1 Einführung in die Datenschutz-Grundverordnung (DS-GVO)[1]

1.1 Die Ausgangslage

Die EU-Verordnung 2016/79 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DS-GVO)“ ist nach Veröffentlichung im Amtsblatt der EU am 04.05.2016 am 25.05.2016 in Kraft getreten und wird ab dem 25.05.2018 (Art. 99) Geltung haben.

Grundlage für die einheitliche Gestaltung des Datenschutzrechts in der EU ist bis dahin noch die EG-Datenschutzrichtlinie vom 24.10.1995. Eine Richtlinie ist mit dem Ziel der Harmonisierung der geregelten Rechtsmaterie ausschließlich an die Mitgliedstaaten gerichtet und von diesen in nationales Recht umzusetzen, was sodann u.a. im Bundesdatenschutzgesetz (BDSG) geschah. Der speziell unter dem Gesichtspunkt der Schaffung einheitlicher Wirtschaftsbedingungen und der Wettbewerbsgleichheit bedeutsame Harmonisierungseffekt wird aber nur erreicht, wenn die Nationalstaaten sich an die ihnen gewährten Spielräume halten. Dies war in der Praxis nicht hinreichend geschehen. Auf Grund dieser Erkenntnis wird der Datenschutz in der EU nunmehr in einer Verordnung geregelt. Im Gegensatz zu Richtlinien sind Verordnungen allgemein und unmittelbar geltende und in allen ihren Teilen verbindliche Rechtsakte. Gemäß ihrer „Durchgriffswirkung“ müssen sie von den EU-Mitgliedstaaten nicht in nationales Recht umgesetzt werden (Art. 288 Abs. 2 AEUV).

Andererseits kann eine Verordnung durch „Öffnungsklauseln“ auch weiterhin Regulierungen im nationalen Recht gestatten bzw. nationale Gestaltungsspielräume eröffnen. Dies geschieht in der DS-GVO in gewichtiger Zahl. Einige Öffnungsklauseln geben den Mitgliedstaaten einen Handlungsauftrag; andere – und das ist die Mehrzahl – eröffnen einen in das Ermessen der Staaten gestellten Handlungsspielraum. Je nach Zählweise kann man 50 bis 60 Öffnungsklauseln feststellen. Im Ergebnis wird sich ab 2018 die europäische Datenschutzlandschaft auch weiterhin komplex und unübersichtlich darstellen.

1.2 Neuregelungen des Datenschutzes durch die DS-GVO

1.2.1 Allgemeines

Aufbauend auf den bewährten Prinzipien der EU-Datenschutzrichtlinie werden zahlreiche Themen angegangen, die z.B. auch Gegenstand der von den Aufsichtsbehör-

1. Ursprünglich erschienen in Müthlein (Hrsg.), Datenschutz-Grundverordnung – zweisprachige Textausgabe Englisch-Deutsch, 2. Auflage 2017, Peter Gola: Einführung in die Datenschutz-Grundverordnung (DS-GVO)

den vorgelegten Eckpunkte eines „modernen Datenschutzrechts“ sind. Dazu gehören die Neuformulierung der Schutzrichtung, der technikneutrale Ansatz, erweiterte Transparenzverpflichtungen oder der besondere Schutz Minderjähriger. Weitere aktuelle Forderungen der Fortschreibung des Datenschutzrechts finden ihren Niederschlag in der Regelung der „privacy by design and by default“ (Art. 25), der Datenübertragbarkeit (Art. 20) und der speziellen Ausgestaltung der Löschung in Form des „Rechts auf Vergessenwerden“ (Art. 17 Abs. 2).

Basis der Verordnung sind die in Art. 5 für die Verarbeitung personenbezogener Daten aufgestellten Grundsätze. Dazu gehören das Prinzip der Rechtmäßigkeit, der Richtigkeit, die Grundsätze von Treu und Glauben und der Transparenz, der Zweckbindung, der Daten- und Speicherminimierung, der Integrität und Vertraulichkeit und der Accountability.

Die Praxis mit Mehraufwand belasten wird nicht nur die Umsetzung der die obigen Grundsätze konkretisierenden Artikel, sondern auch die umfangreichen Dokumentationsaufwendungen, die das Unternehmen hinsichtlich des Nachweises seiner diesbezüglichen Verpflichtungen zu erfüllen hat.

1.2.2 Geltungsbereich

1.2.2.1 Sachlicher Anwendungsbereich

Nach Art. 2 Abs. 1 findet die Verordnung Anwendung auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

1.2.2.1.1 Personenbezogene Daten

Mit einem personenbezogenen Datum wird weiterhin jede Art von Informationen über eine bestimmte oder bestimmbare natürliche, d.h. „betroffene“ Person gemeint (Art. 4 Nr. 1). Identifizierbar ist jemand, wenn er direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck seiner Identität sind, von dem Verantwortlichen oder einer anderen Person ermittelbar ist. Daten, die erst durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, gelten als personenbezogen, wenn dem Verantwortlichen oder anderen Personen zu deren Erlangung nach allgemeinem Ermessen finanzielle und technische Mittel zur Verfügung stehen. Insoweit unterscheiden sich weiterhin pseudonymisierte Daten von anonymen bzw. anonymisierten Informationen, bei denen die betroffene Person nicht oder nicht mehr identifiziert werden kann. Weiterhin nicht eindeutig beantwortet bleibt die Frage nach der Relativität des Personenbezugs, d.h. ob Daten für den einen, der Zugang zu dem Zusatzwissen hat, als pseudonym und für andere, bei denen das nicht der Fall ist, als anonym gelten.

1.2.2.1.2 Die Verarbeitung

Als „Verarbeitung“ wird sodann jeder mit oder ohne Hilfe automatisierter Verfahren stattfindende Umgang mit personenbezogenen Daten, beginnend mit dem Erheben und endend mit dem Löschen oder Vernichten (Art. 4 Nr. 2), definiert. Trotz des in Art. 4 erheblich erweiterten Begriffskatalogs werden die bisherigen „klassischen“ Erscheinungsformen der Verarbeitung des § 3 Abs. 3 bis 7 BDSG nicht mehr definiert, obwohl sie, wie z.B. das Übermitteln oder das Löschen, gesondert geregelt werden. Eine Ausnahme bildet das „Sperren“ von Daten, das nunmehr als „Recht auf Einschränkung der Verarbeitung“ firmiert (Art. 4 Nr. 3).

