Zeitablauf EU-DSGVO

Begleitende Prozesse

- Gesetz zu nationalen Anpassungen (BDSG-neu im DSAnpUG-EU[4])
- Frist für Meldung der nationalen Umsetzungen bis 24. Mai 2018 23:59 Uhr

---

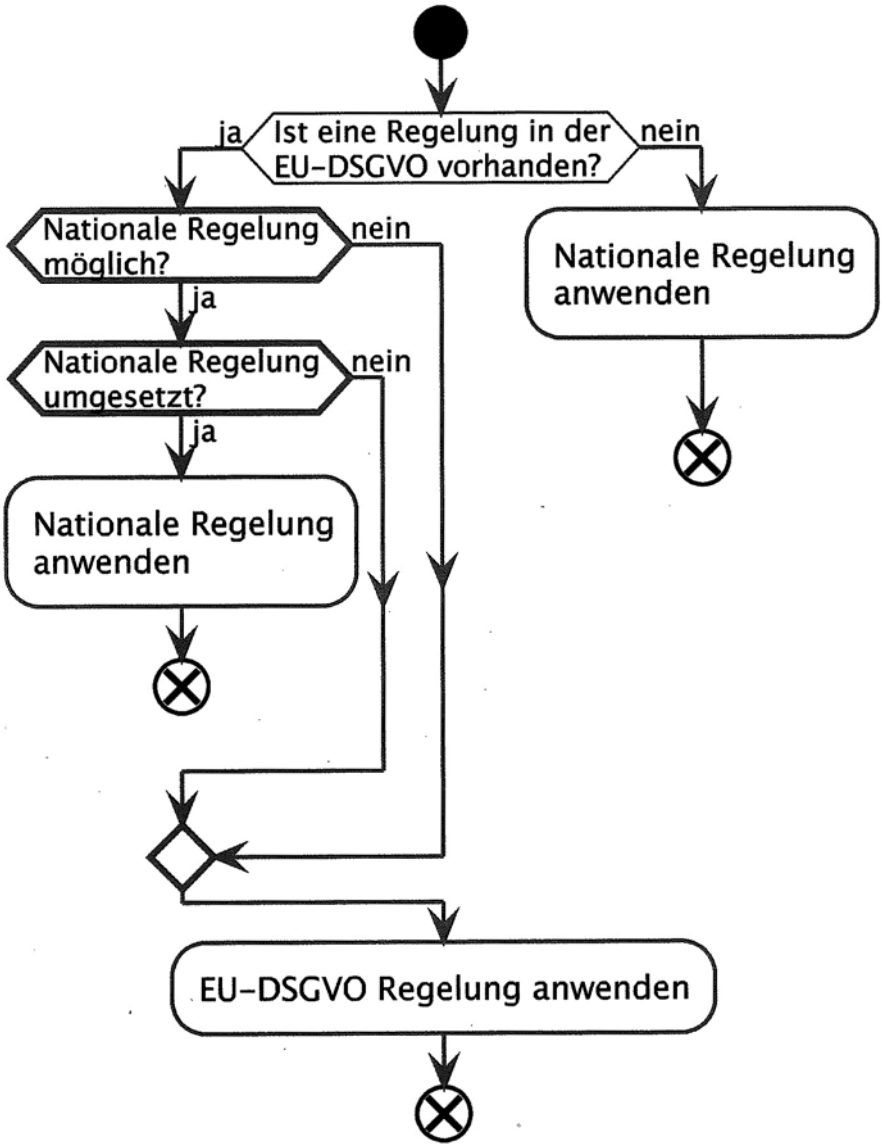
Bemerkung: Um ein reibungsloses Zusammenspiel der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 mit dem deutschen Datenschutzrecht sicherzustellen, wird das bisherige Bundesdatenschutzgesetz (BDSG) durch ein neues Allgemeines Bundesdatenschutzgesetz (ABDSG) abgelöst.

