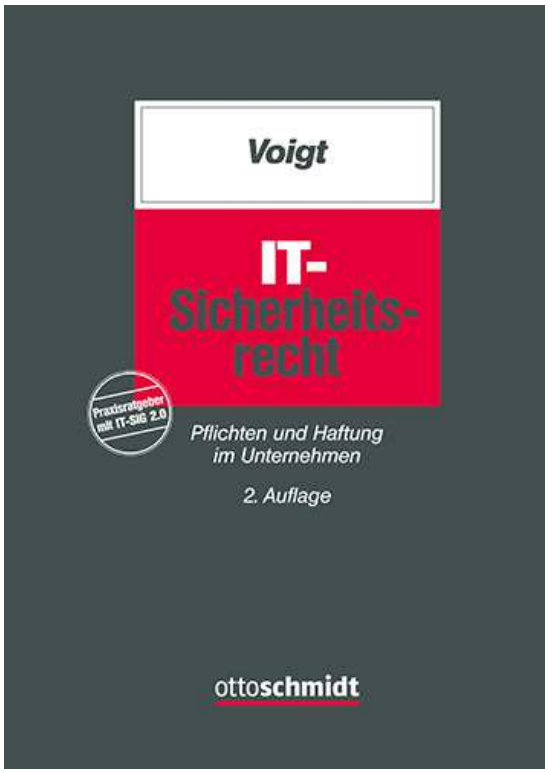
Leseprobe zu

Voigt

IT-Sicherheitsrecht

Pflichten und Haftung im Unternehmen



ISBN 978-3-504-56108-6

2. Auflage 2021, ca. 250 Seiten Lexikonformat, brosch.

79,80 € inkl. MwSt.

Vorwort zur zweiten Auflage

Das Informationssicherheitsrecht im Allgemeinen und das IT-Sicherheitsrecht im Konkreten sind in den letzten Jahren umfangreich fortentwickelt worden. Eine der wichtigsten Neuerungen stellt sicherlich das IT-Sicherheitsgesetz 2.0 dar, welches den Anwendungsbereich der Verpflichteten, die Befugnisse des BSI, die zu ergreifenden Sicherheitsmaßnahmen sowie die bei Nichtbefolgung zu erwartenden Bußgelder deutlich erweitert hat. Daneben führten Änderungen im Telekommunikations- und Telemedienrecht, im Gesundheitsrecht und Finanzrecht, im Arbeitsrecht und im allgemeinen Zivilrecht ebenso zu Änderungen im Informations- und IT-Sicherheitsrecht wie das Inkrafttreten des Geschäftsgeheimnisgesetzes.

Neben den vorgenannten umfangreichen rechtlichen Änderungen ist auch die Bedrohungslage aus IT-Sicherheitssicht eine andere als zum Zeitpunkt des Erscheinens der ersten Auflage dieses Handbuchs. KRITIS-Betreiber werden zunehmend Gegenstand von Ransomware-Attacken, und Angriffe auf Krankenhaus-IT führten aufgrund ausgefallener medizinischer Geräte zu ersten Todesfällen. Auch die Corona-Pandemie und das manchmal überhastet eingeführte Home-Office haben aufgrund der damit häufig einhergehenden geringeren Absicherung der IT-Systeme zu einem Anstieg der IT-Angriffe auf Unternehmen geführt.

Vor diesem Hintergrund war es notwendig, das vorliegende Handbuch umfangreich zu überarbeiten und an die neue Sach- und Rechtslage anzupassen. Ich danke Mahsum Bas, Rita Danz, Christoph Emde, Christin Carlsen und Mirjam Dietrich für die Unterstützung bei der Überarbeitung des Handbuchs und für diverse konstruktive Gespräche. Daneben bedanke ich mich bei Frau Sonja Behrens-Khaled vom Verlag Dr. Otto Schmidt für die Betreuung und zeitnahe Herausgabe des Buchs.

Wie immer bin ich dankbar für Hinweise, Anregungen und Kritik jeder Art zu diesem Buch, welche Sie gerne per E-Mail an p.voigt@taylorwessing.com richten können.

Berlin, im November 2021

Paul Voigt

Inhaltsverzeichnis

E. Datenschutz und IT-Sicherheit

I. Vorbemerkung

Eine der bedeutsamsten Quellen des Rechts der Informationssicherheit bildet das Datenschutzrecht, welches Vorgaben hinsichtlich der **Sicherheit personenbezogener Daten** aufstellt. Der Schutz dieser aus Sicht der betroffenen Personen besonders schützenswerten Informationen wird über unterschiedliche **Anforderungen an die unternehmenseigenen IT-Systeme und Verfahrensabläufe** gewährleistet. Personenbezogene Daten haben sich längst zu einem wertvollen Wirtschaftsgut entwickelt und spielen auch **im Unternehmensalltag** eine **wichtige Rolle**.[1] So verarbeiten Unternehmen täglich personenbezogene Daten von Mitarbeitern, Kunden oder Geschäftspartnern. Aus diesem Grund müssen die Vorgaben des Datenschutzrechts berücksichtigt werden, nicht zuletzt unter dem Gesichtspunkt, dass mit Inkrafttreten der **DSGVO** nicht nur eine Verschärfung der Datenschutzanforderungen, sondern gleichsam auch der drohenden Bußgelder für entsprechende Verstöße stattgefunden hat. 164

II. Rechtsentwicklung und Rechtsquellen

Mit der raschen Zunahme IT-gestützter Unternehmensführung und dem Anstieg massenhafter und schneller Verarbeitungen von Daten riefen die dadurch auftretenden **Risiken für die Persönlichkeitsrechte** der Betroffenen bereits in den 1970er Jahren den Gesetzgeber auf den Plan.[2] Das Datenschutzniveau wurde im Zuge zahlreicher Anpassungen des BDSG seitdem stetig angehoben. Dafür war ganz erheblich auch das **Tätigwerden des europäischen Gesetzgebers** entscheidend. Nicht nur Daten können ohne weiteres nationale Landesgrenzen überwinden, sondern auch die Geschäftstätigkeiten von Unternehmen beschränken sich häufig nicht bloß auf den nationalen Kontext. Um die erheblich voneinander abweichenden Datenschutzbestimmungen in den Mitgliedstaaten der EG (jetzt: EU) anzugleichen und damit Rechtssicherheit in Bezug auf grenzüberschreitende Verarbeitungsvorgänge zu schaffen, wurde 1995 die EG-Datenschutzrichtlinie[3] verabschiedet.[4] 165

1 *Reiners*, ZD 2015, 51, 55; *Martini* in Paal/Pauly, DSGVO, Art. 25 Rz. 45; *Voigt*/*von dem Bussche*, Handbuch DSGVO, Teil 1.

2 *Gusy*/*Eichenhofer* in BeckOK-DatenschutzR, 37. Edition, 1.8.2021, BDSG § 1 Rz. 5 f.; zur historischen Entwicklung ausführlich *Simitis*/*Hornung*/*Spiecker gen. Döhmann* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Einleitung Rz. 1 ff.

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

4 *Bretthauer* in Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rz. 3 ff.; *Voigt*/*von dem Bussche*, Handbuch DSGVO, Teil 1.1.1.

166 Bei der Umsetzung der **EG-Datenschutzrichtlinie** ins nationale Recht der Mitgliedstaaten konnte das verfolgte Ziel der Angleichung des Datenschutzniveaus innerhalb der EU nicht vollständig erreicht werden. Ausgehend von den nationalen Umsetzungsgesetzen wurden unterschiedliche Datenschutz-Regime und damit auch unterschiedliche nationale Informations-Sicherheitsvorgaben in Bezug auf die Verarbeitung personenbezogener Daten etabliert. Datenverarbeitungen, die in einem EU-Mitgliedstaat rechtskonform waren, konnten in einem anderen im Hinblick auf die spezifische Ausführung der Verarbeitung rechtswidrig sein.[1] Zur stärkeren Angleichung des Datenschutzes innerhalb der EU wurde die seit dem 25.5.2018 anwendbare **EU-Datenschutz-Grundverordnung**[2] geschaffen, die in allen EU-Mitgliedstaaten unmittelbare Anwendung findet.

1. DSGVO und BDSG

167 Durch die **unmittelbare Anwendbarkeit der DSGVO** innerhalb der EU-Mitgliedstaaten wird ein einheitliches datenschutzrechtliches Informations-Sicherheitsniveau geschaffen. Die Rechtsform der europäischen Verordnung lässt grundsätzlich wenig Raum für das Tätigwerden des nationalen Gesetzgebers.[3] Für Unternehmen bedeutet die Vereinheitlichung des Datenschutzstandards **innerhalb der EU** eine erhöhte **Rechtssicherheit hinsichtlich** der Anforderungen an ihre Datenverarbeitungstätigkeiten. Davon erhoffte sich die EU nicht zuletzt eine Förderung der digitalen Wirtschaft im europäischen Binnenmarkt.[4] An Unternehmen stellt die DSGVO im Vergleich zur vorher geltenden Rechtslage erhöhte **Informations-Sicherheitsanforderungen**. Neben der Verschärfung bereits bestehender Datenschutzpflichten und Bußgeldrahmen wurden auch neue Pflichten eingeführt.