1.2.2.1.3 Automatisiertes/dateigebundenes Verfahren

Auch die Verordnung gilt „erst“ bei einer ganz oder teilweise automatisierten Verarbeitung der Daten oder wenn ihre Speicherung in einem Dateisystem (Art. 2 Abs. 1) erfolgt, worunter eine in Art. 4 Nr. 6 definierte manuelle Verarbeitung in einem strukturierten Ablagesystem zu verstehen ist. Erfasst wird also auch die mündliche Befragung von Bewerbern, vorausgesetzt, das Ergebnis wird zumindest dateimäßig notiert. Die klassische, unstrukturierte Akte fällt nicht unter die Verordnung.

1.2.2.2 Räumlicher Anwendungsbereich

1.2.2.2.1 In der EU ansässige Verantwortliche

Die DS-GVO zu beachten hat jeder, der – unabhängig von dem Ort, an dem die Verarbeitung erfolgt – von einer Niederlassung in der Union aus agiert (Art. 3 Abs. 1). Wenn der Betroffene seinen Arbeitsplatz bzw. Aufenthaltsort in einem Drittland hat oder ausländischer Staatsangehöriger ist, ändert das an seinen datenschutzrechtlichen Positionen nichts (ErwG 14).

1.2.2.2.2 Außerhalb der EU ansässige Verantwortliche

Auch Verarbeitungen eines nicht in der Union Niedergelassenen bzw. von hier aus Agierenden werden u.a. erfasst, wenn die Datenverarbeitung dazu dient, das Verhalten von Personen in der EU zu beobachten oder ihnen Dienstleistungen anzubieten (Art. 3 Abs. 2 Lit. b). Die Norm stellt – ebenso wie Art. 37 Abs. 1 Lit. b hinsichtlich der diesbezüglichen Bestellpflicht eines Datenschutzbeauftragten – ab auf die Beobachtung und Auswertung von Internetaktivitäten (ErwG 24) und die Erstellung von Kundenprofilen. Gleichwohl ist nicht erkennbar, weshalb sie bei Beschäftigtendatenverarbeitung nicht anwendbar sein sollte. Eine dauernde Auswertung von Leistungs- und Verhaltensdaten und ein das Mitarbeiterverhalten bewertendes Human-Resource-System eines im Drittland ansässigen internationalen Konzerns erfüllt den Tatbestand daher ebenfalls.

1.2.3 Normadressaten

1.2.3.1 Der „Verantwortliche“ für den Datenschutz

Normadressat, der nunmehr als der „ Verantwortliche“ bezeichnet wird (Art. 4 Nr. 7), ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, wobei z.B. innerhalb eines Unternehmensverbunds auch mehrere als gemeinsam Verantwortliche kooperieren können (Art. 26).

1.2.3.2 Auftragsverarbeiter

Unmittelbar mit Pflichten belegt werden nunmehr auch als „Auftragsverarbeiter“ bezeichnete Stellen, d.h. Stellen, die personenbezogene Daten weisungsgebunden für den Verantwortlichen verarbeiten (Art. 3 Nr. 8). Der Auftragnehmer wird nicht mehr zum „Dritten“, wenn er seinen Sitz im Drittland hat (Art. 4 Nr. 10). Neu ist, dass die Einhaltung der Pflichten des Auftragnehmers zur Einhaltung der erforderlichen technisch- organisatorischen Maßnahmen durch Anwendung von Verhaltensregelungen nach Art. 40 (Code of Conduct) oder eine Zertifizierung nach Art. 42 nachgewiesen werden kann (Art. 28 Abs. 5). Setzt sich der Auftragnehmer über die ihm gegebenen Weisungen hinsichtlich der Bindung an die Zwecke und Mittel der Datenverarbeitung hinweg, ist er für diese unautorisierte Verarbeitung nunmehr als Verantwortlicher in Rechenschaft zu ziehen (Art. 28 Abs. 10). Neu ist ferner, dass der Auftragsverarbeiter ggf. gemeinsam mit seinem Auftraggeber dem Beschäftigten gegenüber für einen bei ihnen infolge rechtswidriger Datenverarbeitung eingetretenen materiellen und immateriellen Schaden haften muss (Art. 82 Abs. 1).

1.2.3.3 Die bei der Datenverarbeitung Beschäftigten/ Datengeheimnis

Die DS-GVO wendet sich in Art. 29 auch an Personen, die dem Verantwortlichen oder seinen Auftragsverarbeitern unterstellt sind und Zugang zu personenbezogenen Daten haben, und auch an den Auftragsverarbeiter selbst und gibt ihnen vor, personenbezogene Daten grundsätzlich nur auf Anweisung des für die Verarbeitung Verantwortlichen zu verarbeiten. Die Bestimmung entspricht den § 5 S. 1 und § 11 Abs. 3 S. 1 BDSG. Eine Pflicht privater Arbeitgeber, die Beschäftigten bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten, besteht nunmehr nur indirekt, indem Auftragsverarbeiter sicherzustellen haben, dass die von ihnen zur Verarbeitung personenbezogener Daten autorisierten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Lit. b).

1.2.3.4 Datenschutzbeauftragter

Gesetzliche Pflichten werden auch dem nunmehr für alle Mitgliedstaaten eingeführten Datenschutzbeauftragten zugewiesen (Art. 37 ff.). Die DS-GVO sieht eine

Bestellpflicht jedoch nur für solche privaten Stellen vor, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche eine regelmäßige und systematische Beobachtung von betroffenen Personen in großem Umfang erforderlich machen oder die Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 Abs. 1 im großem Umfang oder von Daten zu strafrechtlichen Verurteilungen und Straftaten im Sinne des Art. 9 zum Gegenstand haben. Die Frage, ab wann eine Überwachung von Beschäftigten den Tatbestand erfüllt, kann für deutsche Arbeitgeber ggf. dahinstehen, wenn der deutsche Gesetzgeber gemäß der Öffnungsklausel in Art. 37 Abs. 4 S. 1 für die Bestellpflicht an den bislang geltenden Bestimmungen des § 4f Abs. 1 BDSG festhält. Die Aufgabenstellung des Datenschutzbeauftragten hat nunmehr verstärkt Compliance- und Überwachungsfunktionen, woraus sich die Frage nach seiner Garantenfunktion im straf- und ordnungswidrigkeitsrechtlichen Sinne ergibt.