Grundsätze (Artikel 5)

Grundsatz	Anmerkung
Rechtmäßigkeit	eine Rechtsgrundlage für die Verarbeitung existiert
Treu und Glauben	unbestimmter Rechtsbegriff: redlich, anständig
Transparenz	Für die betroffene Person nachvollziehbar
Zweckbindung	festgelegte, eindeutige und legitime Zwecke
Datenminimierung	Verarbeitung auf das zweckgebundene, notwendige Maß beschränkt
Richtigkeit	Daten müssen sachlich richtig und auf neuestem Stand sein
Speicherbegrenzung	frühestmögliche Löschung nach Wegfall der zweckgebundenen Erforderlichkeit der Speicherung
Integrität und Vertraulichkeit	Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Verlust, Schädigung

Achtung: Der Verantwortliche muss die Einhaltung der Grundsätze nachweisen können („*Rechenschaftspflicht*“)

Prüfvorgehen Anwendung EU-DSGVO



	Checkliste Grundsätze der pbDV	
	Alle der folgenden Voraussetzungen treffen zu	*Gründe*
☐	Die Verarbeitung ist rechtmäßig	Art. 5 Abs. 1a
☐	Die Verarbeitung erfolgt nach Treu und Glauben	Art. 5 Abs. 1a
☐	Die Transparenzpflichten sind eingehalten	Art. 5 Abs. 1a, EG 58
☐	Alle Informationen und Mitteilungen zur Verarbeitung sind leicht erreichbar	EG 39
☐	Alle Informationen und Mitteilungen zur Verarbeitung sind verständlich und in klarer, einfacher Sprache verfasst	EG 39
☐	Der Umfang der Verarbeitung ist dokumentiert	EG 39
☐	Die Zwecke der Verarbeitung sind dokumentiert	EG 39
☐	Es werden nur die für die Verarbeitung erforderlichen Daten verarbeitet	Art. 5 Abs. 1c
☐	Die verarbeiteten Daten sind aktuell und sachlich richtig	Art. 5 Abs. 1d
☐	Unrichtige Daten können unverzüglich gelöscht oder berichtigt werden	Art. 5 Abs. 1d
☐	Es werden kürzestmögliche Löschfristen eingehalten	Art. 5 Abs. 1e
☐	Die Daten werden vor unbefugter und unrechtmäßiger Verarbeitung geschützt	Art. 5 Abs. 1f
☐	Die Daten werden vor unbeabsichtigter Zerstörung und Schädigung geschützt	Art. 5 Abs. 1f
☐	Die vorgenannte Maßnahmen können nachgewiesen werden	Art. 5 Abs. 2

Wichtig: Beachten Sie bitte auch hier die Forderung nach Nachweisbarkeit (Rechenschaftspflicht)

	Checkliste Einwilligung in die pbDV	
	Alle der folgenden Voraussetzungen treffen zu	*Gründe*
☐	Der Verarbeiter ist bekannt	EG 42
☐	Der oder die Zwecke der Verarbeitung sind dargestellt	Art. 6 Abs. 1a, EG 42
☐	Der Umfang der Einwilligung wird beschrieben	EG 42
☐	In verschiedene Verarbeitung kann einzeln eingewilligt werden	Art. 7 Abs. 2, EG 32
☐	Vorformulierte Einwilligungen sind leicht zugänglich und in klarer und einfacher Sprache verfasst	EG 42
☐	Die Einwilligung ist nachweisbar	Art. 7 Abs. 1
☐	Die Einwilligung ist freiwillig	Art. 4 Nr. 11, EG 32
☐	Zur Einwilligung fand eine bestätigende Handlung statt	EG 32
☐	Die Einwilligung erfolgt dediziert und nicht mit anderen Erklärungen zusammen	Art. 7 Abs. 2
☐	Es wird auf das Recht auf Widerruf hingewiesen	Art. 7 Abs. 3, EG 65
☐	Der Widerruf ist genauso einfach zu erklären wie die Einwilligung	Art. 7 Abs. 3
☐	Die Einwilligung wird nicht mit der Erfüllung Verträgen oder Dienstleistungen gekoppelt, wenn dies nicht erforderlich ist	Art. 7 Abs. 4

	Checkliste Rechtmäßigkeit der pbDV	
	Eine der folgenden Voraussetzungen trifft zu	*Gründe*
☐	Die Verarbeitung ist erforderlich zur Erfüllung eines Vertrags mit der betroffenen Person	Art. 6 Abs. 1b, EG 44
☐	Die Verarbeitung ist erforderlich für vorvertragliche Maßnahmen auf Anfrage der betroffenen Person	Art. 6 Abs. 1b, EG 44
☐	Die Verarbeitung ist erforderlich zur Erfüllung einer rechtlichen Pflicht des für die Verarbeitung Verantwortlichen	Art. 6 Abs. 1c, EG 45
☐	Die Verarbeitung ist erforderlich, weil lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person geschützt werden	Art. 6 Abs. 1d, EG 46
☐	Die Verarbeitung ist erforderlich im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt	Art. 6 Abs. 1e, EG 45
☐	Berechtigtes Interesse, wenn schutzwürdige Interessen dem nicht entgegen stehen (insbesondere bei Kindern)	Art. 6 Abs. 1f, EG 47
☐	Einwilligung der Person für einen oder mehrere Zwecke ist nachweisbar	Art. 7 Abs. 1, EG 42