168 Trotz ihrer Allgemeinverbindlichkeit lässt die DSGVO über zahlreiche **Öffnungsklauseln** einen **Spielraum** für die EU-Mitgliedstaaten **zur Schaffung nationaler Regelungen** zur Ergänzung der Verordnung. Dadurch bestehen auch künftig in begrenztem Rahmen nationale Besonderheiten hinsichtlich der datenschutzrechtlichen IT-Sicherheitsstandards fort. Deutschland hat von diesem Spielraum insbesondere im **BDSG**[5] Gebrauch gemacht. In Deutschland tätige oder ansässige Unternehmen (zum Anwendungsbereich s. Rz. 175 ff.) müssen aus diesem Grund die Informations-Sicherheitsvorgaben der DSGVO und des BDSG gleichermaßen einhalten. So **gehen die Regelungen der DSGVO dem BDSG grundsätzlich vor**, wobei das **BDSG**

1 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 1.1.1.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119/1.

3 *Ruffert* in Calliess/Ruffert, EUV/AEUV, Art. 288 AEUV Rz. 19 f.; Ständige Rechtsprechung etwa EuGH, Urt. v. 14.12.1971 – C-43/71, ErwGr. 9; EuGH, Urt. v. 17.5.1972 – C-93/71, ErwGr. 5 f.

4 ErwGr. 9 DSGVO.

5 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU) vom 30.7.2017, BGBl. I S. 2097.

zur Anwendung gelangt, sofern die DSGVO nationale Regelungen über entsprechende **Öffnungsklauseln** ermöglicht, § 1 Abs. 5 BDSG.

2. Bereichsspezifisches Datenschutzrecht

169 Die relevanten datenschutzrechtlichen IT-Sicherheitsvorschriften sind auf verschiedene Spezialgesetze verteilt. Ergänzend zu bzw. anstelle der Regelungen des allgemeinen Datenschutzrechts aus der DSGVO und dem BDSG kommt ggf. bereichsspezifisches Datenschutzrecht zur Anwendung. So **verdrängen** bereichsspezifische Datenschutzregelungen auf nationaler Ebene **entsprechende Regelungen des BDSG**, § 1 Abs. 2 BDSG. Auch die DSGVO enthält eine Reihe von Kollisionsregelungen. So wird die DSGVO gem. ihrem Art. 95 von bereichsspezifischen Datenschutzregelungen, die der Umsetzung der ePrivacy-Richtlinie der EU[1] dienen, verdrängt. Praxisrelevante Regelungen enthält diesbezüglich etwa das **TTDSG** (Telekommunikation-Telemedien-Datenschutz-Gesetz) für den Bereich der Telemedien (s. Rz. 362 ff.) sowie für den Bereich der Telekommunikation (s. Rz. 383 ff.).[2] Trotz der vorhandenen Kollisionsregelungen bestanden bisher **Unklarheiten beim Zusammenspiel verschiedener Rechtsquellen des Datenschutzrechts**, insbesondere in den beiden vorgenannten Bereichen.[3] So bestand in der Vergangenheit Rechtsunsicherheit dahingehend, wann die Datenschutzbestimmungen aus dem TMG, welches bisher datenschutzrechtliche Regelungen für Telemedien enthielt, und des TKG, welches bisher datenschutzrechtliche Regelungen für Telekommunikation enthielt, zur Anwendung gelangen sollten und wann sie vom allgemeinen Datenschutzrecht verdrängt wurden.[4] Hintergrund dieser Schwierigkeiten war, dass die jeweiligen Regelungen die ePrivacy-Richtlinie nicht oder nur zum Teil umsetzten.[5] Um diese Unklarheiten zu beseitigen entschied sich der Gesetzgeber, die Datenschutzbestimmungen des TMG und des TKG, einschließlich der Bestimmungen zum Schutz des Fernmeldegeheimnisses, im TTDSG zusammenzuführen und die bestehenden Vorschriften an die DSGVO und die ePrivacy-Richtlinie anzupassen.

170 Zu den für die IT-Sicherheit relevanten Regelungen des TTDSG gehören u.a. Vorgaben zu **technischen und organisatorischen Vorkehrungen** gem. § 19 TTDSG (für eine ausführliche Darstellung der IT-Sicherheitspflichten nach dem TTDSG s. auch Rz. 366 ff.). Die Regelungen ersetzen die bisherigen Bestimmungen des § 13 Abs. 4–7 TMG. Sie verpflichten den Diensteanbieter u.a. seine Dienste so zu gestalten, dass

1 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201/37.

2 Das TTDSG ist in überwiegenden Teilen zum 1.12.2021 in Kraft getreten. Bis dahin galten die Regelungen des TMG und des TKG weiter.

3 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 8.3.

4 *von dem Bussche/Schelinski* in Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 7.1 Rz. 16, 49, 51 ff.

5 Vgl. *Schwartmann/Benedikt/Reif*, MMR 2021, 99.

- jederzeit eine Möglichkeit für die Nutzer besteht, die Nutzung der Dienste zu beenden und der Nutzer die Dienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann (§ 19 Abs. 1 TTDSG),
- zumutbare technische und organisatorische Maßnahmen zum Schutz der genutzten technischen Einrichtungen vor unerlaubtem Zugriff auf personenbezogene Daten und vor Störungen, einschließlich von außen, ergriffen werden (§ 19 Abs. 4 TTDSG).

171 Die Sicherungspflicht des Diensteanbieters wird entsprechend dieser Vorschrift auf Maßnahmen beschränkt, die technisch möglich und wirtschaftlich zumutbar sind. Diese Kriterien sollen die Verhältnismäßigkeit der Sicherungspflichten gewährleisten.[1] Die Ermittlung dessen, was wirtschaftlich zumutbar ist, erfordert eine Abwägung der Kosten und sonstigen wirtschaftlichen Nachteile einer Maßnahme mit den Gefahren, die ohne diese Maßnahme drohen. Dabei können bspw. die folgenden Kriterien eine Rolle spielen: Kosten der Maßnahme, Effektivität der Maßnahme, Auswirkungen auf den Betrieb bzw. das Angebot durch die Maßnahme, mögliche negative Reaktionen der Nutzer, Wettbewerbssituation zu anderen Anbietern (die dieser Pflicht ggf. nicht unterliegen), drohende Gefahren bei Unterlassen der Maßnahme, Schutzalternativen durch die Nutzer selbst.[2]

172 Zudem sind ergänzende Vorschriften wie § 25 TTDSG, der Regelungen zum Schutz der Privatsphäre bei Endeinrichtungen enthält, zu beachten. Dabei wird die Zulässigkeit von **Cookies** grundsätzlich an ein **Einwilligungserfordernis** entsprechend der DSGVO geknüpft, wovon lediglich zur Diensterbringung „**unbedingt erforderliche**" Cookies ausgenommen werden.[3]

173 Der europäische Gesetzgeber hat die Schwierigkeiten im Zusammenspiel von ePrivacy-Richtlinie und DSGVO, sowie ggf. unterschiedlichen Informationssicherheitsvorgaben der Mitgliedstaaten längst erkannt und **arbeitet seit Jahren** an einer **ePrivacy-Verordnung**, welche die ePrivacy-Richtlinie ersetzen und durch die **Schaffung abschließender bereichsspezifischer Datenschutzregelungen** stärker harmonisierte Anforderungen vorgeben soll.[4] Nachdem die Europäische Kommission im Januar 2017 ihren Vorschlag für die Verordnung veröffentlichte[5], erfolgten mehrere Erörterungen im Rat; die ePrivacy-Verordnung drohte letztlich zu scheitern.[6] Zum 20.5.2021

1 *Schmitz* in Spindler/Schmitz, TMG, § 13 Rz. 97.
2 *Schmitz* in Spindler/Schmitz, TMG, § 13 Rz. 99.
3 *Strocher*, ZD-Aktuell 2021, 05222; s. auch *Piltz/Kühner*, ZD 2021, 123, 126 f.
4 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 8.3 m.w.N.
5 Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Europäischen Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG vom 10.1.2017, abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications, zuletzt aufgerufen am 27.5.2021.
6 Der aktuelle Gesetzgebungsstand ist abrufbar unter: https://eur-lex.europa.eu/procedure/DE/2017_3?&sortOrder=asc, zuletzt aufgerufen am 27.5.2021.

starteten jedoch die Trilog-Verhandlungen zur ePrivacy-Verordnung zwischen Parlament, Kommission und Rat, was die Verabschiedung der Verordnung in greifbarere Nähe rückt.[1] Wann die ePrivacy-Verordnung jedoch das ordentliche Gesetzgebungsverfahren endgültig durchlaufen haben wird, lässt sich derzeit nicht sagen.