1.2.3.5 Die Aufsichtsbehörden

Umfangreiche Neuregelungen zur Kompetenz und insbesondere zur Zusammenarbeit der Aufsichtsbehörden der Mitgliedstaaten sollen eine EU-weite einheitlichere Aufsichtspraxis und effektive Rechtsdurchsetzung der Datenschutzbehörden im Binnenmarkt bewirken. Ein mit weitreichenden Kompetenzen ausgestatteter Europäischer Datenschutzausschuss (Art. 68 ff.), bestehend aus Vertretern der nationalen Aufsichtsbehörden, soll die einheitliche Anwendung des Datenschutzrechts sicherstellen. Parallel dazu soll der sog. „One-Stop-Shop"-Ansatz Betroffenen und verantwortlichen Unternehmen die Interaktion mit der Datenschutzaufsicht erleichtern, indem eine zentrale Behördenzuständigkeit begründet wird. Gleichzeitig wird damit gewährleistet, dass sich der Betroffene immer an die für seinen Wohnsitz oder Arbeitsplatz zuständige Behörde wenden kann (Art. 77). Bei mehreren Zuständigkeiten wird im sog. Kohärenzverfahren eine einheitliche Anwendung der Verordnung sichergestellt. Um der Notwendigkeit einer praktischen Umsetzung der Datenschutzvorschriften Nachdruck zu verleihen, sieht die DS-GVO empfindliche Sanktionen vor. Die Bußgelder werden drastisch erhöht. Bisher betrug das maximale Bußgeld 300.000 Euro. Nunmehr können gegenüber Unternehmen Bußgelder bis zu 20 Mio. Euro oder, z.B. bei einer Verletzung von wesentlichen Grundprinzipien, bspw. in Bezug auf Einwilligungen, Betroffenenrechte oder die Regeln für die internationale Datenübermittlung, bis zu vier Prozent des weltweiten Jahresumsatzes verhängt werden. Vermehrt wurden auch die Bußgeldtatbestände, so dass kaum noch eine Missachtung von Vorschriften der DS-GVO sanktionsfrei bleibt (siehe Art. 83 Abs. 2).

1.2.4 Zulässigkeit der Verarbeitung

1.2.4.1 Verbot mit Erlaubnisvorbehalt

Grundprinzip der DS-GVO bleibt, dass die Verarbeitung personenbezogener Daten unter einem Verbot mit Erlaubnisvorbehalt steht, d.h. jede Form der Verarbeitung ist weiterhin nur zulässig, wenn der Betroffene eingewilligt hat oder die Verordnung selbst die Einwilligung erteilt. Die Erlaubnisnormen der Verordnung, die dem Daten-

verarbeiter Datenverarbeitungen auch ohne oder sogar gegen den Willen des Beschäftigten gestatten, geben die Art. 6 und 7 wieder.

1.2.4.2 Die Einwilligung

Art. 6 Abs. 1 Lit. a nennt die Einwilligung an erster Stelle als Erlaubnistatbestand. Gemäß Art. 4 Nr. 11 muss sie freiwillig („freely given“) erteilt werden. In ErwG 43 wird dazu allgemein ausgeführt, dass eine Einwilligung dann keine Rechtsgrundlage für die Datenverarbeitung darstellt, wenn ein klares Ungleichgewicht zwischen dem Betroffenen und dem für die Verarbeitung Verantwortlichen besteht. Nicht unterstellt wird, wie ein erster Kommissionsvorschlag es noch vorsah, dass im Arbeitsverhältnis ein solches Einwilligungen generell ausschließendes Ungleichgewicht bestehe. Nach ErwG 42 S. 5 sollte auch nur dann davon ausgegangen werden, dass der Beschäftigte die Einwilligung freiwillig abgibt, wenn er eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Andererseits lässt aber ErwG 43 S. 2 die Einholung der Einwilligung als „conditio sine qua non“ zu, wenn die Einwilligung für die Erfüllung eines Vertrags erforderlich ist.

Verlangt wird eine konkrete, informierte Erklärung (Art. 4 Nr. 11), so dass pauschale oder globale Einwilligungen für den Umgang mit personenbezogenen Daten nicht wirksam sind.

Nach Art. 7 Abs. 3 kann die Einwilligung jederzeit widerrufen werden. Auch dies entspricht bereits der geltenden Rechtslage. Nicht als rechtsmissbräuchlich sieht es die Verordnung offensichtlich an, wenn der Beschäftigte bei Einholung einer im Endeffekt belanglosen Einwilligung über sein vermeintliches Selbstbestimmungsrecht getäuscht wird, weil die Verordnung dem Verantwortlichen erlaubt, sich nunmehr trotz Widerruf ggf. auf eine andere Erlaubnisnorm für die Verarbeitung zu berufen.

1.2.4.3 Sich aus einer vertraglichen Beziehung ergebende Zweckbestimmung

Die Verordnung gibt die Erlaubnis für die Verarbeitung – wie bisher § 28 Abs. 1 Abs. 1 S. 1 Nr. 1 BDSG – für Zwecke, die sich aus einem mit dem Betroffenen abgeschlossenen Vertrag bzw. einer vorvertraglichen Beziehung ergeben (Art. 6 Abs. 1 Lit. b), d.h. ein – potenzieller – Vertragspartner darf die Daten verarbeiten, die erforderlich sind für die Begründung, Durchführung und Beendigung der in Betracht kommenden vertraglichen Beziehung.

1.2.4.4 Die Interessenabwägung

Handelt es sich um außerhalb vertraglicher Beziehungen benötigte Daten, kann auf die Interessenabwägungsklausel des Art. 6 Abs. 1 Lit. f zurückgegriffen werden. Danach kann die Rechtmäßigkeit der Verarbeitung durch die berechtigten Interessen des Verantwortlichen oder auch eines Dritten begründet sein. Bei der gebotenen Interessenabwägung sind die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen, die sich u.a. daraus ergeben können, dass sie in den Diensten des

Verantwortlichen steht oder dessen Kunde ist (ErwG 47 S. 2). Trotz der etwas von dem Text des § 28 Abs. 1 S. 1 Nr. 2 BDSG abweichenden Formulierung der Verordnung werden sich im Abwägungsergebnis in der Regel keine Unterschiede ergeben.