Wichtig: Beachten Sie bitte auch hier die Forderung nach Nachweisbarkeit (Rechenschaftspflicht)

	Checkliste Informationspflichten nach Artikel 13 (und 14)	Art. 13	Art. 14
☐	Mitteilung zum Zeitpunkt der Erhebung	✓	
☐	Kontaktdaten des für die Verarbeitung Verantwortlichen, sowie Vertreter	✓	✓
☐	Falls vorhanden: Kontaktdaten Datenschutzbeauftragter	✓	✓
☐	Zwecke	✓	✓
☐	Rechtsgrundlage der Verarbeitung	✓	✓
☐	Falls Art. 6 Abs. 1f: Nennung der berechtigten Interessen, die verfolgt werden	✓	✓
☐	Kategorien der personenbezogenen Daten, die verarbeitet werden		✓
☐	Ggfs. Empfänger oder Kategorien von Empfängern	✓	✓
☐	Ggfs. Drittländer oder internationale Organisationen, an die Daten übermittelt werden, dazu:	✓	✓
☐	Ggfs. das Fehlen oder Vorhandensein eines Angemessenheitsbeschlusses der Kommission	✓	✓
☐	Ggfs. Hinweis auf geeignete Garantien (z.B. Standardvertragsklauseln, genehmigte Verhaltensregeln, genehmigte Zertifizierungen, BCRs) und wo diese verfügbar sind	✓	✓
☐	Speicherdauer der Daten oder die Kriterien für die Festlegung der Dauer	✓	✓
☐	Hinweise auf auf die Rechte auf *Auskunft (Art. 15)*, *Berichtigung (Art. 16)*, *Löschung (Art. 17)*, *Einschränkung der Verarbeitung (Art. 18)*, eines *Widerspruchsrechts (Art. 21)* sowie des Rechts auf *Datenübertragbarkeit(Art. 20)*	✓	✓
☐	Bei Verarbeitung aufgrund einer Einwilligung: das Recht, die Einwilligung mit Wirkung auf die Zukunft zu widerrufen	✓	✓
☐	Hinweis, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist	✓	
☐	Hinweis, ob die Bereitstellung der personenbezogenen Daten für einen Vertragsabschluss erforderlich ist	✓	
☐	Hinweis, ob die betroffene Person verpflichtet ist, die Daten bereit zu stellen	✓	
☐	Hinweis, welche Folgen die Nichtbereitstellung hätte	✓	
☐	Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde	✓	✓
☐	Hinweis aus welcher Quelle die Daten stammen und ob sie aus öffentlich zugänglichen Quellen stammen		✓
☐	Bei automatisierten Einzelentscheidungen: aussagekräftige Informationen über die Logik	✓	✓
☐	Bei automatisierten Einzelentscheidungen: Tragweite und Auswirkungen der Verarbeitung für die betroffene Person	✓	✓
☐	Bei geplanter Zweckänderung: neuen Zweck und alle vorher genannten Informationen angeben	✓	✓
☐	Ein-Monats-Frist einhalten		✓

Checkliste der wichtigsten Änderungen durch die DSGVO

Drastisch erhöhte Bußgelder: bis zu vier Prozent des globalen Umsatzes

Deutlich erweiterte zivilrechtliche Haftung: Ersatz auch immaterieller Schäden, Verbandsklagen, Beweislastumkehr

Stellung des Datenschutzbeauftragten: Zusätzliche Verantwortung und Haftung für DSBs

Stark erweiterte Dokumentations- und Nachweispflichten

Datenschutz-Folgenabschätzung statt Vorabkontrolle: Weitergehende Prüf- und Abstimmungspflichten