Unternehmen sollten berücksichtigen, dass trotz Inkrafttreten des TTDSG bestimmte IT-sicherheitsspezifische Vorschriften des TKG fortbestehen (s. Rz. 362 ff.). Eine Änderung entsprechender Bestimmungen im TKG erfolgte unlängst über das Telekommunikationsmodernisierungsgesetz (s. Rz. 383 ff.). Diesen Regelungen unterfallende Unternehmen müssen die Vorgaben von TTDSG, TKG, DSGVO bzw. BDSG entsprechend berücksichtigen.[2] 174

III. Anwendungsbereich

Die DSGVO zeichnet sich durch einen sehr weiten Anwendungsbereich aus und findet daher auf zahlreiche **Unternehmen innerhalb und außerhalb der EU** Anwendung. Neben der DSGVO können auf nationaler Ebene auch das BDSG und die Landesdatenschutzgesetze sowie etwaige weitere datenschutzrechtliche Spezialnormen zur Anwendung gelangen. 175

1. Sachlicher Anwendungsbereich

Auf Grundlage von Art. 2 DSGVO umfasst der sachliche Anwendungsbereich der DSGVO grundsätzlich **jegliche Verarbeitung personenbezogener** Daten, etwa in Form des Erhebens, Erfassens, der Organisation, des Ordnens, der Speicherung oder des Löschens von Daten.[3] Dies bezieht sich nicht nur auf **IT-gestützte Datenverarbeitungsvorgänge**, etwa durch Computer, Smartphones oder Smart Devices, sondern auch auf **manuelle Datenverarbeitungen**, etwa durch Mitarbeiter des Unternehmens, sofern eine systematische Verwaltung manuell verarbeiteter Daten erfolgt.[4] 176

a) Personenbezogene Daten

Die Verarbeitung muss sich für eine Anwendbarkeit der DSGVO auf „personenbezogene Daten" beziehen, wobei es sich gem. Art. 4 Nr. 1 DSGVO um **Informationen** bzw. Einzelangaben handelt, **die sich auf** eine **identifizierte oder identifizierbare** 177

1 *Rauer/Ettig*, ZD 2021, 18, 20; *Piltz*, ePrivacy Verordnung: Mitgliedstaaten sollen über opt-in oder opt-out für den Einsatz von Cookies für Werbezwecke entscheiden, abrufbar unter: https://www.delegedata.de/2018/01/eprivacy-verordnung-mitgliedstaaten-sollen-ueber-opt-in-oder-opt-out-fuer-den-einsatz-von-cookies-fuer-werbezwecke-entscheiden/, zuletzt aufgerufen am 27.5.2021.

2 Vgl. *Schallbruch*, CR 2016, 663, 669; *Schneider*, Datenschutz, Kapitel 7 VI 5; *Sydow* in Sydow, DSGVO, Einleitung Rz. 44.

3 *Ernst* in Paal/Pauly, DSGVO, Art. 2 Rz. 2 ff.; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.1.

4 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.1 m.w.N.; *Bäcker* in BeckOK-DatenschutzR, 37. Edition, 1.8.2021, Art. 2 Rz. 4 ff.

natürliche Person beziehen.[1] Es ist ausreichend, wenn eine Person mittels Zuordnung zu einem oder mehreren Kennungsmerkmalen ermittelt werden kann, wie etwa Namen, Identifikationsnummern (Sozialversicherungs-, Personalausweisnummer), Standortdaten oder Online-Kennungen (IP-Adressen, Cookies, etc.).[2] Eine solche Identifikationsmöglichkeit ist auch gegeben, wenn ein **Unternehmen ohne unverhältnismäßigen Aufwand** auf **zusätzliche (externe) Informationen zugreifen kann**, die eine Identifikation betroffener Personen ermöglichen.[3] Dabei kann es sich etwa um (leicht) zugängliche Daten aus dem Internet handeln.[4] Für die Bestimmung der Identifizierungsmöglichkeit sind etwa die zeitlichen, technischen und finanziellen Mittel zur Informationsbeschaffung sowie Informationsrechte des Unternehmens gegenüber Dritten (etwa bzgl. Kommunikationsdaten im Falle von Cyber-Angriffen, s. Rz. 595 ff.) zu berücksichtigen.[5] Je einfacher und schneller ein Unternehmen Zugriff auf entsprechende Informationen erlangen kann, desto eher ist eine Person identifizierbar und die DSGVO gelangt zur Anwendung.

b) Anonymisierung als Mittel zum Ausschluss der Anwendbarkeit der DSGVO

178 Die Anonymisierung von personenbezogenen Daten bildet eine von verschiedenartigen Techniken zur Veränderung personenbezogener Daten, um deren **Sicherheit zu erhöhen** und kann zur Anwendung gelangen, soweit ein Personenbezug der verarbeiteten Daten nicht mehr erforderlich ist. Bei der Anonymisierung werden die **Daten** so **modifiziert**, dass deren **Verbindung zu einer natürlichen Person nicht (mehr) besteht**.[6] Um zu ermitteln ob diese Aufhebung gelungen ist, könnte entweder der **absolute oder relative Personenbezug** maßgeblich sein. Eine Anonymisierung unter Zugrundelegung des absoluten Personenbezugs setzt voraus, dass eine Wiederherstellung des Personenbezugs für niemanden möglich ist, wohingegen eine Anonymisierung unter Zugrundelegung des relativen Personenbezugs vorliegt, wenn eine Identifizierung der Person nach allgemeiner Lebenserfahrung oder dem Stand der Wissenschaft und Technik aufgrund des unverhältnismäßigen Aufwands beim konkreten Datenempfänger nicht zu erwarten ist.[7] Von dieser Unterscheidung ausgehend stellt sich die Frage, welche dieser Varianten die Anforderungen an eine erfolgreiche Anonymisierung im Sinne der DSGVO erfüllt. Eine Anonymisierung unter Zugrundelegung des absoluten Personenbezugs ist in Zeiten von **Big Data** kaum realisierbar. Big Data bezeichnet die Auswertung großer, aus einer Vielzahl unterschiedlicher Quellen stammender unstrukturierter Daten zum Zwecke der Erkennung von Gesetzmäßigkeiten, Korrelationen und Kausalitäten und der Generierung neuer Informationen (Kontext-

1 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2 m.w.N.
2 *Borges* in BeckOK IT-Recht, 3. Edition, 1.7.2021, Teil 3 DSGVO Art. 4 Rz. 11 ff.; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2 m.w.N.
3 *Schild* in BeckOK-DatenschutzR, 37. Edition, 1.8.2021, DS-GVO Art. 4 Rz. 15: *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2.1 m.w.N.
4 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2.1 m.w.N.
5 ErwGr. 26 DSGVO; BGH, Urt. v. 16.5.2017 – VI ZR 135/13 = CR 2017, 662.
6 ErwGr. 26 DSGVO; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2.2.
7 *Roßnagel*, ZD 2021, 188, 189.

wissen).[1] Nach einer Studie[2] konnten aus Datensätzen mit 15 Merkmalen wie Alter oder Wohnort 99,98 % der US-Amerikaner identifiziert werden, in 80 % der Fälle genügten sogar nur die drei Merkmale Geschlecht, Geburtsdatum und Postleitzahl zur Re-Identifikation.[3] Eine **Anonymisierung unter Zugrundelegung des absoluten Personenbezugs** derart, dass die Wiederherstellung des Personenbezugs für niemanden möglich ist, dürfte – wie dieses Beispiel illustriert – häufig nicht möglich sein und ist daher im Regelfall datenschutzrechtlich auch **nicht gefordert**.[4]

179 Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach **allgemeinem Ermessen** wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Die zum Zeitpunkt der Verarbeitung verfügbaren **Technologien und technologischen Entwicklungen** sind zu berücksichtigen, sodass eine fortlaufende **Risikoanalyse** erfolgen muss um festzustellen, ob die Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden können. **Objektive Faktoren**, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, können dabei zur Beurteilung herangezogen werden.[5] Die Anonymisierung lässt sich technisch auf ganz unterschiedliche Art und Weise umsetzen. Dabei kann der Personenbezug der Daten z.B. über die Veränderung ihrer Genauigkeit (Randomisierung) oder die Verallgemeinerung der Kennungsmerkmale der betroffenen Person (Verallgemeinerung) entfernt werden.[6]

180 Unternehmen halten regelmäßig große Datenbestände vor, von denen sie letztlich nur einen kleinen Teil für ihre Verarbeitungstätigkeiten benötigen.[7] Die **Nicht-Erfassung oder Löschung überschüssiger Daten** kann dabei helfen, eine Anonymisierung umzusetzen.[8] Diese Maßnahmen ermöglichen nicht nur die Sicherheit der Daten, sondern die **DSGVO ist überdies nicht anwendbar**, so dass das **Unternehmen keinen datenschutzrechtlichen Informationssicherheitspflichten** bzgl. der entsprechenden

1 *Schulz* in Gola, DS-GVO, Art. 6 Rz. 254.

2 *Rocher/Hendrickx/de Montjoye*, Estimating the success of re-identifications in incomplete datasets using generative models, Article number: 3069 (2019), abrufbar unter: https://www.nature.com/articles/s41467-019-10933-3, zuletzt aufgerufen am 28.5.2021; *Schürmann*, DSB 2021, 49, 51.

3 *Schürmann*, DSB 2021, 49, 51.

4 *BfDI*, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche vom 29.6.2020, S. 4, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Positionspapier-Anonymisierung-DSGVO-TKG.html, zuletzt abgerufen am 28.5.2021; *Ziebarth* in Sydow, DSGVO, Art. 4 Rz. 29 f.; ErwGr. 26 DSGVO.