Nach ErwG 48 sollen Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ggf. ein berechtigtes Interesse haben, personenbezogene Daten von Mitarbeitern innerhalb der Unternehmensgruppe für interne Verwaltungszwecke zu übermitteln. Gemäß Art. 4 Nr. 19 und ErwG. 37 versteht man unter einer „Unternehmensgruppe“ ein herrschendes und von diesem abhängige Unternehmen. Ein zentrales Unternehmen, das die Verarbeitung personenbezogener Daten in angeschlossenen Unternehmen kontrolliert, bildet mit diesen eine Einheit, die ebenfalls als Unternehmensgruppe behandelt werden kann. Die DS-GVO enthält damit zwar kein Konzernprivileg, macht aber doch deutlich, dass spezielle Konzerninteressen in der Abwägung mit den schutzwürdigen Interessen der Beschäftigten im Rahmen des Art. 6 Abs. 2 Lit. f oder auch bei der Gestaltung von Betriebsvereinbarungen ein besonderes Gewicht haben können.

1.2.4.5 Erfüllung gesetzlicher Vorgaben

Eine Verarbeitung ist zwangsläufig auch dann gestattet, wenn sie für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist, die sich aus dem EU-Recht oder Datenschutzgrundsätzen genügendem Recht eines Mitgliedstaats ergibt (Art. 6 Abs. 2 Lit. c), oder wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung einer dem für die Verarbeitung Verantwortlichen übertragenen hoheitlichen Gewalt erfolgt (Art. 6 Abs. 2 Lit. e). Damit ist z.B. die Zulässigkeit der Verarbeitung der auf Grund gesetzlicher Vorgaben in einem Gehaltsabrechnungsprogramm erforderlichen Daten durchweg gerechtfertigt.

1.2.4.6 Sensible Daten

Besondere, dem Art. 6 DS-GVO vorrangige Zulässigkeitsregelungen (Art. 9 Abs. 2) gelten für die in Art. 9 Abs. 1 benannten besonderen Kategorien personenbezogener Daten. Ergänzend zu den bereits in § 3 Abs. 9 BDSG genannten zählen hierzu die Gewerkschaftszugehörigkeit und der eindeutigen Identifizierung einer Person dienende genetische und biometrische Daten, die in Art. 4 Nr. 13 und 14 definiert werden.

Die eigentliche Besonderheit liegt darin, dass die Erlaubnistatbestände des Art. 9 Abs. 2 strengere Voraussetzungen beinhalten als Art. 6. Andererseits erlaubt Art. 9 Abs. 2 Lit. b ausdrücklich die Verarbeitung, wenn sie erforderlich ist, damit der Arbeitgeber oder der Beschäftigte den ihm aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechten bzw. Pflichten nachkommen bzw. diese erhalten kann.

Schließlich enthält Art. 9 Abs. 5 eine Öffnungsklausel, nach der die Mitgliedstaaten weitere Bestimmungen, einschließlich Beschränkungen, zur Verarbeitung genetischer, biometrischer Daten und Gesundheitsdaten beibehalten oder einführen können.

1.2.4.7 Strafurteile und Straftaten

Nach Art. 10 darf die Verarbeitung von Daten über Strafurteile und Straftaten nur erfolgen, wenn diese nach dem Recht des Mitgliedstaats unter angemessenen Garantien für die Rechte der betroffenen Person zulässig ist. Auszugehen ist davon, dass nunmehr eine konkrete bereichsspezifische Regelung für die Erhebung von Vorstrafen beim Bewerber oder Mitarbeiter benötigt wird. Polizeiliche Führungszeugnisse können nur dann verlangt werden, wenn das Gesetz es ausdrücklich vorsieht, wie es für sog. besondere polizeiliche Führungszeugnisse der Fall ist (§ 30a BZRG).

1.2.4.8 Daten aus öffentlichen Quellen

Eine Privilegierung der Verarbeitung von allgemein zugänglichen Daten, wie sie § 28 Abs. 1 S. 1 Nr. 3 oder § 29 Abs. 1 S. 1 Nr. 2 BDSG kennt, enthält die DS-GVO erstaunlicherweise nur für die Verarbeitung besonderer Arten personenbezogener Daten, die die betroffene Person offenkundig öffentlich gemacht hat (Art. 9 Abs. 2 Lit. e). Die insoweit erleichterte Erlaubnis wird aber auch ansonsten bei Anwendung der Interessenabwägungsklausel des Art. 6 Abs. 2 Lit. f zugunsten des Arbeitgebers herangezogen werden können. Damit bleibt ein Googeln von Bewerberdaten weiterhin in den bisherigen Grenzen zulässig, wobei nunmehr jedoch die Transparenzregelung des Art. 14 zu beachten ist.

1.2.4.9 Automatisierte Einzelentscheidungen und Profiling

Art. 21 und Art. 22 regeln die Zu- bzw. Unzulässigkeit einer automatisierten Einzelentscheidung eines dieser Entscheidung ggf. zugrundeliegenden Profilings. Nach der Definition in Art. 4 Nr. 4 bezeichnet der Begriff des „Profilings“ jede Art der automatisierten Verarbeitung persönlicher Aspekte zur Bewertung einer Person, wobei es insbesondere um die Analyse ihrer Arbeitsleistung, wirtschaftlichen Lage, Gesundheit, persönlichen Vorlieben oder Interessen, ihrer Zuverlässigkeit oder ihres Verhaltens, ihres Aufenthaltsorts oder von Ortswechseln gehen kann.

Nach Art. 22 Abs. 1 ist es grundsätzlich untersagt, den Betroffenen einer allein, ggf. auf einem Profiling beruhenden, ihn beeinträchtigenden automatisierten Entscheidung zu unterwerfen. Eine Ausnahme gilt u.a., wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages erfolgt und dem Betroffenen z.B. ein Recht auf ein persönliches Eingreifen oder zur Darlegung des eigenen Standpunkts eingeräumt ist. Dies entspricht der Regelung in § 6a Abs. 2 BDSG.

Zu beachten ist zudem das gegenüber einem Profiling nach Art. 21 Abs. 1 bestehende Widerspruchsrecht, auf das der Bewerber/Beschäftigte spätestens zum Zeitpunkt der ersten Kommunikation mit ihm ausdrücklich und in einer verständlichen und von anderen Informationen getrennten Form hingewiesen werden muss (Art. 21 Abs. 4).