Risikobasierter Datenschutz

Globale bzw. extraterritoriale Anwendung der DSGVO möglich

Anwendungsvorrang der DSGVO: Vorrang statt Auffangregelung

Massiv erweiterte Transparenzanforderungen

Datensicherheit

Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen

Erweiterte Melde und Benachrichtigungspflichten bei Datenschutzverstößen

Striktere Löschpflichten und Recht auf Vergessenwerden

Neue Vorgaben für Zweckänderungen

Erleichterter Datenaustausch im Konzern

Koppelungsverbot bei Einwilligungen

Überblick über die in der Checkliste zusammengefassten Änderungen

Insgesamt bringt die DSGVO für Wirtschaftsunternehmen erheblichen Mehraufwand mit sich. Zwar sind sich die DSGVO und das BDSG in Aufbau und Systematik durchaus ähnlich. Unternehmen müssen aber umfassende neue Strukturen und Prozesse schaffen, um den Vorgaben der DSGVO zu entsprechen. Der nachstehende Überblick zeigt, auf welche Vorgaben der DSGVO man bei der Umsetzung der neuen Anforderungen besonders achten sollte.

1. Höhere Bußgelder

Art. 83 DSGVO sieht für Unternehmen Bußgelder von bis zu 4 Prozent des globalen Umsatzes vor. An Verstößen gegen die DSGVO beteiligte natürliche Personen müssen mit Geldbußen von bis zu 20 Millionen Euro rechnen. Bei Unternehmen kommen mit der umsatzbezogenen Berechnung noch deutlich höhere Bußgelder in Betracht. Bei großen

Unternehmen oder Konzernen können durchaus dreistellige Millionenbeträge erreicht werden.

Damit verschärft sich der Bußgeldrahmen gegenüber dem bisherigen Recht drastisch. Bislang sah § 43 BDSG Bußgelder von maximal 300.000 Euro vor. Der kommende, auf den Umsatz basierte Bußgeldrahmen ermöglicht Sanktionen, die bei großen Unternehmen ohne weiteres dreistellige Millionenbeträge erreichen können. Die Aufsichtsbehörden sollen sicherstellen, dass die Geldbußen für Verstöße gegen die Verordnung „wirksam, verhältnismäßig und abschreckend“ sind.

2. Erweiterte Haftung für Verantwortliche und für Auftragsverarbeiter

Neben den Bußgeldern steigen die Risiken für Unter- nehmen auch im Hinblick auf die zivilrechtliche Haftung wegen tatsächlichen oder behaupteten Datenschutz- verstößen. Nach Art. 82 Abs. 1 DSGVO sind materielle und immaterielle Schäden zu erstatten, die auf Verstößen gegen die Verordnung beruhen. Die ausdrückliche Nennung immaterieller Schäden kann in der Praxis zu einer erheblichen Veränderung gegenüber der bisherigen Rechtslage führen. Deutsche Gerichte waren in der Vergangenheit zurückhaltend damit, betroffenen Personen wegen Datenschutzverstößen nennenswerte Schadensersatzzahlungen zuzusprechen. Hier dürfte der EuGH künftig auf der Grundlage der Verordnung neue Maßstäbe anlegen. Eine weitere Neuerung ist die ausdrückliche Erweiterung der Haftung auch auf Auftragsverarbeiter, Art. 82 Abs. 1 DSGVO.

3. Stellung und Haftung des Datenschutzbeauftragten

Datenschutzbeauftragte dürfen sich künftig über eine wichtigere Stellung im Unternehmen freuen. Umgekehrt müssen sie sich künftig jedoch auch auf einen schärferen Haftungsmaßstab einstellen.

Grundsätzlich sieht die Verordnung eine Pflicht zur Bestellung eines Datenschutzbeauftragten nur unter engenVoraussetzungenvor.1Falls aber das Recht eines Mitgliedstaates eine Bestellung vorschreibt, müssen Unternehmen zwingend einen Datenschutzbeauftragten bestellen, Art. 37 Abs. 4 DSGVO. Sofern der deutsche Gesetzgeber § 4f BDSG nicht aufhebt oder durch eine andere Regelung ersetzt, bleibt es bei den dort genannten Voraussetzungen für die Bestellung eines Datenschutzbeauftragten. Es besteht derzeit auch kein Anlass zu der Annahme, dass Art. 37 bis Art. 39 DSGVO den bislang in § 4f Abs. 3 BDSG geregelten Kündigungsschutz, das Benachteiligungsverbot oder den Schutz vor Widerruf der Bestellung verdrängen. Vielmehr dürfte es sich hier um weiterhin geltende flankierende einzelstaatliche Regelungen zur DSGVO handeln.

