Das neue Datenschutzrecht und die Organhaftung bei Datenschutzverletzungen

3

Jürgen Monhemius

3.1 Einführung

Am 25. Mai 2018 wird ein neues Kapitel im europäischen und deutschen Datenschutzrecht aufgeschlagen: Ab diesem Zeitpunkt wird die Datenschutz-Grundverordnung (DS-GVO) – VO (EU) 2016/679[1] – (General Data Protection Regulation) gelten, die europaweit die Datenverarbeitung sämtlicher Unternehmen, Behörden und sonstigen Organisationen (*Verantwortliche,* „controller")[2] *unmittelbar* regeln wird, ohne dass es eines nationalen Umsetzungsgesetzes bedarf. Allerdings enthält die DS-GVO eine Reihe von sogenannten *Öffnungsklauseln*, die präzisierende oder ergänzende Regelungen in einem nationalen Gesetz erlauben. Demgemäß wurde vom Bundestag das neue BDSG[3] (im folgenden BDSG 2018 genannt) verabschiedet, welches das noch aktuelle BDSG ablösen wird und von den Verantwortlichen dann ebenfalls zu beachten ist.[4]

Darüber hinaus gelten nach wie vor zahlreiche *bereichsspezifische* Datenschutzregelungen, insbesondere im arbeits- und sozialrechtlichen Bereich, so z. B. die Melde- und

[1] ABl. 2016 L 119/1.

[2] Das Thema der Auftragsverarbeitung wird aus Platzgründen nicht behandelt.

[3] Art. 1 Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 05.07.2017, BGBl. I S. 2097.

[4] Der Umfang der datenschutzrechtlichen Regeln hat beträchtlich zugenommen: Musste ein Unternehmen bislang nur die §§ 1–11 und 27−38a BDSG in den Blick nehmen, sind es jetzt allein in der DS-GVO 99 Artikel nebst 173 teils umfangreichen „Erwägungsgründen" (im Folgenden abgekürzt ErwGr) sowie die §§ 1–44 im BDSG 2018.

J. Monhemius (✉)
H-BRS, Sankt Augustin, Deutschland
E-Mail: juergen.monhemius@h-brs.de

A. Gadatsch et al. (Hrsg.), *Nachhaltiges Wirtschaften im digitalen Zeitalter,*
https://doi.org/10.1007/978-3-658-20174-6_3

Aufzeichnungspflichten des Arbeitgebers im Rahmen der Sozialversicherung, §§ 28 ff. SGB IV.

Somit müssen die mit Datenverarbeitung befassten Organisationen künftig mindestens zwei oder sogar drei verschiedene Regelungswerke gleichzeitig im Blick haben, um datenschutzrechtskonform zu handeln.

Zusätzlich wird die Rechtsanwendung dadurch erschwert, dass die DS-GVO – anders als das BDSG – nicht zwischen Unternehmen (nicht-öffentliche Stellen) und Behörden (öffentliche Stellen) unterscheidet. Das Unternehmen kann sich also nicht auf bestimmte Regelungen der DS-GVO konzentrieren, sondern muss bei allen datenschutzrelevanten Vorgängen europäisches und nationales Recht in Gänze berücksichtigen.

Schließlich hat sich auch die Rechtslage im Hinblick auf *drohende Bußgelder* bei Datenschutzrechtsverstößen tief greifend verändert:

War bislang gem. § 43 BDSG der Bußgeld-Höchstrahmen mit 50.000 EUR bei Verstößen gegen formelle bzw. administrative Datenschutzpflichten bzw. 300.000 EUR bei Verstößen gegen materielles Datenschutzrecht noch recht „übersichtlich", so müssen sich die Unternehmen jetzt auf Bußgeldbeträge nach dem Vorbild des Kartellrechts einstellen, wobei Art. 84(1) DS-GVO die generelle Zielsetzung unmissverständlich vorgibt: Sanktionen für Verstöße gegen das Datenschutzrecht müssen „wirksam, verhältnismäßig und abschreckend (effective, proportionate and dissuasive) sein".

Dementsprechend sieht die DS-GVO bei fast allen Datenschutzpflichten der Unternehmen für den Fall eines Verstoßes eine Geldbuße vor, Art. 83 DS-GVO. Handelt es sich um eine Verletzung formeller Pflichten, beträgt der Höchstrahmen nunmehr 10 Mio. EUR oder – falls höher – 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres. Wird gegen materielles Datenschutzrecht (Datenschutzgrundsätze, Rechte betroffener Personen; Erlaubnistatbestände etc.) verstoßen, liegt die Höchstgrenze gar bei 20 Mio. EUR bzw. 4 % des Weltjahresumsatzes.

Adressat der Bußgeldtatbestände ist das Unternehmen im Sinne des Kartellrechts (Art. 101,102 AEUV), d. h. insbesondere der Konzern als *wirtschaftliche Einheit,* sodass sich die Bemessungsgrundlage aus dem Jahresumsatz des gesamten Konzerns ergibt.

Beispiel

Laut Geschäftsbericht betrug der Weltjahresumsatz des Daimler-Konzerns 2016 153,26 Mrd. EUR. Folglich liegt der Bußgeld-Höchstrahmen für diese Unternehmensgruppe bei 6,13 Mrd. EUR!

Im Folgenden wird zunächst ein Überblick über wesentliche materielle und organisatorische *Neuerungen* des Datenschutzrechts gegeben, die für die Unternehmen von Relevanz sind. Im Anschluss daran werden die *haftungsrechtlichen Konsequenzen* für die Unternehmensleitung im Fall von Datenschutzverletzungen diskutiert.