5 ErwGr. 26 DSGVO; *Klar/Kühling* in Kühling/Buchner, DS-GVO BDSG, Art. 4 Nr. 1 Rz. 20 ff.

6 Ausführlich zu verschiedenen Methoden zur Pseudonymisierung und Anonymisierung von personenbezogenen Daten *Bischoff/Drechsler*, PharmR 2020, 389, 390 ff.; *Schürmann*, DSB 2021, 49, 50; Art.-29-Datenschutzgruppe, WP 216 vom 10.4.2014, S. 12, 16.

7 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2.2.

8 *Schröder*, Datenschutzrecht für die Praxis, Kapitel 2 Teil II.1.b; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2.2.

Daten unterliegt.[1] Jedoch ist die Anonymisierung der personenbezogenen Daten nach wohl herrschender Meinung selbst eine Verarbeitungstätigkeit und damit am Rechtmäßigkeitsmaßstab der DSGVO zu messen.[2] Abgesehen von rechtlichen Vorteilen kann eine solche Datenminimierung im Unternehmen zur **Einsparung von Zeit, Kosten und personellen Ressourcen** führen, die für die Verwaltung der Datenbestände erforderlich sind.[3] Unternehmen sollten daher prüfen, ob und welche Daten anonymisiert werden können.

2. Persönlicher Anwendungsbereich

181 Die DSGVO findet auf Unternehmen Anwendung, die personenbezogene Daten verarbeiten oder für deren Verarbeitung verantwortlich sind. Dabei können ihnen entweder als **„Verantwortliche" oder „Auftragsverarbeiter"** Pflichten im Hinblick auf den Datenschutz zugewiesen werden.

a) Verantwortlicher

182 Umfassenden Datenschutzverpflichtungen unterliegen „Verantwortliche". Dabei handelt es sich nach Art. 4 Nr. 7 DSGVO um **jedes Unternehmen**, welches allein oder gemeinsam mit anderen **über** die **Zwecke und Mittel der Verarbeitung** von personenbezogenen Daten **entscheidet**. Die datenschutzrechtliche Verantwortlichkeit knüpft nicht an die Ausführung von Verarbeitungstätigkeiten durch das Unternehmen, sondern an dessen **Entscheidungsbefugnis** in Bezug auf die Verarbeitung an. Der Verantwortliche entscheidet **über die Zwecke und wesentlichen Elemente der Datenverarbeitung**, etwa welche Daten für wie lange durch wen verarbeitet werden sollen und welche Sicherheitsmaßnahmen ergriffen werden müssen.[4] Eine datenschutzrechtliche Verantwortlichkeit ergibt sich vorrangig in folgenden Konstellationen:[5]

- **Implizite rechtliche Verantwortlichkeit**: Diese ergibt sich aus allgemeinen Rechtsvorschriften oder ständiger Rechtspraxis. Ganz unterschiedliche Rechtsbereiche können Unternehmen eine Entscheidungsbefugnis bzgl. Daten einräumen, etwa Zivil-, Handels- oder Arbeitsrecht. So ist bspw. der Arbeitgeber grundsätzlich für die Daten seiner Mitarbeiter verantwortlich.
- **Tatsächliche Einflussmöglichkeit**: Eine Verantwortlichkeit des Unternehmens kann sich auch auf der Grundlage seiner Verträge mit Dritten ergeben. So muss ein

1 ErwGr. 26 DSGVO.

2 Zu den möglichen Rechtsgrundlagen s. *Schürmann*, DSB 2021, 49, 50; *BfDI*, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche vom 29.6.2020, S. 5 ff.

3 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.1.2.2.

4 *Mantz/Spittka* in Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, § 6 Rz. 35 ff.; *Borges* in BeckOK IT-Recht, 3. Edition, 1.7.2021, Teil 3 DSGVO Art. 4 Rz. 78 ff.; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.2.1.3.

5 *Laue* in Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 1 Einführung Rz. 47–51; Art.-29-Datenschutzgruppe, WP 169 vom 16.2.2010, S. 10 ff.

Unternehmen zur Abwicklung seiner Verträge mit Kunden etwa deren Kontaktdaten verarbeiten und ist damit für deren Verarbeitung verantwortlich.

Innerhalb von **Konzernstrukturen ist jedes Unternehmen grundsätzlich eigenständig** für die seiner Kontrolle unterliegenden Verarbeitungstätigkeiten **verantwortlich**, so dass die einzelnen Gesellschaften jeweils Verantwortliche sind.[1] Daneben kennt die DSGVO auch den Fall der „**gemeinsam für die Verarbeitung Verantwortlichen**", welcher z.B. im Fall von Konzernstrukturen vorliegen kann. Legen mehrere Unternehmen die Zwecke und/oder wesentlichen Mittel der Datenverarbeitung gemeinsam fest, teilen sie gem. Art. 26 DSGVO ihre Datenschutzpflichten und müssen etwa die Verantwortlichkeit für die datenschutzrechtlichen IT-Sicherheitspflichten klar untereinander aufteilen. 183

b) Auftragsverarbeiter

Neben dem Verantwortlichen treffen nach der DSGVO auch den „Auftragsverarbeiter" in einem etwas **geringeren Umfang Datenschutzpflichten**. Dabei handelt es sich nach Art. 4 Nr. 8 DSGVO um **Unternehmen**, die **personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten**. Eine entsprechende Beteiligung an der Datenverarbeitung beruht damit auf einer Entscheidung des Verantwortlichen, der die Datenverarbeitung entweder intern durchführen kann oder ein oder mehrere externe Unternehmen mit der Datenverarbeitung beauftragt, was letztere zu Auftragsverarbeitern macht.[2] Dabei kann es sich etwa um **Outsourcing-Anbieter, Cloud-Computing-Anbieter oder Betreiber von Rechenzentren** handeln.[3] 184

3. Räumlicher Anwendungsbereich

Der **räumliche Anwendungsbereich** der DSGVO wurde **an die Aktivitäten global agierender Unternehmen und Konzerne angepasst** und macht an den Außengrenzen der EU nicht Halt. Die Bestimmungen des Art. 3 DSGVO knüpfen an die **Verbindung der Datenverarbeitung zur EU** an, sei es, weil die Verarbeitung im Rahmen der Tätigkeit einer europäischen Niederlassung des Unternehmens stattfindet oder weil die Verarbeitung natürliche Personen in der EU betrifft. **Ähnliche Kriterien** sieht auch das BDSG vor, um die **deutschen Regelungen** anwendbar zu machen. 185

a) DSGVO

Findet eine Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung des Unternehmens in der EU statt, so findet die DSGVO gem. ihrem Art. 3 Abs. 1 Anwendung. Dafür ist es nicht erforderlich, dass die **Niederlassung** die Verarbeitung selbst 186

1 *Schild* in BeckOK-DatenschutzR, 37. Edition, 1.8.2021, Art. 4 Rz. 87 ff.; *Borges* in BeckOK IT-Recht, 3. Edition, 1.7.2021, Teil 3 DSGVO Art. 4 Rz. 76; Art.-29-Datenschutzgruppe, WP 169 vom 16.2.2010, S. 13 f.

2 Art.-29-Datenschutzgruppe, WP 169 vom 16.2.2010, S. 30 f.

3 *Schulz* in Gola/Heckmann, BDSG, § 46 Rz. 49 ff.; s. zur Abgrenzung von Verantwortlichem und Auftragsverarbeiter *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.2.2 m.w.N.

ausführt.[1] Es reicht aus, wenn die Niederlassung **mit ihren Tätigkeiten** die **vom Unternehmen ausgeführten Verarbeitungstätigkeiten wirtschaftlich unterstützt**.[2] Der eigentliche Ort der Datenverarbeitung ist daher für die Anwendbarkeit der DSGVO letztlich nicht entscheidend. Eine Niederlassung erfordert die effektive und tatsächliche Ausübung einer Tätigkeit mittels **fester Einrichtung**.[3] So ist es unerheblich, ob die wirtschaftliche Förderung der Datenverarbeitung durch eine bloße Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit erfolgt, solange die Niederlassung einen **gewissen Grad an Beständigkeit** aufweist.[4] Entscheidend dafür ist die konkrete Art der Tätigkeit, mit der die Niederlassung an der Datenverarbeitung mitwirkt.[5] Bietet ein Unternehmen seine Dienstleistungen ausschließlich über das Internet an, so kann es für eine Niederlassung ausreichen, wenn ein einziger Vertreter in einem EU-Mitgliedstaat in das Anbieten oder die Verwaltung der Dienstleistungen involviert ist.[6] Sowohl **personelle als auch materielle Ressourcen** können eine „feste Einrichtung" bilden, etwa das Vorhandensein eines Bankkontos oder Postfachs in der EU.[7]

187 Unterhält ein datenverarbeitendes Unternehmen keine Niederlassung in der EU, kann die DSGVO dennoch nach Art. 3 Abs. 2 DSGVO zur Anwendung gelangen, wenn ein Unternehmen **Kunden im europäischen Binnenmarkt anvisiert**.[8] Eine solche Situation liegt etwa vor, wenn ein Unternehmen **gezielt Waren oder Dienstleistungen gegenüber betroffenen Personen in der EU anbietet** und in diesem Zusammenhang Daten verarbeitet, etwa im Falle über das Internet agierender Unternehmen.[9] Derartige Geschäftstätigkeiten liegen bei der Verwendung einer in der EU gesprochenen Sprache, der Akzeptanz des Euro als Währung, der Erwähnung von europäischen Kunden oder der Möglichkeit von Warenlieferungen in die EU nahe.[10] Die DSGVO findet ebenfalls Anwendung, sofern eine Datenverarbeitung damit im Zusammenhang steht, das **in der EU stattfindende Verhalten von natürlichen Personen zu überwachen**. Dies betrifft Datenverarbeitungen zur Analyse/Vorhersage von Präferenzen, Verhaltensweisen und Meinungen von Kunden.[11] Die Vorschrift betrifft Un-