Zu den Aufgaben des Datenschutzbeauftragten zählen unter anderem: die Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten beim Datenschutz, die Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften sowie die Überwachung der Strategien für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, Schulungen und Überprüfungen. Zudem berät er auf Anfrage zu der Datenschutz-Folgenabschätzung und der Überwachung ihrer Durchführung, arbeitet mit der Aufsichtsbehörde zusammen und ist deren Ansprechpartner.

Nach § 4f Abs. 1 Satz 1 BDSG „wirkt der Datenschutzbeauftragte auf die Einhaltung“ der Vorschriften über den Datenschutz hin. Danach hat er derzeit eine beratende und unterstützende Funktion und übernimmt keine Gewähr dafür, dass die verantwortliche Stelle alle datenschutzrechtlichen Standards umsetzt. Anders als nach dem bisherigen Recht sieht Art. 39 Abs. 1 lit. b DSGVO umfassende Überwachungspflichten vor. Diese gehen ihrem Wortlaut nach über ein bloßes „Hinwirken“ deutlich hinaus. Es bleibt daher abzuwarten, ob und in welchem Umfang Gerichte und Behörden Datenschutzbeauftragte künftig im Rahmen einer straf- und ordnungswidrigkeitenrechtlichen Verantwortlichkeit als „Überwachergaranten“ einordnen werden

4. Erweiterte Dokumentations- und Nachweispflichten

Die DSGVO sieht für Verantwortliche und Auftragsver- arbeiter deutlich erweiterte Nachweispflichten vor (sogenannte „accountability“). Art. 5 Abs. 2 DSGVO schreibt vor, dass der für die Verarbeitung Verantwortliche nachweisen können muss, dass er die in Art. 5 Abs. 1 DSGVO geregelten Datenschutzgrundsätze einhält. Verstößt ein verantwortliches Unternehmen gegen diese Vorgabe, drohen Bußgelder von bis zu 4 Prozent des Umsatzes. Nach Art. 24 Abs. 1 DSGVO muss der für die Verarbeitung Verantwortliche nachweisen können, dass er personenbezogene Daten in Übereinstimmung mit der Verordnung verarbeitet. Auftragsverarbeiter müssen dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, damit der Verantwortliche nachweisen kann, dass er seine in Art. 32 bis Art. 36 DSGVO geregelten Pflichten erfüllt.

5. Datenschutz-Folgenabschätzung

Das Konzept der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO weicht erheblich von dem der Vorabkontrolle nach § 4d Abs. 5 BDSG ab. Hat eine Datenverarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten der davon betroffenen Personen zur Folge, so muss der Verantwortliche eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchführen. Hierbei sollen insbesondere Eintrittwahrscheinlichkeit und Schwere möglicher Risiken bewertet werden. Das Unternehmen soll auch Art, Umfang, Umstände, verfolgte Zwecke sowie Ursachen möglicher Risiken bewerten. Dabei soll es auch Maßnahmen, Garantien und Verfahren prüfen, mit denen Unternehmen bestehende Risiken eindämmen und die sonstigen Vorgaben der Verordnung einhalten können.

Sofern die Datenschutz-Folgenabschätzung ergibt, dass die geplante Datenverarbeitung tatsächlich ein hohes Risiko zur Folge hätte, muss der Verantwortliche nach Art. 36 DSGVO die zuständige Aufsichtsbehörde zu Rate ziehen, sofern er keine Maßnahmen zur Eindämmung des Risikos trifft.

6. Risikobasierter Datenschutz

An vielen Stellen der DSGVO stehen die von der Verordnung geforderten Maßnahmen in direkter Abhängigkeit von den Risiken, die eine Datenverarbeitung für die persönlichen Rechte und Freiheiten betroffener Personen mit sich bringt. Dieser risikobasierte Ansatz beim Datenschutz ist gerade im Hinblick auf den Verhältnismäßigkeitsgrundsatz im Rahmen einer Verarbeitung nach Treu und Glauben folgerichtig, vgl. Art. 5 Abs. 1 DSGVO. Ein solches risikobasiertes Vorgehen ist gerade bei sogenannten Compliance Management Systemen (CMS) üblich und zweckmäßig. Daher lassen sich viele Erfahrungen aus Compliance-Strukturen und dem Risikomanagement auf den Datenschutz nach der DSGVO übertragen.