3.2 Das neue Datenschutzrecht

3.2.1 Begriff der Datenverarbeitung; datenschutzrechtliche Pflichtenbündel

Das aktuelle BDSG unterscheidet noch zwischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten, § 3(3)−(5) BDSG. In der DS-GVO dagegen bildet die *Verarbeitung* („processing“) den Dachbegriff, worunter jeglicher Vorgang im Zusammenhang mit personenbezogenen Daten verstanden wird, Art. 4 Nr. 2 DS-GVO. Die DS-GVO gilt für die automatisierte Verarbeitung personenbezogener Daten, ebenso für die nichtautomatisierte (d. h. ohne Zuhilfenahme einer IT-Struktur) Verarbeitung von Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, Art. 2(1) DS-GVO und ErwGr. 15.

Beispiel

Der Arzt und Senior Dr. Sauerbruch hält jegliche IT für Enkelkram und vertraut weiterhin auf seine in einer Hängeregistratur wohlverwahrten Patientenakten. Auch er unterliegt der DS-GVO, da die Patientenakten regelmäßig nach Namen sortiert sind.

Die sich aus dem Datenschutzrecht (DS-GVO und BDSG 2018) ergebenden *Pflichten des Unternehmens* lassen sich vier Komplexen zuordnen:

- Einhaltung der Grundsätze der Datenverarbeitung, Art. 5 DS-GVO,
- Einhaltung der Rechtmäßigkeitsvoraussetzungen bei den einzelnen Datenverarbeitungsvorgängen, Art. 6 ff. DS-GVO; §§ 4, 22, 24, 26, 31 BDSG 2018,
- Gewährleistung der Rechte der Betroffenen (Kunden, Lieferanten, Beschäftigte), Art. 12 ff. DS-GVO; §§ 29, 32–35 BDSG 2018,
- Durchführung präventiver Datenschutzmaßnahmen und Erfüllung von Dokumentationspflichten, Art. 24, 25, 30, 32 DS-GVO.

Auf diese Pflichtenbündel wird im Folgenden näher eingegangen.

3.2.2 Grundsätze der Datenverarbeitung

Art. 5(1) DS-GVO fixiert die *Grundsätze* der Verarbeitung personenbezogener Daten:

a) Rechtmäßigkeit, Treu und Glauben, Transparenz („lawfulness“, „fairness“, „transparency“)
b) Zweckbindung („purpose limitation“)
c) Datenminimierung („data minimisation“) bzw. Datensparsamkeit
d) Richtigkeit („accuracy“)
e) Speicher(zeit)begrenzung („storage limitation“)
f) Integrität (Datensicherheit) und Vertraulichkeit („integrity“, „confidentiality“)

Obwohl ErwGr. 39 nähere Ausführungen zu den Grundsätzen enthält, bleiben die Grundsätze in ihren Konturen unscharf, produzieren folglich Rechtsunsicherheit beim Rechtsanwender. Deshalb ist die neu eingeführte *Rechenschaftspflicht* („accountability") des Unternehmens gem. Art. 5(2) DS-GVO von besonderer Brisanz: Die Unternehmen sind nicht nur für die Einhaltung der Grundsätze verantwortlich, sondern müssen auch *nachweisen,* dass sie bei allen Datenverarbeitungsaktivitäten die Grundsätze eingehalten haben. Kann das Unternehmen im Konflikt mit Datenschutzbehörden, betroffenen Kunden, Beschäftigten etc. nicht nachweisen, dass es verordnungskonform gehandelt hat, muss es mit einer Geldbuße gemäß Art. 83(5) a) DS-GVO rechnen (Albrecht und Jotzo 2017, S. 56; Plath 2016, Art. 5 DS-GVO Rn. 23; Hamann 2017, S. 1091).

3.2.3 Erlaubnistatbestände

Das BDSG regelt in den §§ 28−30a sehr konkret, unter welchen Voraussetzungen das Unternehmen personenbezogene Daten verarbeiten darf. Demgegenüber formuliert die DS-GVO – vom Tatbestand der Einwilligung einmal abgesehen – mehrere (teilweise sehr allgemein gefasste) Erlaubnistatbestände, Art. 6(1) a)−f) DS-GVO (*Rechtmäßigkeit der Verarbeitung* – „lawfulness of processing"). Danach ist die Verarbeitung nur rechtmäßig, wenn eine der folgenden Bedingungen erfüllt ist:

a) Die betroffene Person (data subject) hat ihre *Einwilligung* („consent") in die Datenverarbeitung für bestimmte Zwecke gegeben. Näheres zur Einwilligung findet sich in Art. 7, 8 DS-GVO.
   Die Datenverarbeitung ist erforderlich ...
b) für die Erfüllung eines *Vertrages* („performance of a contract") mit der betroffenen Person oder Durchführung vorvertraglicher Maßnahmen,
c) für die Erfüllung einer *rechtlichen Verpflichtung* („compliance with a legal obligation") des Verantwortlichen,
d) zum Schutz *lebenswichtiger Interessen* („vital interests") einer betroffenen Person,
e) für die Wahrnehmung einer im *öffentlichen Interesse* („public interest") oder in Ausübung *öffentlicher Gewalt* („official authority") liegenden Aufgabe,
f) zur Wahrung *berechtigter Interessen* („purpose of the legitimate interests") des Verantwortlichen in Abwägung zu den *Grundrechten und Grundfreiheiten* („fundamental rights and freedoms") der betroffenen Person.