1.2.4.10 Zweckänderung/Big Data

In den Beratungen um die DS-GVO war lange strittig, unter welchen Umständen für einen bestimmten Zweck erhobene Daten auch nachträglich für andere, d.h. dem Betroffenen nicht mitgeteilte Zwecke verwendet werden dürfen. Art. 6 Abs. 4 erlaubt die Verarbeitung für einen anderen Zweck als den, für den die Daten erhoben wurden, sofern der Betroffene zustimmt, eine einzelstaatliche Erlaubnisregelung besteht oder eine Reihe die Schutzinteressen des Betroffenen betonender Bedingungen erfüllt sind. Hierzu zählen die Verbindung zwischen den Zwecken, die Art der Daten oder mögliche Konsequenzen für den Betroffenen oder durch z.B. Pseudonymisierung oder Verschlüsselung getroffene Sicherheitsmaßnahmen. Dies zeigt ggf. einen Weg zu Big-Data-Anwendungen.

1.2.4.11 Entfallene Vorschriften

Eine nicht unwesentliche Zahl von Zulässigkeitsregelungen des BDSG taucht in der DS-GVO nicht mehr auf. Dazu zählen die Vorschriften über die Videoüberwachung in § 6b BDSG und zum Einsatz sog. mobiler personenbezogener Speicher- und Verarbeitungsmedien in § 6c BDSG. Nicht mehr geregelt sind automatisierte Abrufverfahren (Art. 10 BDSG). Da die DS-GVO nicht mehr trennt zwischen Stellen, die Daten für eigene Zwecke (§ 28 BDSG) oder geschäftsmäßig zur Übermittlung in personenbezogener (§ 29 BDSG) bzw. anonymisierter Form (§ 30 BDSG) und in der Markt- und Meinungsforschung (§ 30a BDSG) verarbeiten, sind auch die für die letztgenannten drei Bereiche bestehenden Sonderregelungen entfallen.

Weggefallen sind auch einige Zweckbindungsgebote, so u.a. die Regelung des § 6 Abs. 2 BDSG oder die des § 31 BDSG. Ob Daten, die bei einer datenschutzrechtlich bedingten Zugangskontrolle anfallen, auch zur Arbeitszeitkontrolle genutzt werden dürfen, entscheidet sich nun nach Art. 6 Abs. 1 Lit. b bzw. Abs. 4.

1.2.5 Transparenzpflichten

1.2.5.1 Vorbemerkung

Nicht mehr Gesetzestext ist der bislang in § 4 Abs. 3 BDSG geregelte Grundsatz der Direkterhebung. Gleichwohl wird dieser auf Grund des für die Verarbeitung geltenden Grundsatzes von Treu und Glauben (Art. 5 Lit. a) doch weiterhin gelten, weil es ihm entspricht, Daten, die beim Betroffenen erhoben werden können, nicht hinter seinem Rücken anderweitig zu beschaffen. Die Transparenz der Datenverarbeitung wird jedoch durch umfassende, die derzeitigen Informationspflichten der §§ 4 Abs. 3 und 33 BDSG erheblich erweiternde Regelungen in Art. 13 und 14 sichergestellt, wobei die Mitteilungspflichten einmal die konkrete Verarbeitungssituation der Daten des Beschäftigten und zum anderen allgemeine, grundsätzliche Belehrungen über seine Rechtspositionen enthalten.

1.2.5.2 Unabdingbarkeit

Nach § 6 BDSG konnten die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Auch ohne dass diese Rechte benannt wurden, wurde diese Unabdingbarkeit auch für weitere Rechtspositionen der betroffenen Person bejaht; so z.B. für das Recht auf Benachrichtigung, das allgemeine Widerspruchsrecht oder auch die Möglichkeit, sich an die Aufsichtsbehörden zu wenden. Hierbei bleibt es auch bei der DS-GVO, die insoweit als zwingendes Gesetz zu verstehen ist und individuelle Abweichungen nur dort erlaubt, wo sie eine diesbezügliche Einwilligung des Betroffenen zulässt.

1.2.5.3 Datenerhebung bei der betroffenen Person

Bei der Datenerhebung beim Bewerber bzw. Beschäftigten ist nunmehr auch über die Dauer der Speicherung der Daten bzw. die Kriterien für ihre Löschung oder die einschlägigen Auskunfts- und Korrekturrechte nebst dem Beschwerderecht bei der Aufsichtsbehörde zu informieren (Art. 13). Neben den Kontaktdaten des oder der für die Verarbeitung Verantwortlichen sind auch die des ggf. zu benennenden Datenschutzbeauftragten mitzuteilen.

Sollen die Daten zu einer automatisierten Einzelentscheidung und zum Profiling verwendet werden, sind ggf. Angaben über die verwendete Logik sowie ihre Auswirkungen zu machen.

Die Informationspflicht entfällt, wenn der Betroffene bereits über die Information „verfügt“ (Art. 13 Abs. 4).

1.2.5.4 Nicht bei der betroffenen Person stattfindende Datenerhebung

Die Benachrichtigungspflicht hinsichtlich der Speicherung von ohne Kenntnis des Betroffenen erhobenen Daten entsteht nach § 33 Abs. 1 S. 1 BDSG bei erstmaliger Speicherung personenbezogener Daten des Betroffenen. Sind über den beschäftigten Betroffenen bereits Daten gespeichert und werden ohne seine Kenntnis erhobene weitere Daten hinzugespeichert, so verneinte die wohl h.M. bislang eine Benachrichtigungspflicht. Diese Einschränkung auf die erstmalige Grundinformation sieht der die Informationspflicht über nicht bei der betroffenen Person erhobene Daten regelnde Art. 14 nicht vor. Die Transparenz gegenüber dem Betroffenen ist bei jeder Datenerhebung herzustellen. Ihr Inhalt entspricht grundsätzlich dem des Art. 13, wobei hier zusätzlich die Quelle der Daten offenzulegen ist. Für die Mitteilung gilt eine Maximalfrist von einem Monat, es sei denn, die Daten werden vorher zur Kommunikation mit dem Betroffen verwendet oder an Dritte weitergegeben (Art. 14 Abs. 3). Werden also über den Bewerber im Internet oder bei Dritten sog. Background Checks durchgeführt, so ist der Bewerber zu informieren und ihm bei Geltendmachung des Auskunftsrechts auch das konkrete Ergebnis mitzuteilen; vorausgesetzt, die Daten werden automatisiert oder dateigebunden verarbeitet.