7. Globale Anwendung der DSGVO

Die Verordnung erweitert den räumlichen Anwendungsbereich des EU-Datenschutzrechts massiv. Die DSGVO gilt zunächst für die Datenverarbeitung im Rahmen von Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union, Art. 3 Abs. 1 DSGVO. Entscheidend ist dabei der Ort der Niederlassung und nicht der Ort der Datenverarbeitung. Das Niederlassungsprinzip der Verordnung wird durch das sogenannte „Marktortprinzip“ des Art. 3 Abs. 2 DSGVO noch erweitert. Nach dieser Vorschrift kann die Verordnung auch auf Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der EU Anwendung finden.

Die DSGVO gilt zum einen für Datenverarbeitungen, die dazu dienen, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten, Art. 3 Abs. 1 lit. a DSGVO. Hierbei ist unerheblich, ob für die angebotenen Waren oder Dienste eine Zahlung zu leisten ist. Zum anderen findet die Verordnung auch auf Datenverarbeitungen Anwendung, die der Beobachtung von betroffenen Personen in der Europäischen Union dienen.

8. Vorrang der DSGVO vor anderen Rechtsvorschriften der Mitgliedsstaaten

Die DSGVO wirkt nach Art. 288 Abs. 2 Satz 1 AEUV unmittelbar und direkt, ohne dass es ihrer innerstaatlichen Umsetzung bedarf. Als EU-Verordnung geht sie Rechtsvorschriften der einzelnen Mitgliedsstaaten vor. Sofern die DSGVO keine ausdrücklichen Möglichkeiten für einzelstaatliche Regelungen vorsieht, verdrängt die Verordnung Vorschriften der Mitgliedsstaaten zur Datenverarbeitung. Die DSGVO ist anders als das BDSG kein Auffanggesetz, sondern eine Vorrangregelung. Die Verordnung geht “normalgesetzlichen” Regelungen wie etwa dem Kreditwesengesetz, dem Betriebsverfassungsgesetz oder den Sozialgesetzbüchern vor, sofern diese nicht die in der DSGVO aufgestellten Anforderungen an Ausnahmevorschriften zur DSGVO erfüllen.

9. Erweiterte Transparenzvorschriften

Künftig müssen Unternehmen betroffene Personen deutlich umfassender als bislang und in einer nachvollziehbaren Weise darüber informieren, wie sie deren Daten verarbeiten. Nach Art. 5 Abs. 1 DSGVO zählt der Transparenzgrundsatz zu den wesentlichen Prinzipien der Verordnung. Sowohl Verstöße gegen Art. 5 DSGVO als auch gegen die Transparenzvorschriften der Art. 12 bis Art. 15 DSGVO werden mit dem erhöhten Bußgeldrahmen von bis zu 4 Prozent des Umsatzes geahndet. Grundsätzlich muss der Verantwortliche betroffene Personen von der Verarbeitung ihrer personenbezogenen Daten „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache“ unterrichten, Art. 12 Abs. 1 DSGVO. Dabei sehen vor allem Art. 12 bis Art. 15 DSGVO umfangreiche Unterrichtungsrechte betroffener Personen und Auskunftspflichten Verantwortlicher vor. Gerade die Unterrichtungspflichten nach Art. 13 und Art. 14 DSGVO gehen weit über die Vorgaben der bislang geltenden § 4 Abs. 3 und § 33 BDSG hinaus.

Die Unterrichtungspflichten nach Art. 13 DSGVO entfallen, wenn und soweit die betroffene Person bereits über die fragliche Information verfügt. Für die Informationspflichten bei Daten, die nicht bei der betroffenen Person erhoben wurden, gelten nach Art. 14 Abs. 5 DSGVO etwas weitgehendere Ausnahmen, bei deren Vorliegen der Verantwortliche von einer Unterrichtung absehen kann.

10. Datensicherheit

Eine weitere für die Praxis wesentliche Änderung ist das Bußgeldrisiko bei unzureichender Datensicherheit. Bislang waren Verstöße gegen § 9 BDSG nicht bußgeldbewehrt. Dies ändert sich mit der Verordnung grundlegend. Art. 32 DSGVO regelt die künftigen Vorgaben zur Datensicherheit. Verstöße gegen diese Vorschrift werden nach der Verordnung mit Bußgeldern von bis zu 2 Prozent des Umsatzes geahndet. Das ist eine wesentliche Änderung gegenüber dem BDSG. Denn Verstöße gegen § 9 BDSG waren nicht bußgeldbewehrt

11. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Art. 25 Abs. 1 DSGVO regelt den Grundsatz der „privacy by design“; Abs. 2 die Anforderung „privacy by default“. Unternehmen müssen ihre IT-Systeme nach Art. 25 Abs. 1 DSGVO grundsätzlich so ausgestalten, dass sie die Datenschutzgrundsätze des Art. 5 DSGVO wirksam umsetzen, insbesondere das Gebot der Datenminimierung – sie sollen also nur gerade so viele Daten erheben, wie zur Erfüllung des verfolgten Zwecks erforderlich.