1 EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 – Google Spain, CR 2014, 460, ErwGr. 52; EuGH, Urt. v. 24.9.2019 – Rs. C-507/17, ErwGr. 41, 48 ff.; *Plath* in Plath, BDSG/DSGVO, Art. 3 Rz. 9; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.3.1.2.
2 EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 – Google Spain, CR 2014, 460, ErwGr. 55; *Plath* in Plath, BDSG/DSGVO, Art. 3 Rz. 9.
3 ErwGr. 22 DSGVO; *Ernst* in Paal/Pauly, DSGVO, Art. 3 Rz. 7.
4 ErwGr. 22 DSGVO; EuGH, Urt. v. 1.10.2015 – Rs. C-230/14 – Weltimmo, CR 2016, 109, ErwGr. 29; *Ernst* in Paal/Pauly, DSGVO, Art. 3 Rz. 7 f.
5 EuGH, Urt. v. 1.10.2015 – Rs. C-230/14 – Weltimmo, CR 2016, 109, ErwGr. 29.
6 EuGH, Urt. v. 1.10.2015 – Rs. C-230/14 – Weltimmo, CR 2016, 109, ErwGr. 29 f.
7 *Plath* in Plath, BDSG/DSGVO, Art. 3 Rz. 8; s. auch *Klar* in Kühling/Buchner, DS-GVO BDSG, Art. 3 Rz. 43 ff.
8 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.3.2.
9 *Barlag* in Roßnagel, DSGVO, § 3 Rz. 18.
10 ErwGr. 23 DSGVO.
11 *Zerdick* in Ehmann/Selmayr, DS-GVO, Art. 3 Rz. 20; ErwGr. 24 DSGVO.

ternehmen, die **Web-Tracking oder Profiling** zu den vorgenannten Zwecken durchführen, etwa über Cookies oder Social-Media-Plug-Ins.[1]

Agieren Unternehmen als Verantwortliche oder Auftragsverarbeiter[2] somit **gezielt auf dem europäischen Markt** – egal ob über eine oder mehrere Niederlassungen oder über das Internet – **ist die DSGVO anwendbar**, so dass die datenschutzrechtlichen IT-Sicherheitspflichten eingehalten werden müssen. Davon sind nicht nur Unternehmen innerhalb der EU, sondern auch zahlreiche Unternehmen außerhalb der EU betroffen.[3] 188

b) BDSG

§ 1 BDSG legt den räumlichen Anwendungsbereich der deutschen Konkretisierungsvorschriften zur DSGVO fest. Das **BDSG** enthält der DSGVO inhaltlich entsprechende Regelungen, so dass **in Deutschland tätige Unternehmen** grundsätzlich zusätzlich zur DSGVO den Regelungen des BDSG unterliegen. Dies kann entweder der Fall sein, weil sie als **Verantwortliche/Auftragsverarbeiter** personenbezogene Daten **in Deutschland** verarbeiten oder Datenverarbeitungen im Rahmen der Tätigkeiten einer **deutschen Niederlassung** erfolgen, § 1 Abs. 4 Nr. 1, 2 BDSG. Zudem finden die Vorschriften des BDSG auf Unternehmen Anwendung, die zwar keine Niederlassung in der EU haben, aber in den Anwendungsbereich der DSGVO fallen, weil sie mit ihren Tätigkeiten **Kunden im EWR anvisieren**, § 1 Abs. 4 Nr. 3 BDSG.[4] Für länderübergreifend agierende Unternehmen ergeben sich erhebliche Rechtsunsicherheiten daraus, dass das **BDSG keinen ausdrücklichen Inlandsbezug voraussetzt.** Zum Teil wird daher sinnvollerweise über den Wortlaut hinaus eine einschränkende Auslegung der Vorschrift befürwortet. Danach soll ein territorialer Bezug, wie die Anvisierung des deutschen Marktes vorausgesetzt werden.[5] Zudem fehlt es an einer **Kollisionsregel** für Fälle, in denen neben den deutschen Vorschriften auch **nationale DSGVO-Umsetzungsgesetze anderer EU-Mitgliedstaaten** potentiell zur Anwendung gelangen.[6] Dies wird Unternehmen künftig vor Probleme bei der Umsetzung datenschutzrechtlicher IT-Sicherheitsvorgaben stellen. 189

Beispiel:[7] 190
Ein amerikanisches Unternehmen visiert mit seinen Verarbeitungstätigkeiten den deutschen und den österreichischen Markt an.

1 ErwGr. 24 DSGVO; *Schantz*, NJW 2016, 1841, 1842; *Hornung*, ZD 2012, 99, 102; *Voigt*/*von dem Bussche*, Handbuch DSGVO, Teil 2.3.2.2; *Klar* in Kühling/Buchner, DS-GVO BDSG, Art. 3 Rz. 90 f.

2 Zu diesem Fall ausführlich *Voigt*, Die räumliche Anwendbarkeit der EU Datenschutz-Grundverordnung auf Auftragsverarbeiter im Drittland, 2020, sowie *Voigt*, CR 2021, 307.

3 *Voigt*, CR 2021, 307, 307 ff.

4 Deutscher Bundestag, Drucksache 18/11325, S. 79 f.

5 *Schmidt* in Taeger/Gabel, DSGVO BDSG, § 1 Rz. 34; *Gola*/*Reif* in Gola/Heckmann, BDSG, § 1 Rz. 19.

6 S. dazu *Voigt*/*von dem Bussche*, Handbuch DSGVO, Teil 2.4.

7 *Voigt*/*von dem Bussche*, Handbuch DSGVO, Teil 2.4; *Klar* in Kühling/Buchner, DS-GVO BDSG, § 1 Rz. 30.

Aus § 1 Abs. 5 BDSG resultiert zunächst die Anwendbarkeit der DSGVO. Im Bereich der Öffnungsklauseln gelangt auf Grundlage seines § 1 Abs. 4 Nr. 3 das BDSG zur Anwendung, weil seinem Wortlaut nach das amerikanische Unternehmen den deutschen Markt anvisiert. Sieht das österreichische Gesetz ebenfalls eine solche Anwendbarkeitsregelung vor, muss das Unternehmen beide nationalen Gesetze gleichzeitig berücksichtigen. Daher muss es ggf. divergierende Vorgaben im Bereich der Öffnungsklauseln erfüllen.

191 Das Beispiel verdeutlicht, dass im Bereich der Öffnungsklauseln ein kompliziertes Geflecht aus nationalen datenschutzrechtlichen Besonderheiten auch mit Inkrafttreten der DSGVO aufrechterhalten wird.[1] **Unternehmen** müssen dann im Hinblick auf ihre Tätigkeiten in verschiedenen EU-Mitgliedstaaten **ggf. unterschiedliche nationale IT-Sicherheitsstandards** erfüllen. Die Problematik fehlender oder nicht hinreichend klarer Kollisionsregelungen dürfte in Anbetracht der mit der DSGVO angestrebten Vollharmonisierung weiterhin Diskussionsbedarf auslösen.[2]

IV. Datenschutzrechtliche IT-Sicherheitsvorgaben

192 Aus dem Personenbezug der in den Anwendungsbereich der DSGVO fallenden **Daten** ergibt sich deren **erhöhte Sensibilität** und Schutzwürdigkeit, die dazu führt, dass die Anforderungen an **IT-Sicherheitsstandards** in Bezug auf den Umgang mit personenbezogenen Daten **besonders hoch** sind. Das Datenschutzrecht gibt dabei nicht nur konkrete Schutzmaßnahmen für die Datenverarbeitung vor, sondern sieht gegenüber Aufsichtsbehörden und betroffenen Personen insbesondere auch Meldepflichten für den Fall von Datenschutzverletzungen vor.

