_5bVVTAuftragsverarbeiter.pdf (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe DS-GVO XI. Verpflichtung auf die Vertraulichkeit. Dezember 2017. Online: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe XV. Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO (Joint Controllership). Dezember 2019. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_15_JointControllership_1.0.pdf (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDD-Praxishilfe Verzeichnis von Verarbeitungstätigkeiten – Verantwortlicher, Version 2.1. April 2022. Online: https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfeDSGVOVerzeichnisvonVerarbeitungsttigkeiten.pdf (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): GDPR Good Practices – XI. Confidentiality agreement. Mai 2020. Online: https://www.gdd.de/downloads/praxishilfen/gdpr-good-practices-xi.pdf (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): Muster Benennung eines/einer Datenschutzbeauftragten. o. D. Online: https://www.gdd.de/der-datenschutzbeauftragte/copy_of_zertifizierung/benennung-dsb (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): Muster Stellenbeschreibung für eine/n Datenschutzbeauftragte/n. o. D. Online: https://www.gdd.de/der-datenschutzbeauftragte/copy_of_zertifizierung/stellenbeschreibung-dsb (abgerufen am 11.05.2022).

Gesellschaft für Datenschutz und Datensicherheit e.V. (Hg.): Template Processing in accordance with Article 28 General Data Protection Regulation (GDPR). Juni 2021. Online: https://www.gdd.de/downloads/praxishilfen/ph-iv-mustervertrag_zur_auftragsverarbeitung_ds-gvo_english (abgerufen am 11.05.2022).

Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (Hg.): Praxisratgeber: Die/der Beauftragte für den Datenschutz. Teil II: Persönliche Voraussetzungen Durchführung der Benennung Stellung und Aufgaben Beendigung der Benennung. November 2019, S. 14 f. Online: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/11/Praxisratgeber-LfDI-BW-Der-Beauftragte-f%C3%BCr-den-Datenschutz-Teil-II.pdf (abgerufen am 11.05.2022).

Landesbeauftragte für Datenschutz- und Informationsfreiheit Nordrhein-Westfalen (Hg.): Information über die Erhebung von personenbezogenen Daten nach Art. 13, 14 und 21 Datenschutz-Grundverordnung Umsetzungshilfe zu den Datenschutzhinweisen. Januar 2022. Online: https://www.ldi.nrw.de/system/files/media/document/file/ldi_nrw_-_umsetzungshilfe_datenschutzinformation_2022-01.pdf (abgerufen am 11.05.2022).

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Hg.): Verhaltensregeln/Code of Conduct für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirt-

schaftsauskunfteien. August 2020. Online: https://www.ldi.nrw.de/system/files/media/document/file/dw_coc_genehmigung_2020_des_aenderungsantrags_2019_1.pdf (abgerufen am 11.05.2022).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Hg.): Praxisreihe Datenschutzbestimmungen praktisch umsetzen. Videoüberwachung. Juni 2019. Online: https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-5-Videoueberwachung.pdf (abgerufen am 11.05.2022).

www.awv-net.de

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages