1&1 IONOS

White Paper

# Überblick zur neuen EU-Datenschutz-Grundverordnung

Praxisnahe Umsetzungsvorschläge für den deutschen Mittelstand

Internet made in Germany

# 1. Inhaltsverzeichnis

## 2. Zusammenfassung/Checkliste

### Zusammenfassung

Die neue EU-Datenschutz-Grundverordnung gilt für alle Unternehmen in der Europäischen Union ab dem 25.05.2018 und stellt eine Reihe neuer, datenschutzrechtlicher Pflichten auf. Sie gilt nicht nur für EU-Unternehmen, sondern auch für solche mit Sitz in Drittländern, die Waren/Dienstleistungen an EU-Bürger anbieten. Neu sind zunächst die direkte Haftung von Auftragsverarbeitern (IT-Dienstleister), deutlich höhere Bußgelder (bis zu 4% des weltweiten Konzernumsatzes oder EUR 20 Mio.) und die einheitliche Aufsichtsbehörde für Konzerne (One-Stop-Shop). Als wichtige Vorgaben sind insbesondere die Folgenden hinzugekommen: Erweiterte Dokumentations-, Nachweis- und Informationspflichten, Datenschutz-Folgenabschätzung, Recht auf Vergessenwerden, Verarbeitungsverzeichnis, erweiterte Pflichten bei Datenpannen, Privacy by Design/Default, Recht auf Datenübertragbarkeit und Ausweitung der Rechte für Betroffene. Es gelten weiterhin die Grundprinzipien Recht auf informationelle Selbstbestimmung, Verbot mit Erlaubnisvorbehalt, Datenvermeidung/Datensparsamkeit, Zweckbindung und Transparenz.

### Checkliste

Folgende Punkte sollten bis zum 25.05.2018 insbesondere umgesetzt werden:

- Dokumentation sämtlicher Geschäftsprozesse (neue Rechenschaftspflicht)
- Überprüfung der Geschäftsprozesse auf Bestehen von Erlaubnistatbeständen
- Interessenabwägung bei Verarbeitungen auf Grundlage berechtigter Interessen dokumentieren
- Verarbeitungsverzeichnis erstellen bzw. Verfahrensverzeichnis überarbeiten
- Verfahren zur Datenschutz-Folgenabschätzung einrichten
- Einwilligungserklärungen überarbeiten und ggf. neu bei Betroffenen einholen
- Belehrung von Betroffenen neu ausgestalten (Datenschutzerklärung etc.)
- Meldeverfahren bei Datenpannen implementieren
- Datentransfers im Konzern oder zu Drittunternehmen auf Rechtskonformität prüfen
- Verträge zur Auftragsdatenverarbeitung anpassen und mit Dienstleistern neu abschließen
- Löschkonzept entwickeln/überarbeiten und Verfahren bei Anträgen auf Löschung einrichten
- Recht auf Datenübertragbarkeit technisch ermöglichen
- Privacy by Design/Default als Grundsätze in Entwicklungsprozess integrieren
- Datenschutz-Richtlinie für Mitarbeiter überarbeiten

## 3. Einführung

Die neue EU-Verordnung 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, kurz „DSGVO") ist am 24. Mai 2016 in Kraft getreten und entfaltet ab dem 25. Mai 2018 Wirkung. Am 05. Juli 2017 wurde das deutsche Umsetzungsgesetz zur DSGVO, das neue Bundesdatenschutzgesetz (kurz „BDSG-neu") im Bundesgesetzblatt verkündet; es tritt ebenfalls am 25. Mai 2018 in Kraft. Die rechtlichen Grundlagen zum neuen Datenschutzrecht liegen daher vor.

Viele Unternehmen, gerade im Mittelstand, haben sich dem Thema noch nicht angenommen. Sie gehen davon aus, dass es auch Anfang 2018 noch rechtzeitig ist, mit der Umsetzung zu beginnen. Angesichts der Tatsache, dass alle Geschäftsprozesse und Datentransfers analysiert, alle datenschutzbezogenen Dokumente überarbeitet und neue, technische Verfahren implementiert werden müssen, sollten Unternehmen jedoch bei der Umsetzung der neuen Vorgaben keine Zeit verlieren. Dieser Leitfaden gibt auf 17 Seiten einen Überblick über die wichtigsten Inhalte der DSGVO und praktische Ratschläge zur Umsetzung im Unternehmen.

## 4. Anwendungsbereich

Die neue DSGVO gilt einerseits für Unternehmen, die im Rahmen der Tätigkeit einer Niederlassung in der Europäischen Union personenbezogene Daten verarbeiten (**Niederlassungsprinzip**). Andererseits findet sie jedoch auch Anwendung auf Unternehmen, die zwar innerhalb der EU keine Niederlassung haben, jedoch ihre Waren und Dienstleistungen hier ansässigen Personen Seite 5 White Paper Überblick zur neuen EU-Datenschutz-Grundverordnung anbieten (**Marktortprinzip**) oder diese hier beobachten. Dies sieht Art. 3 DSGVO[1] so vor. Unternehmen wie Google oder Facebook würden daher auch ohne Niederlassung innerhalb der EU unter die DSGVO fallen, da sie sich mit ihren Angeboten auch an EU-Bürger richten. Derartige Unternehmen haben nach Art. 27 einen Inlandsvertreter zu bestellen als Ansprechpartner für Betroffene und Aufsichtsbehörden.