1. IT-Sicherheitsstandard

193 Um die Sicherheit personenbezogener Daten zu gewährleisten, müssen Unternehmen **technische und organisatorische Schutzmaßnahmen** bei der Datenverarbeitung einsetzen. Der gesetzliche Pflichtenumfang folgt dabei einem risikobasierten Ansatz: je mehr Risiken die Verarbeitung für die betroffenen Personen und ihre Daten mit sich bringt, desto umfangreichere Schutzmaßnahmen müssen zum Einsatz kommen.[3] Der **Pflichtenumfang** für Unternehmen ist somit **einzelfallabhängig**, was zu erheblicher Rechtsunsicherheit führt. Es fällt schwer, ein generelles Programm an datenschutzrechtlichen IT-Sicherheitspflichten abzulesen, so dass die Umsetzung der Vorgaben von DSGVO und BDSG Unternehmen vor einige Herausforderungen stellt.[4]

194 Das Datenschutzrecht dient dem Schutz der von der Datenverarbeitung betroffenen Personen, Art. 1 Abs. 1, 2 DSGVO, und nicht demjenigen der Rechtsgüter des Unter-

1 *Schmidt* in Taeger/Gabel, DSGVO BDSG, § 1 Rz. 34; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.4; *Karg*, ZD 2013, 371, 373.
2 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 2.4; *Karg*, ZD 2013, 371, 373.
3 *Schmitz* in Hoeren/Sieber/Holznagel, Multimedia-Recht, Teil 16.2 Rz. 236 f.; ErwGr. 74, 75, 76 DSGVO.
4 *Martini* in Paal/Pauly, DSGVO, Art. 24 Rz. 24; ErwGr. 74, 75, 76 DSGVO.

nehmens.[1] Die allgemeinen unternehmerischen IT-Sicherheitspflichten (s. Rz. 32 ff.) können daher in Konflikt mit den IT-Sicherheitsvorgaben des Datenschutzrechts geraten. Die aus Unternehmenssicht zum Schutz der eigenen Infrastruktur optimalen **Sicherheitsmaßnahmen** lassen sich zum Schutz personenbezogener Daten **nur unter** den teilweise einschränkenden **Vorgaben von DSGVO** und BDSG **umsetzen**, um die Rechte und Rechtsgüter betroffener Personen zu gewährleisten.[2]

Hinweis zum Konflikt Datenschutzrecht und IT-Sicherheitsstandard: 195
Für die Verarbeitung personenbezogener Daten, z.B. in Form einer Erfassung oder Speicherung, bedarf es stets einer Rechtsgrundlage. Hinzu kommen organisatorische Datenschutzanforderungen und Betroffenenrechte, die das datenverarbeitende Unternehmen erfüllen muss. Bestimmte IT-Sicherheitsmaßnahmen lassen sich nur bei Erfassung personenbezogener Daten wirksam umsetzen, wie z.B. **Data-Loss-Prevention-Maßnahmen**, ein **Intrusion-Prevention-System** oder **Logging**.[3] Möchte ein Unternehmen diese IT-Sicherheitsmaßnahmen einsetzen, sind die Vorgaben des Datenschutzrechts unbedingt einzuhalten. Steht dem Unternehmen etwa für eine bestimmte Maßnahme keine Verarbeitungsgrundlage zur Erfüllung, ist ein Ausweichen auf alternative Maßnahmen erforderlich. Damit ist die Bandbreite möglicher IT-Sicherheitsmaßnahmen ggf. eingeschränkt.

a) Technische und organisatorische Maßnahmen

Verantwortliche und **Auftragsverarbeiter** sind **zur Anwendung technischer und organisatorischer Maßnahmen** zum Schutz personenbezogener Daten **verpflichtet**, die dem Risiko der durchgeführten Verarbeitungstätigkeiten entsprechen, Art. 24 Abs. 1, 28 Abs. 1, 32 DSGVO. Hierbei handelt es sich um eine der grundlegendsten Datenschutzpflichten während des Verarbeitungsprozesses.[4] Unternehmen obliegt es daher auch, den Einsatz entsprechender Maßnahmen durch alle an der Verarbeitung beteiligten Mitarbeiter sicherzustellen, Art. 32 Abs. 4 DSGVO. Die Maßnahmen dienen vorrangig der **Datensicherheit**, also dem umfassenden Schutz der zur Verarbeitung eingesetzten IT und Systeme.[5] Konkrete Vorgaben hinsichtlich der einzusetzenden Maßnahmen enthält die DSGVO nicht, so dass Unternehmen eine **ganze Bandbreite möglicher Schutzinstrumente** zur Verfügung steht. Auch die in § 64 BDSG genannten Sicherheitsmaßnahmen können nur Anregungen für die zu implementierenden technischen und organisatorischen Maßnahmen bieten: § 64 BDSG dient der Umsetzung der Richtlinie (EU) 2016/680[6] und findet auf nichtöffentliche Stellen keine Anwendung. 196

1 ErwGr. 1 DSGVO; *Schmidl* in Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rz. 67.
2 *Schmidl* in Hauschka/Moosmayer/Lösler, Corporate Compliance, § 29 Rz. 66 f. m.w.N.; s. zum allgemeinen Konflikt zwischen Compliance und Datenschutzrecht *Voigt*/*Oenning*/*Oenning* in von dem Bussche/Voigt, Konzerndatenschutz, Datenschutzrecht und Compliance, Rz. 1 ff.
3 *Mantz*/*Spittka* in Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, § 6 Rz. 176.
4 *Richter* in Jandt/Steidle, Datenschutz im Internet, Teil B.IV. Rz. 36 ff.; *Voigt*/*von dem Bussche*, Handbuch DSGVO, Teil 3.3.
5 *Mantz* in Sydow, DSGVO, Art. 32 Rz. 1.
6 ABl. L 119/89.

197 **Beispiele technischer und organisatorischer Schutzmaßnahmen[1]:**
- Minimierung der Menge verarbeiteter Daten;
- Pseudonymisierung personenbezogener Daten;
- betroffenen Personen die Überprüfung der Verarbeitungsvorgänge ermöglichen;
- bauliche Maßnahmen zur Verhinderung unbefugter physischer Zugriffe auf personenbezogene Daten, etwa gesicherte Räume, Wachpersonal, passwortgesicherter Zugang oder Mitarbeiterkennungsmaßnahmen;
- regelmäßige Datenschutz-Schulungen für Mitarbeiter;
- kodierte Datenübermittlungen.

198 Welche technischen und organisatorischen Maßnahmen im konkreten Fall angemessen sind, muss das Unternehmen im Wege einer **umfassenden objektiven Risikoabwägung** ermitteln.[2] Dabei sind die Risiken aller an der Verarbeitung Beteiligten zu berücksichtigen: des Unternehmens, der betroffenen Personen und etwaiger Dritter. Das Gesetz nennt darüber hinaus in Art. 32 Abs. 1 DSGVO weitere Gesichtspunkte zur Ermittlung angemessener Schutzmaßnahmen: den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen. Zur **praktischen Umsetzung** der umfassenden Abwägung bietet sich **folgende Vorgehensweise** an:[3]

(1) Ermittlung des Schutzbedarfs der betroffenen Daten: Um den Schutzbedarf der von der Verarbeitung betroffenen Daten zu ermitteln, sollte das Unternehmen prüfen, welches **Schadenspotential** durch Datensicherheitsdefizite im Hinblick auf die betroffenen Daten besteht. Dabei bietet sich eine **Kategorisierung der Daten nach** normalem, hohem und sehr hohem **Schutzbedarf** an. Je größer der Schutzbedarf, desto umfangreicher sollten auch die technischen und organisatorischen Schutzmaßnahmen ausfallen.

(2) Ermittlung des Risikopotentials der Verarbeitung dieser Daten: Die dem Schutzbedarf entsprechenden Maßnahmen müssen unter Berücksichtigung des Risikos ihrer Verarbeitung ausgewählt werden. Dabei sind vorrangig die **Risiken für die betroffenen Personen** zu berücksichtigen, etwa durch die unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung der betroffenen Daten. Ein hohes Risikopotential besteht insbesondere dann, wenn besonders sensible personenbezogene Daten oder die Daten von Kin-

1 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.3.1 m.w.N.; s. auch Bayerisches Landesamt für Datenschutzaufsicht, Good Practice bei technischen und organisatorischen Maßnahmen vom 13.10.2020, abrufbar unter: https://www.lda.bayern.de/media/checkliste/bayl da_checkliste_tom.pdf, zuletzt aufgerufen am 7.6.2021.

2 *Petri* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO, Art. 24 Rz. 11 ff.; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.3.3 m.w.N.

3 S. für die nachfolgenden Ausführungen Bayerisches Landesamt für Datenschutzaufsicht, Sicherheit der Verarbeitung – Art. 32 DS-GVO vom 9.6.2016, abrufbar unter: https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf, zuletzt aufgerufen am 7.6.2021; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.3.3 m.w.N.; *Martini* in Paal/Pauly, DSGVO, Art. 32 Rz. 46 ff.

dern von der Verarbeitung betroffen sind.[1] Bei der Entwicklung angemessener Schutzkonzepte sind allerdings auch die **Interessen des Unternehmens** im Rahmen der Abwägung zu berücksichtigen, etwa die erforderlichen technischen, personellen und finanziellen Ressourcen zur Umsetzung technischer und organisatorischer Maßnahmen, Folgen einer Verletzung des Datenschutzrechts (s. Rz. 232 ff.), Haftungsrisiken und geschäftliche Risiken. Kommt das Unternehmen anhand der konkreten Verarbeitungsumstände zu der Erkenntnis, dass die Datenverarbeitung ein **hohes Risiko** für die betroffenen Personen birgt, ist es zur Durchführung einer noch umfangreicheren Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Datenschutz verpflichtet, Art. 35 DSGVO. Das Ergebnis einer solchen **Datenschutz-Folgenabschätzung** ist ebenfalls im Rahmen der Risikobewertung zu berücksichtigen.[2]

(3) Entwicklung eines Datenschutzkonzepts: Die verschiedenen Risiken und Interessen sind gegeneinander abzuwägen und ihre Ergebnisse dienen als Grundlage für die Entwicklung des angemessenen Datenschutzkonzepts. Dabei werden die Pflichten für jedes Unternehmen auf Einzelfallbasis ausdifferenziert, um ein **angemessenes Verhältnis** von **Aufwand und Nutzen der technischen und organisatorischen Maßnahmen** zu erreichen. Der Aufwand ist dabei auf ein solches Maß beschränkt, welches wirtschaftlich berechtigterweise vom Verantwortlichen/Auftragsverarbeiter erwartet werden kann.[3] Allerdings können unzureichende Schutzmaßnahmen nur bedingt mit Kostengründen gerechtfertigt werden, da bestimmte Mindestanforderungen hinsichtlich des Sicherheitsstandards (s. sogleich Rz. 200 ff.) bestehen. Je nach Größe des Unternehmens ließen sich entsprechende Datenschutzmaßnahmen etwa als Teilbestandteil eines **IT-Sicherheitsmanagementsystems** umsetzen (s. Rz. 643 ff.).