Für die Datenverarbeitung in Unternehmen sind vor allem die Tatbestände zu a), b) und f), aber auch c) praxisrelevant, wie folgende Beispiele zeigen:

Beispiel

- zu a): Einwilligung neuer Kunden in die Datenverarbeitung im Rahmen des Vertragsabschlusses
- zu b): Datenverarbeitung zu Abrechnungszwecken (Honorare, Gehälter, sonstige Entgelte), für Zwecke der Lieferung (Adressen, Kommunikationsverbindungen)
- zu c): Meldepflichten des Arbeitgebers gegenüber den Sozialversicherungsträgern
- zu f): Marktforschung, Werbung, Scoring

Die verschiedenen *unbestimmten Rechtsbegriffe* (bestimmte Zwecke, Erforderlichkeit, berechtigte Interessen etc.) in Art. 5 und 6 DS-GVO machen den rechtskonformen Umgang mit den Regelungen im unternehmerischen Alltag nicht einfach. Vor allem die gem. Art. 6(1) f) DS-GVO erforderliche Güterabwägung zwischen der „Wahrung der berechtigten Interessen des Verantwortlichen" (= Unternehmen) und den „Interessen oder Grundrechte(n) und Grundfreiheiten der betroffenen Person" (= Kunde, Lieferant, Beschäftigter) muss – um sie für den betrieblichen Alltag handhabbar zu machen – für die typischen datenrelevanten Unternehmensaktivitäten konkretisiert werden (etwa durch die Formulierung eindeutiger Fallbeispiele, die unternehmensintern verbindlich gelten), ErwGr. 47.

An dieser Stelle dürfte für die Unternehmen hilfreich sein, dass die DS-GVO eine Selbstregulierung zulässt: Zukünftig können (Branchen-)Verbände, die datenverarbeitende Unternehmen vertreten, für ihre Mitgliedsunternehmen konkretisierende *Verhaltensregeln* („codes of conduct") zum Datenschutz ausarbeiten, der Aufsichtsbehörde zur Genehmigung und anschließenden Veröffentlichung vorlegen, Art. 40 DS-GVO.

Wie bereits erwähnt, enthält die die DS-GVO zahlreiche Öffnungsklauseln, die von den EU-Mitgliedstaaten mit nationalen Regelungen ausgefüllt werden können. Dementsprechend wurden in das BDSG 2018 eine Reihe zusätzlicher unternehmensrelevanter Datenverarbeitungstatbestände aufgenommen, die großteils auch schon im bisherigen BDSG enthalten waren:

- Videoüberwachung, insbesondere zur Wahrnehmung des Hausrechts, § 4 BDSG 2018,
- Verarbeitung besonderer Kategorien personenbezogener Daten, § 22 BDSG 2018,
- Weiterverarbeitung personenbezogener Daten, § 22 BDSG 2018,
- Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses, § 26 BDSG 2018.

Äußerst fraglich ist, ob der Gesetzgeber § 4 BDSG 2018 europarechtskonform gestaltet hat, da die DS-GVO für die Videoüberwachung für private Zwecke (z. B. das Hausrecht) keine Öffnungsklausel für nationale Rechtsnormen enthält (Kühling 2017, S. 1987). Diese Rechtsfrage wird letztlich der Europäische Gerichtshof entscheiden müssen. Den Unternehmen ist zu raten, bis zu einer höchstrichterlichen Entscheidung ihren Einsatz von Videoanlagen nicht nur mit § 4 BDSG 2018, sondern auch anhand der Voraussetzungen gem. Art. 6(1) f) DS-GVO zu prüfen.

3.2.4 Rechte der betroffenen Personen

Die der betroffenen Person zustehenden Rechte sind in Kapitel III DS-GVO geregelt:

- Grundprinzip der Transparenz („transparent information, communication and modalities for the exercise of the rights“), Art. 12 DS-GVO
- Informationspflicht („information to be provided“), Art. 13, 14 DS-GVO; §§ 29, 32, 33 BDSG 2018
- Auskunftsrecht („right of access“), Art. 15 DS-GVO; §§ 29, 34 BDSG 2018
- Recht auf Berichtigung („right to rectification“), Art. 16 DS-GVO
- Recht auf Löschung/Vergessenwerden („right to erasure"/"right to be forgotten“), Art. 17 DS-GVO; § 35 BDSG 2018
- Recht auf Einschränkung der Verarbeitung („right to restriction of processing“), Art. 18 DS-GVO; § 35 BDSG 2018
- Recht auf Datenübertragbarkeit („right to data portability“), Art. 20 DS-GVO
- Widerspruchsrecht („right to object“), Art. 21 DS-GVO

Verglichen mit dem BDSG sind die Betroffenenrechte in der DS-GVO erheblich umfassender formuliert; zudem werden neue Rechte eingeführt. Das Recht auf Löschung sowie das Recht auf Datenübertragbarkeit dürfte bei den Unternehmen einen erheblichen Anpassungs- und Umsetzungsaufwand hervorrufen:

Löschungsvorschriften gibt es schon nach dem aktuell geltenden Datenschutzrecht, vgl. § 35 BDSG. Dies wurde jetzt zu einem Recht der betroffenen Person auf unverzügliche *Löschung* ausgestaltet, falls einer der Tatbestände des Art. 17 DS-GVO vorliegt. Angesichts einer Vielzahl von Regelungen zu Aufbewahrungsfristen im Hinblick auf personenbezogene Daten im Handelsrecht, Steuerrecht etc. wird ein Unternehmen nicht daran vorbeikommen, ein umfassendes Löschkonzept im Hinblick auf sämtliche personenbezogenen Daten im Unternehmen zu entwickeln (Keppeler und Berning 2017, S. 314).

Weiterhin wurde erstmalig ein Recht auf *Datenübertragbarkeit* eingeführt. Dieses Recht ist bedeutsam nicht nur für Unternehmen des Social Media Bereichs, sondern für alle Unternehmen mit Massengeschäft, wie Banken, Versicherungen, Energieversorger, Internetversender etc. (Strubel 2017, S. 355). Die betroffene Person, vor allem der Kunde, hat das Recht, die ihn betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und zu erwirken, dass die Daten direkt von einem Verantwortlichen an einen anderen Verantwortlichen (zum Beispiel ein neuer Vertragspartner des Kunden) übermittelt werden, Art. 20(2) DS-GVO.