1.2.5.5 Vorherige Information über zweckändernde Verwendungen

Sollen Daten nach Art. 6 Abs. 4 für einen anderen Zweck weiterverarbeitet werden als den, für den sie erhoben wurden, so besteht eine vor der Weiterverarbeitung zu erfüllende Benachrichtigungspflicht (Art. 13 Abs. 3 bzw. Art. 14 Abs. 4). Die umfassende Erfüllung dieser Informationspflicht und das dem Betroffenen offenzulegende Widerspruchsrecht werden Big-Data-Analysen zweifelsohne einschränken.

1.2.5.6 Meldung bei „Datenpannen“

Die Meldepflicht des § 42a BDSG hat ihre Parallelregelung in zwei Artikeln der Verordnung gefunden. Art. 33 enthält die Voraussetzungen zur Pflicht zur Mitteilung „von Verletzungen des Schutzes personenbezogener Daten“ an die Aufsichtsbehörde und Art. 34 zur Benachrichtigung der betroffenen Person. Die Informationspflicht setzt voraus, dass die in jeglichem Rechtsverstoß liegende DS-GVO-Verletzung voraussichtlich zu einem Risiko bzw. zu einem hohen Risiko (so für die Benachrichtigungspflicht gegenüber der betroffenen Person) für die persönlichen Rechte und Freiheiten der betroffenen Person führt. In der diesbezüglichen Bewertung steht der Verantwortliche zunächst allein da, was im Hinblick auf die bei einer Verletzung der Mitteilungspflicht anstehenden gravierenden Bußgelddrohung wohl zu zunehmender Beschäftigung der Aufsichtsbehörde führen wird, zumal die zu meldenden Verstöße nicht mehr auf Fälle beschränkt sind, in denen bestimmte Arten sensibler Daten unrechtmäßig in die Hände Dritter gelangt sind.

1.2.5.7 Wegfall der Informationspflichten

Generell entfallen die Benachrichtigungspflichten nach Art. 13 und 14, wenn und soweit die betroffene Person bereits über die Kenntnis der ansonsten mitzuteilenden Informationen verfügt (Art. 13 Abs. 4, Art. 14 Abs. 5 Lit. a). Dies ist der Fall, wenn ein entsprechendes Merkblatt ausgehändigt wurde, unabhängig davon, ob es gelesen wurde.

Über eine nicht beim Betroffenen stattgefundene Datenerhebung entfällt die Benachrichtigungspflicht u.a. auch dann, wenn die Daten einem Berufsgeheimnis einschließlich einer satzungsmäßigen Geheimhaltungspflicht unterliegen. Auffällig ist, dass eine Geheimhaltungsberechtigung bei verdeckt durchgeführten internen Ermittlungen, wie sie sich in § 33 Abs. 2 S. 1 Nr. 7 Lit. b BDSG für „ihrem Wesen nach“ – ggf. vorübergehend – geheimzuhaltende Daten wiederfindet, in den Ausnahmetatbeständen des Art. 14 Abs. 5 nicht enthalten ist.

1.2.5.8 Rechtmäßigkeitsvoraussetzung

Die Nichterfüllung der Informationspflicht führt im Regelfall nicht dazu, dass die nach der DS-GVO erlaubte Verarbeitung rechtswidrig würde, d.h. die Erfüllung der Informationspflicht ist wie bisher keine Rechtmäßigkeitsvoraussetzung. Anders muss es

im Einzelfall bei bewusster gravierender Missachtung der in Art. 5 enthaltenen Grundsätze für die Verarbeitung personenbezogener Daten sein, die in Abs. 1 Lit. a wie folgt lauten: „Personenbezogene Daten müssen auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbare Weise verarbeitet werden."

1.2.5.9 Das Auskunftsrecht und das Recht auf Datenportabilität

Das in Art. 15 geregelte Auskunftsrecht verpflichtet zur Mitteilung des Zwecks, der Empfänger oder Kategorien von Empfängern, einschließlich der Drittlandübermittlung und der Angaben zur Dauer der Verarbeitung, und beinhaltet zahlreiche auch in Art. 13 und 14 enthaltene Belehrungspflichten. Eine konkrete Auskunft über die Daten kann in elektronischer Form und auch in Form einer Kopie der verarbeiteten Daten verlangt werden (Art. 15 Abs. 1).

Das Auskunftsrecht wird ergänzt durch das Recht auf Datenportabilität (Art. 20), das wohl – was der Wortlaut aber nicht deutlich macht – zwar für den Wechsel eines Dienstanbieters von Social Networks konzipiert ist, aber auch bei anderen Vertragspartnern wie Versicherungen, Banken oder Energieversorgern hinsichtlich der diesen zur Verfügung gestellten Daten Anwendung findet. Der Betroffene kann sich dann aussuchen, ob er die Daten selbst zwecks Weitergabe an den neuen Vertragspartner erhalten will oder ob der bisherige Verarbeiter die Daten unmittelbar an den neuen Verarbeiter weitergeben soll. Ebenso kann ein Arbeitnehmer seine in ein Datensystem des Arbeitgebers eingegebenen Skill-Daten bei einem Wechsel zu einem anderen Arbeitgeber an diesen weitergeben lassen.

1.2.6 Korrekturrechte

1.2.6.1 Berichtigung

Art. 16 gibt dem Betroffenen ein Recht auf Berichtigung unzutreffender oder unvollständiger Daten ggf. durch Einfügung einer ergänzenden Erklärung. Keine Aussage wird getroffen, wer den Nachweis der Richtigkeit der Erklärung zu führen hat und ob der Verantwortliche eine vorgelegte ergänzende Erklärung des Betroffenen, deren Angaben er für unzutreffend hält, anders als es bei der personalaktenrechtlichen Gegendarstellung des § 83 Abs. 1 S. 3 BetrVG der Fall ist, zurückweisen kann. Dies ist wohl nach Art. 18 Abs.1 Lit. a und Abs. 3 nach entsprechender Überprüfung der Fall, wobei bis dahin die Daten einer eingeschränkten Verarbeitung unterliegen.