Zudem sollen IT-Systeme so „voreingestellt“ sein, dass sie grundsätzlich nur solche personenbezogenen Daten verarbeiten, deren Verarbeitung für den jeweils verfolg- ten Zweck erforderlich ist, Art. 25 Abs. 2 DSGVO. Maßnahmen zur Umsetzung dieser Anforderungen sollen etwa darin liegen, dass Verantwortliche perso- nenbezogene Daten minimieren und Daten so schnell wie möglich zu pseudonymisieren. Das Recht auf Datenschutz soll bereits bei der Entwicklung und Ausgestaltung von IT-Produkten, Diensten oder Anwendun- gen berücksichtigt werden. Verstöße gegen das Gebot, Datenschutz durch

Technik und datenschutzfreundliche Voreinstellungen zu gewährleisten, können mit Bußgeldern von bis zu 2 Prozent des Umsatzes des Unternehmens geahndet werden.

12. Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

Die Verordnung sieht in Art. 33 und Art. 34 DSGVO umfassendere Meldepflichten gegenüber der Aufsichts- behörde sowie Benachrichtigungspflichten gegenüber den betroffenen Personen vor, als die bisherige Rege- lung in § 42a BDSG dies tut.

Wesentliche Voraussetzung für eine mögliche Melde- beziehungsweise Benachrichtigungspflicht ist eine Da- tenschutzverletzung. Nach Art. 4 Nr. 12 DSGVO ist eine „Verletzung des Schutzes personenbezogener Daten“ eine „Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob zufällig oder unrechtmäßig, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu perso- nenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“. Diese Definition ist deutlich weiter als die bislang in § 42a BDSG geregelten Tatbestandsmerkmale.

Grundsätzlich muss das verantwortliche Unternehmen der Aufsichtsbehörde jede Datenschutzverletzung un- verzüglich und möglichst innerhalb von 72 Stunden melden, nachdem dem Verantwortlichen die Verletzung bekannt wurde. Ausnahmsweise besteht keine Pflicht zur Meldung bei der Aufsichtsbehörde, wenn die Verlet- zung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen führt.

Hat eine Datenschutzverletzung darüber hinaus voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge, muss der Verantwortliche grundsätzlich die hiervon betroffenen Personen ohne unangemessene Verzögerung benachrichtigen, Art. 34 Abs. 1 DSGVO. Ausnahmsweise kann der Verantwortliche von der Benachrichtigung absehen, wenn er Risiken für die betroffenen Personen durch geeignete technische und organisatorische Sicherheitsvorkehrungen oder durch nachfolgende Maßnahmen ausgeschlossen hat, vgl. Art. 34 Abs. 3 DSGVO. Fehler bei der Umsetzung der Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen werden mit Bußgeldern von bis zu 2 Prozent des Umsatzes geahndet.

13. Löschen von Daten und Recht auf Vergessenwerden

Die DSGVO sieht umfassendere Löschpflichten vor als bislang § 35 BDSG. Künftig regelt Art. 17 DSGVO das Recht auf Löschung personenbezogener Daten. Der Verantwortliche muss personenbezogene Daten ohne unangemessene Verzögerung löschen, sofern einer der in Art. 17 Abs. 1 DSGVO genannten Gründe zutrifft. Einer der dort aufgeführten Gründe kann auch darin liegen, dass die betroffene Person nach Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einlegt. Im Falle eines solchen Widerspruchs muss der Verantwortliche diese Daten löschen, sofern keine vorrangigen berechtigten Gründe für die weitere Verarbeitung vorliegen, Art. 17 Abs. 1 lit. c DSGVO.