Kann das Unternehmen die Daten nicht rechtzeitig in einem datenschutzkonformen Format liefern/übertragen und erleidet der Kunde deswegen einen Schaden, muss das Unternehmen mit Schadensersatzansprüchen rechnen.

Beispiel

Unternehmer Bangebux möchte seine mit der Firma Nichtsnutz-Versicherungs-AG bestehenden gewerblichen Versicherungsverträge beenden und zur Firma Sorgenfrei-Versicherungs-AG wechseln, die ihm ein vielversprechendes Vertragsangebot unterbreitet hat. Er bittet Nichtsnutz um Herausgabe seiner personenbezogenen Daten einschließlich der Risikoanalyse zum Versicherungsschutz im geforderten gängigen Format. Da N dieser Bitte nur mit Verzögerung nachkommt, können die Verträge mit S nicht rechtzeitig geschlossen werden. Prompt fällt im versicherungslosen Zeitraum ein Schaden an, der bei bestehender Versicherung abgedeckt gewesen wäre. – N muss den Schaden gemäß Art. 82 DS-GVO übernehmen.

3.2.5 Präventiver Datenschutz

Die DS-GVO enthält eine Reihe von personellen, technischen und organisatorischen Anforderungen an den präventiven Datenschutz. Viele davon sind bereits aus dem bisherigen Datenschutzrecht vom Ansatz her bekannt, allerdings im neuen Datenschutzrecht erheblich ausgebaut worden:

- Führung eines Verzeichnisses über alle Verarbeitungstätigkeiten, Art. 30 DS-GVO
- Durchführung technischer und organisatorischer Maßnahmen zwecks Gewährleistung der rechtmäßigen und sicheren Datenverarbeitung, Art. 24, 25, 32 DS-GVO
- Durchführung von Datenschutz- Folgenabschätzungen, Art. 35, 36 DS-GVO
- Bestellung eines Datenschutzbeauftragten, Art. 37–39 DS-GVO; § 40 BDSG 2018

Nach dem aktuellen BDSG hat das Unternehmen eine Übersicht zu den Verfahren automatisierter Datenverarbeitungen zu erstellen und dem Datenschutzbeauftragten zu übergeben, §§ 4 d (1), 4 g (2) BDSG. Die fehlende oder unzureichende Erstellung einer solchen Verfahrensübersicht ist nicht bußgeldbewehrt (Freiherr von dem Bussche 2016, § 4e BDSG Rn. 16).

Zukünftig muss das Unternehmen ein *Verzeichnis über alle Verarbeitungstätigkeiten* („record of processing activities“) führen, welches auf Anfrage der Aufsichtsbehörde vorzulegen ist, Art. 30 DS-GVO. Mit ihm soll das Unternehmen den Nachweis führen, dass es alle Regelungen der DS-GVO (formelles und materielles Datenschutzrecht) eingehalten hat, ErwGr. 82 (Wybitul 2016, Rn. 137–144; Hamann 2017, S. 1092–1094; Gossen und Schramm 2017, S. 7).

Unternehmen mit weniger als 250 Beschäftigten sind unter bestimmten Voraussetzungen von der Verzeichnispflicht befreit, Art. 30(5) DS-GVO. Gleichwohl ist auch für diese Unternehmen die Erstellung eines solchen Verzeichnisses sinnvoll, da andernfalls die umfangreichen Informations- und Auskunftsrechte betroffener Personen gem. Art. 13–15 DS-GVO nicht ohne Weiteres erfüllt werden können. Im Übrigen dürfte die Befreiung von der Verzeichnispflicht nur selten greifen, da die Rückausnahme der „nicht nur

gelegentlichen Verarbeitung“ praktisch immer gegeben ist: Auch in kleinen Unternehmen existiert – zumindest in manchen Bereichen wie z. B. in der Personalverwaltung – eine regelmäßige (= nicht nur gelegentliche) Datenverarbeitung, sodass auch von diesen Unternehmen ein Verzeichnis zu führen ist (Martini 2017, Art. 30 Rn. 34).

Das Verzeichnis muss gem. Art. 30(1) DS-GVO folgende Angaben enthalten:

a) Namen und Kontaktdaten des für die Verarbeitung Verantwortlichen (ggf. auch Vertreter und Datenschutzbeauftragter)
b) Zwecke der Verarbeitung
c) Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
d) Kategorien von Empfängern, an die die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (auch in Drittländern)
e) Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32(1) DS-GVO

Die Nichterstellung, aber auch ein unvollständiges Verzeichnis ist bußgeldbewehrt, vgl. Art. 83(4) a) DS-GVO.

Auch der Gegenstand des Verzeichnisses hat sich geändert: von den *Verfahren automatischer Verarbeitungen* zu den *Verarbeitungstätigkeiten*.

Der Begriff des *Verfahrens* gemäß §§ 4d, 4e BDSG wird mit Blick auf Art. 18(1) Datenschutz-Richtlinie eher großzügig verstanden: nicht jede einzelne Verarbeitung, sondern Bündel von Verarbeitungsvorgängen mit einheitlichem Zweck ist Verfahren i. S. der Vorschrift, so z. B. die Telefondatenerfassung, die Personalverwaltung etc. (Freiherr von dem Bussche 2016, § 4d BDSG Rn. 6).

Dagegen stellt Art. 30(1) DS-GVO auf die *Verarbeitungstätigkeit* ab, wobei Verarbeitung in Art. 4 Nr. 2 DS-GVO legaldefiniert ist und grds. den einzelnen Vorgang meint (Spoerr 2017, Art. 30 Rn. 6). Dementsprechend sieht die Praxis in der Erstellung eines solchen (notgedrungen umfangreichen) Verzeichnisses auch den „Löwenanteil“ der bis zum 25.05.2018 zu leistenden Anpassungstätigkeiten des Unternehmens (Baumgartner 2017, S. 406; Hamann 2017, S. 1092 f.).