1.2.6.2 Löschung

Die Pflicht zur Löschung besteht nach Art. 17 Abs. 1 Lit. a und d, wenn die Daten unrechtmäßig verarbeitet werden, was auch regelmäßig der Fall ist, wenn der ursprüngliche Verarbeitungszweck entfällt oder der Beschäftigte einen berechtigten

Widerspruch nach Art. 21 Abs. 1 einlegt oder seine zunächst erteilte Einwilligung zurückzieht und keine die Verarbeitung gleichwohl rechtfertigende Norm vorliegt.

1.2.6.3 Das Recht auf „Vergessenwerden“

Die in Art. 17 Abs. 2 geregelte Pflicht zur Realisierung des „Vergessenwerdens“ findet sich bereits in der „Google-Spain“-Entscheidung des EuGH, in der eine Sperrverpflichtung von Suchmaschinenbetreibern bejaht wurde, die über die Löschpflichten der eigentlichen Webseitenbetreiber hinausgeht.

Der Verantwortliche, der personenbezogene Daten öffentlich gemacht und zur Löschung verpflichtet ist, hat Dritte darüber zu informieren, dass die betroffene Person die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten auch vom Dritten verlangt hat. Suchmaschinen oder News-Sites, die ihrerseits zur Löschung eines Links verpflichtet sind, müssen den Erstveröffentlichenden vom Löschbegehren in Kenntnis setzen. Gleichzeitig ist der Erstveröffentlichende gehalten, auf jeden Dritten einzuwirken, der die Daten nun weiterverarbeitet. Eine eigenständige Löschverpflichtung Dritter wird durch die Mitteilung nicht begründet, diese richtet sich originär nach Art. 17 Abs. 1. Das Recht auf Vergessenwerden bedingt die Identifizierung der jeweiligen Dritten durch den Verantwortlichen. Dies soll anhand angemessener Maßnahmen unter Berücksichtigung der verfügbaren Technologie und der jeweiligen Implementierungskosten erreicht werden.

1.2.6.4 Einschränkung der Verarbeitung

Der im BDSG als „Sperrung“ (§ 3 Abs. 4 S. 2 Nr. 4 BDSG) bezeichnete Vorgang der „Einschränkung der Verarbeitung“ besteht nach Art. 4 Abs. 3 in der „Markierung“ gespeicherter personenbezogener Daten mit dem Ziel, dass sie (abgesehen von ihrer Speicherung) nur noch unter besonders engen Voraussetzungen und besonderen Zweckbestimmungen verarbeitet werden dürfen.

Die „Einschränkung der Verarbeitung“ tritt an die Stellung der Löschung von Daten, wenn diese im Interesse der betroffenen Person oder des für die Verarbeitung Verantwortlichen anstelle einer Löschung geboten ist.

Im Interesse der betroffenen Person liegt die weitere Existenz der Daten, wenn an und für sich die Löschung ansteht, weil der für die Verarbeitung Verantwortliche sie nicht mehr benötigt, d.h. der Speicherzweck entfallen ist, die betroffene Person der Daten jedoch noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen bedarf (Art. 18 Abs. 1 Lit. b).

Im Interesse des für die Verarbeitung Verantwortlichen liegt die zunächst fortdauernde Existenz solange, bis er, wenn die betroffene Person eine Löschung der Daten wegen Unrichtigkeit oder Verletzung der sich aus ihrer besonderen Situation ergebenden schutzwürdigen Interessen verlangt, die Berechtigung des Begehrens geprüft hat.

Art. 18 Abs. 2 reduziert die Zulässigkeit der nur noch für eingeschränkte Verarbeitungen bestimmten Daten auf vier Tatbestände, nämlich dass die Verarbeitung

- mit Einwilligung der betroffenen Person
  oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
  oder
- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person
  oder
- aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats

erfolgt.

1.2.6.5 Das allgemeine Widerspruchsrecht

Nach Art. 21 Abs. 1 hat jeder das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen eine aufgrund von Art. 6 Abs. 1 Lit. e oder f erfolgende Verarbeitung einschließlich von Profilerstellungen Widerspruch einzulegen. Dem Widerspruch ist nachzukommen, es sei denn, dass zwingende schutzwürdige Gründe, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, für die Verarbeitung dargelegt und nachgewiesen werden oder dass die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Die Regelung entspricht weitgehend der im Beschäftigungsverhältnis kaum relevant gewordenen Bestimmung des § 35 Abs. 5 BDSG.

1.3 Fazit

Die DS-GVO ändert die Konzeption und weitgehend auch die Detailregelungen des geltenden Datenschutzrechts nicht grundlegend. Vielmehr werden vielfach Bestimmungen der die Grundlage des BDSG bildenden Datenschutzrichtlinie 95/46/EG übernommen. Andererseits gibt es aber auch zahlreiche neue datenschutzrechtliche Vorgaben, deren Erfüllung hinsichtlich des immens erhöhten Bußgeldrahmens korrekter Beachtung bedarf. Inwieweit die DS-GVO als Internetgesetz für die Big-Data-Welt und für die digitalisierte Welt der Arbeit zukunftsweisende Regelungen enthält, bleibt abzuwarten.

2 Häufig gestellte Fragen und Irrtümer zur DS-GVO[1]

2.1 „Die Datenschutz-Grundverordnung gilt nicht für kleine Unternehmen.“

Irrtum. Die DS-GVO gilt für jede Person oder Organisation, die personenbezogene Daten elektronisch oder nicht automatisiert in einer strukturierten Ablage verarbeitet. Ausgenommen sind nur Verarbeitungen im Rahmen persönlicher oder familiärer Tätigkeiten und einige staatliche Aktivitäten. Betroffen von der DS-GVO sind folglich

- Unternehmen,
- Vereine,
- Verbände,
- Parteien,
- Stiftungen,
- Körperschaften des öffentlichen Rechts und
- Einrichtungen des Bundes, der Länder und Kommunen.

Die Vorschriften der DS-GVO sind von einem Ein-Personen-Unternehmen genauso einzuhalten wie von einem Konzern. Letzterer verfügt jedoch über mehr Ressourcen und zahlt im Zweifel geringere Bußgelder, da der maximale Bußgeldrahmen ab einem Umsatz von 500 Mio. Euro 4 Prozent des weltweiten Jahresumsatzes beträgt. Für Jahresumsätze unterhalb von 500 Mio. gilt der umsatzunabhängige Maximalbetrag von 20 Mio. Euro.