Im Vergleich zu den konkreten Vorgaben des § 9 BDSG a.F. und dessen Anlage enthält die **Selbsteinschätzung des Schutzbedarfs** durch das Unternehmen ein **größeres Element der Unsicherheit**. Hinzu kommt, dass Unternehmen unter Berücksichtigung des Stands der Technik nach Art. 32 Abs. 1 DSGVO ihre **Maßnahmen an technologische Veränderungen fortlaufend anpassen** müssen.[4] Eine entsprechende Orientierung können zumindest ISO-Bestimmungen und das Grundschutz-Kompendium des BSI bieten.[5] Darüber hinaus haben auch die deutschen Datenschutzbehörden im Rahmen einer gemeinsamen Konferenz ein **Standard-Datenschutzmodell** verabschiedet, 199

1 Höchst sensible personenbezogene Daten unterliegen als „besondere Kategorien personenbezogener Daten" nach Art. 9, 10 DSGVO einem besonderen Schutz. Dabei handelt es sich etwa um personenbezogene Daten, die einen Rückschluss auf die Herkunft, politische Orientierung, Religionszugehörigkeit oder Gesundheit betroffener Personen zulassen.

2 ErwGr. 84 DSGVO; *Martini* in Paal/Pauly, DSGVO, Art. 32 Rz. 49.

3 *Piltz* in Gola, DS-GVO, Art. 32 Rz. 20 f.; *Martini* in Paal/Pauly, DSGVO, Art. 32 Rz. 60; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.3.3.

4 *Piltz* in Gola, DS-GVO, Art. 32 Rz. 15 ff.; *Martini* in Paal/Pauly, DSGVO, Art. 32 Rz. 56 ff.

5 *Martini* in Paal/Pauly, DSGVO, Art. 32 Rz. 58 f. m.w.N.

welches eine der möglichen Vorgehensweisen zur Schaffung rechtskonformer technischer und organisatorischer Maßnahmen vorstellt.[1]

b) Mindestschutzanforderungen

200 Auch wenn die DSGVO keine konkreten Maßnahmen zur Umsetzung eines angemessenen datenschutzrechtlichen IT-Sicherheitsstandards vorgibt, stellt Art. 32 Abs. 1 DSGVO zumindest **Mindestanforderungen** an die technischen und organisatorischen Schutzmaßnahmen des Unternehmens. Die Mindestanforderungen sind zur Gewährleistung eines hinreichenden Datenschutzniveaus grundsätzlich erforderlich. Eine Unterschreitung ist nur unter engen Voraussetzungen möglich.[2]

201 So muss die unternehmerische Datenverarbeitung den klassischen Zielen der IT-Sicherheit entsprechen: Das Unternehmen muss **dauerhaft** die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungsmittel** sicherstellen, Art. 32 Abs. 1 lit. b DSGVO. Das Unternehmen muss sowohl einen unbefugten Zugriff auf als auch die unbefugte Offenlegung von personenbezogenen Daten verhindern, sowie den Schutz der IT vor anderweitigen inneren und äußeren Bedrohungen gewährleisten.[3] Kommt es trotz dieser Maßnahmen zu **physischen oder technischen Datensicherheitszwischenfällen**, muss das Unternehmen die **personenbezogenen Daten** und den **Zugang** zu ihnen **rasch wiederherstellen können**, Art. 32 Abs. 1 lit. c DSGVO. Dafür sollten Unternehmen **Backup-Systeme**, redundante Systeme und/oder Notstromaggregate bereithalten.[4] Wie „rasch" die Wiederherstellung zu erfolgen hat, lässt sich der Vorschrift nicht konkret ablesen, so dass das Unternehmen bei Zwischenfällen so schnell wie möglich agieren sollte.[5] Um die Effektivität der getroffenen technischen und organisatorischen Maßnahmen dauerhaft zu gewährleisten, müssen Unternehmen gem. Art. 32 Abs. 1 lit. d DSGVO die Wirksamkeit dieser Maßnahmen **regelmäßig überprüfen** und bewerten. Damit wird eine **konstante Aufrechterhaltung und Wartung der IT-Sicherheitsvorkehrungen** erforderlich. Die Mindestschutzanforderungen lassen sich wie folgt klassifizieren:[6]

1 Standard-Datenschutzmodell Version 2.0b vom 17.4.2020, abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/Download/SDM-Methode_V20b.pdf, zuletzt aufgerufen am 7.6.2021.

2 Zur Abdingbarkeit *HmbBfDI*, Vermerk: Abdingbarkeit von TOMs (Art. 32 DSGVO) vom 18.2.2021, abrufbar unter: https://datenschutz-hamburg.de/pages/abdingbarkeit-toms/, zuletzt aufgerufen am 10.6.2021; dagegen u.a. *Schwartmann/Hermann* in Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 10.5 Rz. 79.

3 *Mantz* in Sydow, DSGVO, Art. 32 Rz. 14 ff.

4 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.3.2 m.w.N.

5 ErwGr. 87 DSGVO; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.3.2.

6 *Müller* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, E. II.

202

Mindestschutzanforderungen gem. Art. 32 DSGVO		
Maßnahme	**Sicherheitsziel**	**Beispiele zur praktischen Umsetzung**
Zugangskontrolle	Nutzung der Daten durch Unbefugte technisch verhindern	– Personalisierte Nutzerkennungen – Passwörter und Richtlinien zum Umgang mit diesen – Verschlüsselung/Pseudonymisierung
Zutrittskontrolle	Nutzung der Daten durch Unbefugte physisch verhindern	– Wachpersonal – Abgeschlossene Serverräume – Zugangskarten, -schlüssel o.Ä. nur für Berechtigte
Zugriffskontrolle	Nutzung der Daten entsprechend der Berechtigungen gewährleisten	– Berechtigungskonzepte – Überprüfungen – Protokolle
Trennungskontrolle	Trennung der Daten entsprechend der verschiedenen Verarbeitungszwecke	– Archivierungskonzepte – Datenbanken – Nutzung getrennter Server
Weitergabekontrolle	Datenübermittlung nur an berechtigte Empfänger	– Data-Loss-Prevention-System – Datenverschlüsselung – Verbindungsverschlüsselung – Authentifizierungsverfahren – Digitale Signatur
Eingabekontrolle	Nachverfolgbarkeit etwaiger Datenveränderungen	– Nachvollziehbarkeit der Nutzereingaben durch Zeitstempel, Nutzernamen o.Ä. – Plausibilitätsprüfungen
Belastbarkeit	Robustheit der Datenverarbeitungssysteme gewährleisten	– Unterbrechungsfreie Stromversorgung – Virenschutz
Verfügbarkeitskontrolle	Sicherung der Daten gegen Zerstörung oder Verlust	– Notfallkonzept (s. Rz. 683 ff.) – Back-up-Systeme – Regelmäßige Datensicherungen – Redundanz – Gewährleistung der Aktualität/Qualität der Daten
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	Aufrechterhaltung der Sicherheitsmaßnahmen gewährleisten	– Datenschutz-Management – Interne Audits durch den Informationssicherheitsbeauftragten (s. Rz. 620 ff.) – Mitarbeiterbefragungen – Regelmäßige Datenschutzschulungen

203 Als **besonders effektive Schutzmaßnahme** stuft der Gesetzgeber die **Pseudonymisierung und Verschlüsselung** von Daten ein, Art. 32 Abs. 1 lit. a DSGVO.[1] Die Daten werden dabei so verändert, dass sie sich in Unkenntnis entsprechender Schlüssel oder ohne Hinzuziehung entfernter Kennungen bestimmten Personen nicht mehr zuordnen lassen. Auch wenn Unternehmen nicht in jedem Fall eine Pflicht zu einer entsprechenden Veränderung ihrer Datensätze trifft, sollten diese Maßnahmen ernsthaft in Betracht gezogen werden, um die datenschutzrechtlichen IT-Sicherheitspflichten wirksam einzuhalten – nicht zuletzt im Hinblick auf drohende Verletzungsfolgen bei Datenschutzverstößen (s. Rz. 232 ff.).[2]