Bei der Erstellung des Verzeichnisses ist insbesondere zu berücksichtigen, dass sich in den letzten Jahren die Zahl der „Datenverarbeitungsorte“ im Unternehmen vervielfacht hat. Ein Großteil der Beschäftigten ist mit Mobilgeräten und entsprechender Software ausgestattet. Smartphones, Laptops, Notebooks etc. sind technisch imstande, in vielfältiger Weise Datenverarbeitungen vorzunehmen. Schon die Führung eines Personenverzeichnisses mit den üblichen Personenstammdaten (z. B. die Kundenkontakte des Vertriebsmitarbeiters) auf dem Smartphone oder im E-Mail-Account ist Datenverarbeitung im Sinne der DS-GVO, da

es sich um ein Dateisystem i. S. d. Art. 2(1), 4 Nr. 6 DS-GVO handelt. All das muss angemessen dokumentiert werden, um den Informationsrechten der betroffenen Personen gem. Art. 13, 14 DS-GVO nachkommen zu können, ggf. eine Datenschutz-Folgenabschätzung durchführen zu können und geeignete technische und organisatorische Maßnahmen zum Datenschutz umsetzen zu können. Von daher ist jedem Unternehmen die Implementierung eines umfassenden Mobile Device Management zu empfehlen (Tiemeyer 2017, S. 26 f.).

Unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung sowie Wahrscheinlichkeit und Schwere der Risiken für die Rechte der betroffenen Personen muss das Unternehmen geeignete technische und organisatorische Maßnahmen (appropriate technical and organisational measures) ergreifen, um die DS-GVO-konforme Datenverarbeitung sicherzustellen, Art. 24(1) DS-GVO und ErwGr. 74–77. Die getroffenen Maßnahmen müssen erforderlichenfalls überprüft und aktualisiert werden.

Der Begriff der Maßnahmen ist weit zu verstehen: Gemeint sind demnach alle Handlungen, die dem Ziel der verordnungskonformen Datenverarbeitung dienen, ob es nun die technischen Systeme, die Software, das mit der Datenverarbeitung befasste Personal oder die Geschäftsabläufe betrifft (Martini 2017, Art. 24 DS-GVO Rn. 20–23).

Das Unternehmen muss auch den Nachweis dafür erbringen, dass es dieser Pflicht Genüge getan hat. So muss zum Beispiel ein Kunde nicht beweisen, auf welche Art und Weise und wo im Unternehmen eine Datenschutzverletzung zu seinen Lasten begangen wurde; vielmehr muss das Unternehmen den Nachweis erbringen, dass es alle betrieblichen Abläufe DS-GVO-konform organisiert hat. Kann es den Nachweis nicht führen, drohen Geldbuße und Schadensersatz, Art. 82–84 DS-GVO.

Für die Einführung eines solchen Datenschutz-Präventionsmanagements empfiehlt es sich, sich am *Standard-Datenschutzmodell* der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zu orientieren (Erprobungsfassung von der 92. Konferenz im November 2016).

Speziell die Sicherheit der Datenverarbeitung ist in Art. 32 DS-GVO, ErwGr. 83 geregelt. Das Unternehmen muss geeignete technische und organisatorische Maßnahmen treffen, um personenbezogene Daten insbesondere vor Vernichtung, Verlust oder unbefugter Veränderung oder Offenlegung oder unbefugtem Zugang zu schützen.

Auch hier sollten sich Unternehmen der zur Verfügung stehenden Fachexpertise bedienen: So hat das Bundesamt für Sicherheit in der Informationstechnik im März 2017 den BSI-Standard 200-2 (IT-Grundschutz-Methodik) – Community Draft – veröffentlicht, der den Rahmen für ein Informationssicherheits-Managementsystem enthält. Der Rahmen bietet drei Stufen der Absicherung:

- die Basis-Absicherung für den schnellen Einstieg in ein Sicherheitsmanagement
- die Kern-Absicherung für elementare Geschäftsprozesse und Ressourcen
- die Standard-Absicherung für einen hohen Schutzbedarf

Basis- wie auch Kern-Absicherung sind insbesondere für kleine und mittlere Unternehmen geeignet (Münch 2016, S. 29).

Die Aufgaben des *Datenschutzbeauftragten* („data protection officer“) sind in Art. 39 DS-GVO genannt. Der Schwerpunkt der Tätigkeit des Datenschutzbeauftragten wird künftig auf der Beratung und Unterstützung der Unternehmensleitung liegen, s. auch ErwGr. 97. Im Gegensatz zum bisherigen Recht wird der Datenschutzbeauftragte nicht mehr zuständig sein für

- Mitarbeiterschulungen,
- Datenschutz-Folgenabschätzungen (bisherige Vorabkontrolle gemäß § 4d (5) BDSG) und
- die Bereitstellung des Verfahrensverzeichnisses;

diese Aufgaben obliegen ab 2018 dem Unternehmen selbst (Lantwin 2017, S. 413 f.).

3.2.6 Folgen von Datenschutzverletzungen

Bei einer Verletzung des Schutzes personenbezogener Daten („personal data breach“) muss das Unternehmen den Vorfall der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden melden, Art. 33 DS-GVO, ErwGr. 85; zudem muss die Verletzung einschließlich aller damit zusammenhängenden Fakten, ihre Auswirkungen und die ergriffenen Abhilfemaßnahmen dokumentiert werden. Das Unterlassen der Meldung ist bußgeldbewehrt, Art. 83(4) a) DS-GVO.

Von der Meldepflicht kann das Unternehmen dann absehen, wenn von der Verletzung keine Gefahren für die Rechte der Betroffenen ausgehen. Allerdings ist das Unternehmen für diesen Ausnahmetatbestand beweispflichtig, sodass man davon ausgehen kann, dass sich Unternehmen im Zweifel für eine Meldung entscheiden.