2.2 „Vereine sind von der DS-GVO nicht betroffen.“

Die DS-GVO gilt auch für Vereine, sobald diese elektronisch oder nicht automatisiert in einer strukturierten Ablage (z.B. Mitgliederkartei mit Karteikarten) personenbezogene Daten verarbeiten. Da Steuerklärungen elektronisch abgegeben werden müssen, können Vereine grundsätzlich eine elektronische Datenverarbeitung nicht vermeiden.

1. Ursprünglich erschienen in LOHN+GEHALT 1/2017, S. 88-91, Niels Lepperhoff: Hilfe, mein Datenschutzbeauftragter schläft

2.3 „Der deutsche Gesetzgeber wird für Ausnahmen sorgen.“

Gewöhnlich nutzt die EU das Instrument der Richtlinie zur Gesetzgebung. Richtlinien müssen im Gegensatz zu Verordnungen durch nationale Gesetzgeber in Gesetze „übersetzt“ werden. Verordnungen gelten dagegen unmittelbar, d.h. sie benötigen keine „Übersetzung“ in nationale Gesetze. Die DS-GVO ist eine solche Verordnung. Da EU-Gesetze den nationalen Gesetzen vorgehen, kann ein nationaler Gesetzgeber kein EU-Gesetz aufheben oder abschwächen.

Die DS-GVO erlaubt durch sogenannte „Öffnungsklauseln“ in ganz wenigen Fällen dem nationalen Gesetzgeber, die Regelungen der DS-GVO auszugestalten. Zu den für die Wirtschaft relevanten Bereichen zählen der Arbeitnehmerdatenschutz und die Bestellpflicht des Datenschutzbeauftragten. Die meisten Öffnungsklauseln gelten nur für Einrichtungen des Bundes, der Länder und Kommunen.

2.4 „Mit der DS-GVO ändert sich nichts.“

Wer die ersten Pressemitteilungen verfolgte, konnte diesen Eindruck gewinnen. Zwar sind die bekannten Prinzipien des Datenschutzes unverändert geblieben. Unter der Oberfläche fand aber eine umfangreiche Renovierung statt.

Zu den umwälzenden Neuerungen zählt

- die Pflicht, jederzeit das Einhalten der DS-GVO nachweisen zu können und
- durch eine geeignete Organisation die Einhaltung des Datenschutzes systematisch im Unternehmen zu kontrollieren.

2.5 „Die Einhaltung kontrolliert doch keiner.“

Die personelle Ausstattung der Datenschutzaufsichtsbehörden lässt diesen Schluss durchaus zu. Für großflächige Kontrollen fehlt das Personal. Auf der anderen Seite setzt die DS-GVO neben der anlasslosen Kontrolle durch Datenschutzaufsichtsbehörden auch auf die Kontrolle durch die von der Datenverarbeitung betroffenen Personen. Diese müssen zukünftig detailliert über die Art und Weise der Datenverarbeitung informiert werden (siehe Kapitel 19). Dazu gehört auch eine Belehrung über das Beschwerderecht bei der Datenschutzaufsichtsbehörde. Erfahrungsgemäß nutzen unzufriedene Kunden, Lieferanten oder Mitarbeiter die Beschwerdemöglichkeit.

Eine Datenschutzaufsichtsbehörde geht jeder Beschwerde nach, d.h. betroffene Personen lösen mit einer Beschwerde regelmäßig eine Untersuchung gegen das Unternehmen aus. Bei einer Untersuchung profitieren die Datenschutzaufsichtsbehörden von der neuen Rechenschaftspflicht, d.h. der Pflicht, die Einhaltung sämtlicher Vorschriften der DS-GVO jederzeit nachweisen zu können. Eine Datenschut-

zaufsichtsbehörde kann verlangen, dass nachgewiesen wird, dass entgegen der Beschwerde des Betroffenen die Datenverarbeitung in Einklang mit der DS-GVO erfolgte. Schlägt ein solcher Nachweis fehl, bspw. weil die notwendigen Dokumente nicht vorhanden sind, stellt das einen Verstoß gegen Art. 5 Abs. 2 DS-GVO dar, der mit max. 20 Mio. Euro oder – sofern höher – 4 Prozent des weltweiten Jahresumsatzes bußgeldbewehrt ist.

Zusätzlich lässt die DS-GVO auch Verbandsklagen zu Gunsten der Betroffenen zu.

Weiterhin muss an die Datenschutzaufsichtsbehörde gemeldet werden, welche Person als betrieblicher Datenschutzbeauftragter bestellt ist. Damit werden die Datenschutzaufsichtsbehörden in die Lage versetzt, durch Abgleich bspw. mit Unternehmensregistern Unternehmen zu identifizieren, die gegen die Bestellpflicht verstoßen.

2.6 „Wir verarbeiten keine personenbezogenen Daten.“

Die DS-GVO definiert in Art. 4 Nr. 1 personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person‘) beziehen“. Zu diesen Personen zählen sowohl Mitarbeiter von Kunden und Lieferanten als auch die eigenen Mitarbeiter. Es kommt ausschließlich auf den Status als natürliche Person an und nicht auf die Beziehung zum Unternehmen.

Identifizierbar wird eine Person, wenn durch die Kombination der Daten auf eine konkrete Person geschlossen werden kann. Diese muss nicht namentlich bekannt sein. Beispiele für regelmäßig personenbezogene Daten:

- E-Mail-Adresse,
- IP-Nummer,
- Kundennummer,
- Mitarbeiternummer,
- Telefonnummer,
- Sprachaufzeichnung,
- Portraitfoto und
- Videoaufzeichnung der Person.

In der Praxis sind fast alle Daten bzw. Datensätze in einem Unternehmen personenbezogen: Rechnungsdaten werden personenbezogen, wenn der Name des Bearbeiters aufgedruckt wird. Datenbanken speichern die Kennung des Bearbeiters, so dass die bearbeiteten Daten personenbezogen werden. Hierbei spielt es keine Rolle, ob die personenbezogenen Daten der beruflichen Tätigkeit oder dem Privatleben der natürlichen Person zuzurechnen sind.

Für eine praktische Betrachtung empfiehlt es sich, grundsätzlich von einem Personenbezug auszugehen, sofern er nicht widerlegbar ist.