204 Durch die über eine Pseudonymisierung bewirkte sichere Trennung von zu verarbeitenden Daten und Zusatzwissen, das die Identifizierung der betroffenen Person ermöglicht, hat diese eine risikominimierende Wirkung im Verarbeitungsprozess. Folge dessen ist, dass für die so bearbeiteten Daten entsprechend dem risikobasierten Ansatz der DSGVO weniger strenge anderweitige technisch-organisatorische Schutzmaßnahmen ergriffen werden müssen. Die Pseudonymisierung kann sich auch anderweitig positiv auswirken. So kann sie das Risikopotential von Datenschutzvorfällen senken, so dass ggf. eine Meldung nach Art. 33 DSGVO gar nicht erforderlich wird, weil das Risiko des Vorfalls als gering einzustufen sein kann.[3] Außerdem kann sich eine Pseudonymisierung bei der Verhängung von DSGVO-Bußgeldern positiv auf deren Höhe auswirken, da sie als präventive Maßnahme zum Schutz von Betroffenen zugunsten des Verantwortlichen zu werten wäre.[4]

205 **Praxishinweis zur erfolgreichen Datenverschlüsselung[5]:**
Eine Verschlüsselung von Daten bietet sich bei der Zugriffs-, der Zugangs- und/oder der Weitergabekontrolle an:
- Verschlüsselter **Zugang** zu personenbezogenen Daten;
- **Zugriff**: Verschlüsselung von Datenbanken, Ordnern oder Dateien mittels Verschlüsselungsprogrammen;
- verschlüsselter Übertragungsweg zur **Datenweitergabe**, z.B. via VPN.

c) Selbstregulierung und präventive Sicherheitsmaßnahmen

206 Besonders im Datenschutzrecht wird ein gewandelter regulatorischer IT-Sicherheitsansatz des Gesetzgebers augenfällig. So treten an die Stelle gesetzlicher Verbotsnormen zunehmend selbstregulatorische **Steuerungsmechanismen**, deren **Umsetzung präventiv** – also im Vorfeld der Datenverarbeitung – **durch** das **Unternehmen** erfolgt.[6]

1 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.3.2; s. auch *Degen/Emmert*, Elektronischer Rechtsverkehr, § 8 Rz. 112 ff.
2 S. dazu ausführlich *Voigt/von dem Bussche*, Handbuch DSGVO, Teile 2.1.2.2, 3.3.2.
3 *Schürmann*, DSB 2021, 49, 51.
4 Vgl. *Schürmann*, DSB 2021, 49, 51.
5 *Müller* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, E. II.2.
6 *Sydow* in Sydow, DSGVO, Einleitung Rz. 84 m.w.N.

aa) Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Die Sicherheit personenbezogener Daten soll technisch nicht nur während der Verarbeitung durch das Unternehmen sichergestellt werden, sondern bereits im Vorfeld der Verarbeitungstätigkeiten. Dieser präventive Schutzansatz beruht auf der Erkenntnis, dass die Bedingungen für sichere Datenverarbeitungen maßgeblich durch die dafür verwendete IT vorgegeben werden.[1] Er wird über die **unternehmerischen Pflichten** zu **Datenschutz durch Technikgestaltung („Data Protection by Design") und Datenschutz durch datenschutzfreundliche Voreinstellungen („Data Protection by Default")** nach Art. 25 DSGVO sichergestellt. Verantwortliche sind dazu verpflichtet, **technische Datenschutzkonzepte beim Aufsetzen neuer Verarbeitungsvorgänge umzusetzen**.[2] Die beiden Schutzkonzepte erfordern folgende Maßnahmen: 207

- **Datenschutz durch Technikgestaltung**: technische und organisatorische Maßnahmen werden bereits bei der Erarbeitung des Datenverarbeitungsvorgangs integriert. Bei der Entwicklung neuer Produkte sollte die Geschäftsleitung des jeweiligen Unternehmens bereits in einer frühen Phase des Projekts darauf hinarbeiten, Entwickler und Designer auf diese Verpflichtung aufmerksam zu machen;[3]

  Beispiele für Datenschutz durch Technikgestaltung[4]:
  - Entwicklung auf Datenminimierung ausgerichteter IT-Systeme;
  - Pseudonymisierung/Anonymisierung personenbezogener Daten bei ihrer Erfassung;
  - Ermöglichung der Erfüllung von Betroffenenrechten.

- **Datenschutz durch datenschutzfreundliche Voreinstellungen**: Werkseinstellungen werden datenschutzfreundlich vorgenommen. Dadurch werden nur solche Daten erhoben, die zur Erreichung des Verarbeitungszwecks zwingend benötigt werden. Durch Voreinstellungen lassen sich neben der Menge der erfassten Daten auch das Ausmaß ihrer Verarbeitung und Speicherdauer begrenzen.[5]

Die Pflichten werden durch den **Stand der Technik** sowie durch die notwendigen Implementierungskosten begrenzt.[6] Unternehmen sollten in jedem Fall ihre Bemühungen erhöhen, datenschutzfreundliche Produkte zu entwickeln und bei der Verarbeitung personenbezogener Daten möglichst datensparsam vorzugehen. Während sich Datenschutz durch Technikgestaltung nur im Entwicklungsprozess vor der Datenverarbeitung umsetzen lässt, können die Werkseinstellungen von Produkten oder Voreinstellungen von Diensten auch nachträglich eine Anpassung erfahren. Insofern dürfte der Implementierungsaufwand zur Umsetzung von Datenschutz durch datenschutzfreundliche Voreinstellungen regelmäßig geringer ausfallen. 208

1 *Conrad/Hausen* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 36 Rz. 210 ff.
2 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.7 m.w.N.
3 *Gierschmann*, ZD 2016, 51, 53.
4 ErwGr. 78 DSGVO; *Wybitul/Draf*, BB 2016, 2101, 2104.
5 *Gierschmann*, ZD 2016, 51, 53; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.7.
6 *Gausling/Baumgartner*, ZD 2017, 308, 310 f.

bb) Zertifizierungen und Verhaltensregeln

209 Der selbstregulatorische Datenschutzansatz wird auch durch die steigende Bedeutung von Verhaltensregeln, Siegeln und **Zertifizierungen** nach der DSGVO verdeutlicht. Entsprechende Instrumente können von Unternehmen nicht nur genutzt werden, um gegenüber ihren Kunden und Geschäftspartnern mit einem bestimmten Datensicherheitsstandard aufzutreten, sondern können auch den **Nachweis der Einhaltung von IT-Sicherheitspflichten** auf unterschiedliche Art und Weise erleichtern.[1] **Verhaltensregeln** präzisieren die technischen und organisatorischen Datenschutzanforderungen der DSGVO für eine bestimmte Verarbeitungssituation, ein bestimmtes Produkt oder einen bestimmten Sektor.[2] Dadurch ermöglichen sie Unternehmen eine Selbsteinschätzung, ob und inwieweit ihre Tätigkeiten mit dem Datenschutzrecht in Einklang stehen, etwa ob angemessene technische und organisatorische Maßnahmen getroffen wurden.[3] Im Gegensatz dazu konkretisieren **Zertifizierungen** die gesetzlichen Anforderungen nicht, sondern dienen vielmehr dem Nachweis der Vereinbarkeit der durchgeführten Verarbeitungstätigkeiten mit der DSGVO, bspw. gegenüber den Aufsichtsbehörden.[4] So könnten Unternehmen ihre technischen und organisatorischen Maßnahmen zertifizieren lassen, um die Einhaltung datenschutzrechtlicher IT-Sicherheitsstandards nachzuweisen. In Deutschland obliegt die Genehmigung und Überwachung der Einhaltung von Verhaltensregeln grundsätzlich den **Datenschutzaufsichtsbehörden**. Die Entwicklung von Zertifizierungen erfolgt gem. § 39 BDSG durch die **Deutsche Akkreditierungsstelle** in Kooperation mit den Aufsichtsbehörden. Bei Verfügbarkeit entsprechender Instrumente sollte deren Verwendung jedenfalls ernsthaft in Betracht gezogen werden. So können Unternehmen mit entsprechenden **Zertifizierungen** nach außen einen Sorgfalts- und Leistungsnachweis erbringen, über den vertragliche wie deliktische **Haftungsrisiken** zu einem bestimmten Grad **gesteuert werden** können (s. Rz. 550 ff.). Insbesondere bei der Verhängung von Bußgeldern kann die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder genehmigten Zertifizierungsverfahren nach Art. 42 DSGVO als mildernder Faktor berücksichtigt werden, Art. 83 Abs. 2 Satz 2 lit. j DSGVO.[5]

d) Schrems II

210 Werden personenbezogene Daten in Drittländer außerhalb des Europäischen Wirtschaftsraums übermittelt, so ist dies gem. Kapitel V der DSGVO im Regelfall nur zulässig, wenn für die Behandlung der Daten im Drittland ein angemessenes Datenschutzniveau gewährleistet wird.[6] Mit Urteil vom 16. Juli 2020[7] entschied der EuGH,

1 *Gühr/Karper/Maseberg*, DuD 2020, 649, 650; *Laue* in Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 8 Rz. 1; *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.9.1.
2 *von Braunmühl/Wittmann* in Plath, BDSG/DSGVO, Art. 40 Rz. 8.
3 *Voigt/von dem Bussche*, Handbuch DSGVO, Teil 3.9.1.
4 *Bergt*, DSRITB 2016, 483, 496.
5 *Maier/Pawlowska/Lins/Sunyaev*, ZD 2020, 445, 446.
6 Vgl. *Pauly* in Paal/Pauly, DS-GVO, Art. 44 Rz. 1 f.
7 EuGH, Urt. v. 16.7.2020 – C-311/18 – Schrems II, CR 2020, 529.