Darüber hinaus sind auch von einer Datenschutzverletzung *betroffene Personen zu benachrichtigen;* allerdings nur dann, wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Person besteht, Art. 34 DS-GVO, ErwGr. 86.

Betroffene Personen, denen wegen eines Verstoßes gegen das Datenschutzrecht ein Schaden entstanden ist, haben gegen das Unternehmen einen Anspruch auf *Schadensersatz* („right to receive compensation for the damage suffered“), Art. 82 DS-GVO. Von dieser Vorschrift werden nicht nur Verstöße gegen die DS-GVO erfasst, sondern auch Verstöße gegen Vorschriften des BDSG 2018 oder Verstöße gegen bereichsspezifische Datenschutzregelungen, z. B. im Bereich des nationalen Arbeits- und Sozialrechts, vgl. ErwGr. 146.

Während § 7 BDSG lediglich einen Ersatz des materiellen Schadens zulässt, ist gemäß Art. 82 DS-GVO auch der immaterielle Schaden zu ersetzen. Der Begriff des Schadens selbst soll nach dem Willen des Verordnungsgebers weit ausgelegt werden, ErwGr. 146.

Die drohenden drakonischen *Bußgelder* („administrative fines“) gem. Art. 83 DS-GVO wurden bereits in der Einführung dieses Beitrags angesprochen. Weitere Sanktionsmöglichkeiten auf mitgliedstaatlicher Ebene sind, wie Art. 84 DS-GVO zeigt, nicht ausgeschlossen.

Hinzuweisen ist schließlich auf die seit 2016 mögliche *Datenschutzverbandsklage* nach dem Unterlassungsklagengesetz. Danach können Verbraucherschutzverbände ein Unternehmen auf Unterlassung und Beseitigung verklagen, falls das Unternehmen gegen Datenschutzbestimmungen zulasten eines Verbrauchers verstoßen hat, vgl. § 2(2) Nr. 11 UKlaG (Halfmeier 2016, S. 1126).

3.3 Haftung des Organs gegenüber dem Unternehmen

Die bisherigen Ausführungen haben gezeigt, dass ein Unternehmen als Verantwortlicher im Sinne der DS-GVO in verschiedener Hinsicht Nachteile erleiden kann, wenn es ein datenschutzwidriges Verhalten zu verantworten hat. Es können Schadenersatzzahlungen gegenüber betroffenen Personen geleistet worden sein; die Aufsichtsbehörde kann eine Geldbuße verhängt haben; es können Prozesskosten angefallen sein. In allen Fällen stellt sich die Frage, ob und inwieweit das Unternehmen *Dritte in Regress nehmen* kann. Infrage kommen Ansprüche gegen:

- andere Verantwortliche oder Auftragsverarbeiter bei gemeinschaftlicher Datenverarbeitung, Art. 82(4),(5) DS-GVO,
- Beschäftigte des Unternehmens, die gegen das Datenschutzrecht verstoßen haben,
- freie Mitarbeiter oder sonstige Dienstleister (z. B. ein externer Datenschutzbeauftragter) sowie
- Mitglieder des gesellschaftsrechtlichen Organs (Vorstand, Geschäftsführung) des Unternehmens (Organhaftung).

Näher betrachtet werden soll die *Organhaftung.* Zum einen kann ein Organmitglied in eigener Person gegen Datenschutzvorschriften verstoßen. In diesem Fall haftet es selbstverständlich wegen Verletzung seiner Pflicht, bei der Ausübung seiner Tätigkeit immer die gesetzlichen Verpflichtungen seines Unternehmens zu beachten. Im unternehmerischen Alltag stellt sich aber meistens die Frage, ob Organmitglieder auch *für Gesetzesverletzungen haften,* die *von Beschäftigten des Unternehmens oder Externen begangen* wurden. Darauf soll im Folgenden eingegangen werden.

3.3.1 Aufgaben, Pflichten, Verantwortung

Organe der Aktiengesellschaft und der GmbH als juristische Personen sind der Vorstand bzw. die Geschäftsführung. Der Vorstand leitet die Aktiengesellschaft, § 76(1) AktG; die Geschäftsführer führen die Geschäfte der GmbH.

Vorstand bzw. Geschäftsführung sind für die Erledigung sämtlicher Geschäfte zuständig, die der Betrieb des Unternehmens mit sich bringt (Grundsatz der Allzuständigkeit). Besteht das Organ aus mehreren Personen, bestehen die Pflichten nebeneinander und

sind parallel zu erfüllen (Grundsatz der *Gesamtzuständigkeit*). Für die Erfüllung ihrer Pflichten sind die Organmitglieder gemeinsam verantwortlich und haften auch gemeinschaftlich gegenüber der Gesellschaft (Grundsatz der *Gesamtverantwortung*), (Schmidt-Husson 2016, § 6 Rn. 4).

Im Einzelnen lassen sich die *Pflichten eines Organs* wie folgt unterscheiden:

- gesellschaftsrechtliche Pflichten laut Satzung/Gesellschaftsvertrag oder Gesetz
- Treuepflicht gegenüber dem Unternehmen
- Pflicht zur kollegialen Zusammenarbeit innerhalb des Organs
- Pflicht zur sorgfältigen Unternehmensleitung nach anerkannten technischen, betriebswirtschaftlichen und sonstigen fachlichen Methoden im Rahmen des Geschäftsleiterermessens
- Einhaltung gesetzlicher Pflichten des Unternehmens aus den verschiedenen Bereichen des Rechts wie z. B. Arbeitsrecht, Wettbewerbsrecht, Verwaltungsrecht, Steuerrecht, Sozialrecht oder Datenschutzrecht (Legalitätspflicht) (Raiser und Veil 2015, § 14 Rn. 65, 78–95; § 42 Rn. 79–89)

3.3.2 Delegation

Die Grundsätze der Allzuständigkeit und der Gesamtzuständigkeit sind dispositiv; d. h., die Organe können Aufgabenbereiche, Pflichten und Befugnisse grundsätzlich delegieren:

- Eine *horizontale* Delegation ist gegeben, wenn das mehrköpfige Organ Ressorts bildet und eine entsprechende Geschäftsverteilung vornimmt, z. B. Personal-, IT-, Vertriebs- oder Produktionsvorstand.
- Von einer *vertikalen* Delegation spricht man, wenn Aufgaben auf hierarchisch nachgeordnete Beschäftigte übertragen werden.
- Schließlich können Aufgaben auch an externe Dritte abgegeben werden, **externe** Delegation (zum Beispiel im Rahmen des Outsourcing).