Wenn ein Verantwortlicher zu löschende personenbezogene Daten öffentlich gemacht hat, muss er andere Verantwortliche, die diese Daten verarbeiten, davon informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu oder aller Kopien oder Replikationen von diesen personenbezogenen Daten verlangt hat, Art. 17 Abs. 2 DSGVO. Art. 17 Abs. 3 DSGVO regelt die Ausnahmen von den Löschpflichten. Diese Ausnahmeregelungen sind insgesamt enger gefasst als im bisherigen Recht. Fehler bei der Verpflichtung zum Löschen von personenbezogenen Daten werden mit Bußgeldern von bis zu 4 Prozent des Umsatzes geahndet.

14. Zweckänderungen und Vereinbarkeit

Grundsätzlich entscheidet der bei der Erhebung von Daten verfolgte Zweck über die mögliche Zulässigkeit ihrer weiteren Verarbeitung. Wenn personenbezogene Daten für einen anderen Zweck verarbeitet werden sollen als den, für den sie erhoben wurden, spricht man von einer Zweckänderung. Im bisherigen Recht waren die Voraussetzungen für die Übermittlung oder Nutzung personenbezogener Daten für einen anderen Zweck vor allem in § 28 Abs. 2 BDSG geregelt. In der Verordnung sind Zweckänderungen künftig in Art. 6 Abs. 3 DSGVO geregelt. Künftig soll die Verarbeitung personenbezogener Daten für einen anderen Zweck als den, zu dem die Daten erhoben werden, zunächst zulässig sein. Voraussetzung ist, dass die betroffene Person in eine solche Zweckänderung eingewilligt hat oder eine Rechtsvorschrift im Sinne von Art. 23 Abs. 1 DSGVO dies erlaubt.

Der in der Praxis wichtigste Anwendungsfall für Zweckänderungen dürfte in einer Verarbeitung für Zwecke liegen, die mit dem ursprünglichen Zweck „vereinbar“ sind. Der Verantwortliche muss diese Vereinbarkeit vor der Zweckänderung prüfen. Kriterien hierfür sind die Verbindung zwischen dem ursprünglichen und dem neuen Zweck, der Kontext der Datenerhebung, die Art der Daten, die möglichen Folgen der beabsichtigten Weiterverarbeitung sowie das Vorhandensein angemessener Garantien. Solche Garantien können etwa in der Verschlüsselung oder Pseudonymisierung personenbezogener Daten liegen.

15. Erleichterter Datenaustausch im Konzern

Die DSGVO stellt weniger strenge Anforderungen an die Übermittlung personenbezogener Daten zwischen Verantwortlichen, die Teil einer Unternehmensgruppe sind. Denn Art. 6 Abs. 1 lit. (f) DSGVO differenziert anders als das BDSG nicht zwischen Datenverarbeitungen für eigene Zwecke und Datenverarbeitungen zur Wahrung berechtigter Interesse Dritter. Die Vorschrift erlaubt die Datenverarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Erwägungsgrund 37 stellt zudem klar, dass Verantwortliche, die Teil einer Unternehmensgruppe sind, ein berechtigtes Interesse haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke zu übermitteln. Dies soll ausdrücklich auch für die Verarbeitung personenbezogener Daten von Kunden und Beschäftigten gelten.

16. Koppelungsverbot bei Einwilligungen

Die Einwilligung nach Art. 7 DSGVO soll durch eine eindeutige Handlung erfolgen, mit der die betroffene Person ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich bekundet, dass sie mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist. Um sicherzustellen, dass die Einwilligung ohne Zwang erfolgt, sollte diese keine rechtliche Handhabe liefern, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht. Verantwortliche dürfen die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung nicht mehr davon abhängig machen, dass die betroffene Person in Datenverarbeitungen einwilligt, die für die Erfüllung dieses Vertrags nicht erforderlich sind.

17. Bewertung der Veränderungen durch die DSGVO

Die DSGVO bringt gegenüber dem BDSG erhebliche Veränderungen. Unternehmen müssen zusätzliche Anforderungen erfüllen. Weitgehend jede neue Vorgabe ist zudem bußgeldbewehrt. Unternehmen sind gut beraten, die notwendigen Veränderungen zeitnah umzusetzen. Dies erfordert vor allem die Anpassung von Arbeitsabläufen und anderen Prozessen, IT- Systemen und Strukturen der Datenverarbeitung. Schwerpunkte liegen dabei auf Transparenz und Dokumentation. Gerade bei größeren Unternehmen wird die Einführung oder Anpassung effektiver Datenschutz Management Systeme hierbei eine zentrale Rolle spielen