Nicht in allen Fällen ist eine Delegation zulässig; *nicht delegierbar* sind Aufgaben, die zum *Kern der Unternehmensführung* gehören; gleichwohl können andere Personen durchaus mit vorbereitenden Tätigkeiten für diese Leitungsentscheidungen betraut werden (Schmidt-Husson 2016, § 6 Rn. 6 ff., 15 ff.).

Im Bereich der **IT und des Datenschutzes** müssen die zu delegierenden Aufgaben, Pflichten und Befugnisse mit besonderer Akkuratesse analysiert werden, da das neue Datenschutzrecht – wie gezeigt – zahlreiche inhaltliche, organisatorische und technische Pflichten enthält; insbesondere genügt es nicht, einem Vorstandsmitglied pauschal den Bereich der Informationstechnik zuzuordnen.

Die Einhaltung der Rechtmäßigkeitsvoraussetzungen bei den einzelnen Datenverarbeitungen wird bei den einzelnen Fach- bzw. Bereichsvorständen verbleiben müssen:

Der Personalvorstand ist für den Arbeitnehmerdatenschutz zuständig; dem Vertriebsvorstand obliegt der Datenschutz im Hinblick auf die Kundendaten usw. Die Gewährleistung der Rechte der Betroffenen (Kunden, Lieferanten, Beschäftigte) sollte ebenfalls in der Obhut der jeweiligen Bereichsvorstände verbleiben. Die Meldepflichten und sonstige Kontakte gegenüber der Aufsichtsbehörde werden zweckmäßigerweise beim Datenschutzbeauftragten angesiedelt.

3.3.3 Legalitätskontrollpflicht

Allerdings ändert auch die Durchführung einer – an sich zulässigen – Delegation nichts an dem Grundsatz der *Gesamtverantwortung:* Sie verbleibt beim Organ und ist *unteilbar*. Die Organmitglieder können ihrer Gesamtverantwortung nicht entrinnen. Zwar kann sich das Organ durch Ressortbildung (horizontale Delegation) oder vertikale bzw. externe Delegation von bestimmten Handlungspflichten befreien; dafür entsteht mit Durchführung der Delegation eine *organschaftliche Aufsichtspflicht,* die wiederum aus mehreren Einzelpflichten besteht, nämlich den Pflichten, den Delegat *sorgfältig (!) auszuwählen, einzuweisen und zu überwachen (Legalitätskontrollpflicht)* (Schmidt-Husson 2016, § 6 Rn. 10, 12, 26–35 mit weiteren Nachweisen zur Rechtsprechung und Literatur)[5].

Diese Pflicht zur sorgfältigen Auswahl, Einweisung und ständigen Überwachung dürfte einem Mitglied des Vorstandes oder der Geschäftsführung ohne Weiteres einleuchten, soweit es sich die Situation der ihm nachgeordneten Mitarbeiterinnen und Mitarbeiter vor Augen führt. Diese Kontrollpflicht gilt aber auch auf horizontaler Ebene, wenn das Kollegialorgan (d. h. der Gesamtvorstand bzw. das Geschäftsführergremium) einzelnen Mitgliedern des Organs Aufgaben und Befugnisse zuweist, die der Legalitätspflicht unterliegen.

[5]Insbesondere das vielbeachtete Urteil des Landgerichts München I vom 10.12.2013 in der Sache Siemens ./. Neubürger hat die rechtswissenschaftlichen Erkenntnisse zur Corporate Compliance zusammengefasst und die Gesamtverantwortung des Vorstands für die Sicherstellung legalen Handelns des Unternehmens durch Überwachung hervorgehoben. – Zum Hintergrund: Nach der Aufdeckung zahlreicher „schwarzer Kassen“ im Jahr 2006 hatte die Siemens AG gegenüber den in diesem Zeitraum amtierenden Vorstandsmitgliedern Schadensersatzforderungen geltend gemacht. Man hatte sich mit den Beteiligten einvernehmlich auf Ersatzleistungen einigen können. Lediglich der ehemalige Finanzvorstand Hans-Joachim Neubürger war dazu nicht bereit. Die daraufhin von Siemens im Januar 2010 gegen Neubürger erhobene Klage über 15 Mio. EUR endete mit dem bereits erwähnten stattgebenden Urteil des Landgerichts vom Dezember 2013. Im Sommer 2014 schlossen Siemens und Neubürger einen Vergleich über 2,5 Mio. EUR ab, der Ende Januar 2015 von der Hauptversammlung akzeptiert wurde. Im Februar 2015 beging Hans-Joachim Neubürger Suizid.

Beispiel

Der Vorstand der Ruhesanft Lebensversicherungs-AG weist im Rahmen der Geschäftsverteilung dem frisch gebackenen Vorstandsmitglied und promovierten Altphilologen Megabit die Zuständigkeit für die Informationstechnik zu mit der Begründung, dass er doch „so versiert im Umgang mit seinem Smartphone sei". Der Vorstandsbeschluss ergeht auf Anregung des Vorstandsvorsitzenden Brüllkopf, dessen Vorschläge grundsätzlich niemand infrage zu stellen wagt. Unterlagen zu den konkret übertragenen Aufgaben und Handlungsbefugnissen existieren nicht.

Der im Beispiel beschriebene Beschluss dürfte gleich aus mehreren Gründen keine wirksame Delegation darstellen: Der Gesamtvorstand hätte vor der Zuweisung an Megabit eine Aufgabenbeschreibung für einen IT-Vorstand mit entsprechendem Anforderungsprofil entwickeln und überprüfen müssen, ob Megabit das Anforderungsprofil hinreichend erfüllt. Zudem müssten die zu übertragenden Aufgaben und Handlungsbefugnisse konkret beschrieben sein, damit die Erfüllung der Legalitätspflicht des Gesamtvorstands überhaupt auf Megabit übergehen kann.

Auch die Tatsache, dass sich alle Vorstandsmitglieder der Autorität des Vorsitzenden gebeugt haben, ist rechtlich irrelevant: Es gibt keine Richtlinienkompetenz des Vorstandsvorsitzenden; vielmehr ergehen die Entscheidungen des Gremiums gemäß den festgelegten Beschlussfassungs- und Abstimmungsregeln. Hält ein Organmitglied eine Maßnahme des Organs für einen Verstoß gegen die Legalitätspflicht, muss er sich bei seinen Kollegen mittels Gegenvorstellung (Remonstration) nachdrücklich für die Umsetzung seiner eigenen Vorstellungen einsetzen und notfalls sogar das Überwachungsorgan (Aufsichtsrat etc.) einschalten.

Ist die Delegation nicht korrekt durchgeführt worden, verbleibt es bei der Gesamtzuständigkeit des Vorstands, sodass jedes Vorstandsmitglied weiterhin verpflichtet ist, die IT-Aktivitäten in allen (!) Bereichen des Unternehmens ständig zu überwachen.

Literatur

Albrecht JP, Jotzo F (2017) Das neue Datenschutzrecht der EU. Nomos, Baden-Baden

Baumgartner U (2017) Die Umsetzung der DS-GVO in der Praxis – ein Werkstattbericht. Zeitschrift für Datenschutz 2017(9):405

Bundesamt für Sicherheit in der Informationstechnik (2017) BSI-Standard 200-2 – Community Draft. Bonn

Freiherr von dem Bussche A (2016) In: Plath K-U (Hrsg) BDSG/DS-GVO, 2. Aufl. Otto Schmidt, Köln

Halfmeier A (2016) Die neue Datenschutzverbandsklage. Neue Juristische Wochenschrift 2016(16):1126

Gossen H, Schramm M (2017) Das Verarbeitungsverzeichnis der DS-GVO. Zeitschrift für Datenschutz 2017(1):7

Hamann C (2017) Europäische Datenschutz-Grundverordnung – neue Organisationspflichten für Unternehmen. Betriebs-Berater 2017(20):1090

Keppeler LM, Berning W (2017) Technische und rechtliche Probleme bei der Umsetzung der DS-GVO-Löschpflichten. Zeitschrift für Datenschutz 2017(7):314
Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2016) Das Standard-Datenschutzmodell
Kühling J (2017) Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen. Neue Juristische Wochenschrift 2017(28):1985
Landgericht München I (2013) Urteil vom 10.12.2013, Az. 5 HK O 1387/10
Lantwin T (2017) Risikoberuf Datenschutzbeauftragter ? – Die Haftung nach der neuen DS-GVO. Zeitschrift für Datenschutz 2017(9):411
Martini M (2017) In: Paal B, Pauly D (Hrsg) Datenschutz-Grundverordnung. C.H. Beck, München
Münch I (2016) Informationssicherheit in Unternehmen, comply 2016(3):29. www.comply-online.de. Zugegriffen: 28. Sept. 2017
Plath K-U (2016) In: Plath K-U (Hrsg) BDSG/DS-GVO, 2. Aufl. Otto Schmidt, Köln
Raiser T, Veil R (2015) Recht der Kapitalgesellschaften, 6. Aufl. Vahlen, München
Schmidt-Husson F (2016) In: Hauschka C et al (Hrsg) Corporate compliance, 3. Aufl. C.H. Beck, München
Spoerr W (2017) In: Wolff HA, Brink S (Hrsg) BeckOK Datenschutzrecht. C.H. Beck, München
Strubel M (2017) Anwendungsbereich des Rechts auf Datenübertragbarkeit. Zeitschrift für Datenschutz 2017(8):355
Tiemeyer E (2017) Technologien für die Digitalisierung. Computer und Arbeit 2017(5):26
Wybitul T (2016) EU-Datenschutz-Grundverordnung im Unternehmen. dfv, Frankfurt a. M.

Über den Autor

Dr. jur. Jürgen Monhemius ist seit 1998 Inhaber der Professur für Wirtschaftsrecht und Arbeitsrecht am Fachbereich Wirtschaftswissenschaften der Hochschule Bonn-Rhein-Sieg in Sankt Augustin und zertifizierter Mediator.

Studium der Rechtswissenschaften in Bochum, München und Bonn; Referendarzeit beim Oberlandesgericht Köln; Promotion an der Universität Bonn. Mehrjährige Tätigkeit in einer mittelständischen Wirtschaftsprüfungsgesellschaft; danach mehrjährige Tätigkeit als Verwaltungsleiter und Haushaltsbeauftragter bei einer Bundesoberbehörde; von 1994 bis 1998 Inhaber einer Professur für Dienstrecht und Polizeirecht an der Hochschule des Bundes für öffentliche Verwaltung, Fachbereich Bundespolizei in Lübeck. Veröffentlichungen auf dem Gebiet des Dienstrechts sowie des Wirtschafts- und Gesellschaftsrechts.