[1] Alle nachfolgenden Artikel ohne Benennung der betreffenden Gesetzesgrundlage sind solche der DSGVO.

## 5. Zulässigkeit der Datenverarbeitung

### a) Verbot mit Erlaubnisvorbehalt

Die DSGVO geht, wie auch zuvor die EU-Datenschutzrichtlinie 95/46/EG und das Bundesdatenschutzgesetz, davon aus, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn eine Erlaubnis vorliegt (Verbot mit Erlaubnisvorbehalt). Unternehmen müssen daher sicherstellen, dass für die betreffende Verarbeitung personenbezogener Daten entweder eine Einwilligung des Betroffenen oder eine **gesetzliche Erlaubnis** vorliegt. Eine solche gesetzliche Erlaubnis kann sich gemäß Art. 6 insbesondere aus dem Erfordernis zur Vertragserfüllung oder auf Grundlage eines berechtigten Interesses ergeben.
Die Wirksamkeit einer **Einwilligung** regelt Art. 7. Hiernach muss das Unternehmen das Bestehen der Einwilligung nachweisen. Sie ist allerdings nun, im Gegensatz zum alten BDSG, nicht mehr zwingend in Schriftform abzugeben. Man kann daher die Einwilligung zukünftig **auch elektronisch** oder anderweitig einholen, sollte jedoch beachten, dass die Nachweispflicht hierfür beim Unternehmen liegt. Verboten ist es, die Vertragserfüllung von einer Einwilligung abhängig zu machen, soweit die betreffenden Daten für die eigentliche Vertragserfüllung nicht erforderlich sind (**Kopplungsverbot**).

---

**Praxistipp:** *Bereits vorhandene Einwilligungen behalten nach Erwägungsgrund 171 ihre Gültigkeit, soweit bislang zulässig. Da Art. 13 jedoch deutlich umfassendere Informationspflichten vorsieht, sollten alle Einwilligungsvorlagen dahingehend überarbeitet werden.*

### b) Gesetzliche Ermächtigung

Ohne Einwilligung ist eine Verarbeitung personenbezogener Daten nur mit gesetzlicher Ermächtigung zulässig (Art. 6). Neben einer Erforderlichkeit zur Vertragserfüllung (Frage: Ist die Verarbeitung der betreffenden, personenbezogenen Daten zur Erfüllung des Vertrages notwendig?) und auf **Grundlage berechtigter Interessen** kommen hier Ausnahmefälle in Betracht, z.B. zur 1 Alle nachfolgenden Artikel ohne Benennung der betreffenden Gesetzesgrundlage sind solche der DSGVO. Seite 6 White Paper Überblick zur neuen EU-Datenschutz-Grundverordnung Erfüllung rechtlicher Verpflichtungen, zum Schutz lebenswichtiger Interessen oder zur Wahrnehmung öffentlicher Aufgaben. Wichtig ist die Verarbeitung auf Grundlage berechtigter Interessen. Diese Variante wird zukünftig die wohl größte Rolle beim Datenschutz spielen. Unternehmen müssen im Rahmen der Interessenabwägung feststellen, ob nicht schutzwürdige Interessen der betroffenen Person vorliegen, die höher wiegen, also die eigenen, berechtigten Interessen zur Datenverwendung. Nur falls dies nicht der Fall ist, dürfen die betreffenden Daten verarbeitet werden. Die Interessenabwägung ist zu dokumentieren, denn die Datenschutzbehörden werden beim nächsten Audit um Vorlage dieser Dokumentation bitten. Wichtig ist auch das (neue) Widerrufsrecht nach Art. 21 DSGVO, das Betroffene bei Verarbeitung

auf Grundlage berechtigter Interessen in Anspruch nehmen können, wobei hier die Ausnahme in § 36 BDSG-neu in Fällen öffentlichen Interesses zu berücksichtigen ist.

**Praxistipp:** *Die Dokumentation der Interessenabwägung war bislang zwar ratsam, jedoch nicht zwingend notwendig. Dies ist daher eine mühsame, jedoch wichtige, neue Aufgabe bei der Umsetzung der DSGVO in allen Fällen, wo die Verarbeitung personenbezogener Daten nicht auf die Vertragserfüllung oder Einwilligung gestützt werden kann.*

### c) Sonderfall: Sensible Daten

Für den Fall der Verarbeitung besonders sensibler Daten wurden in Art. 9 Sonderregelungen getroffen. Hiernach ist die Verarbeitung von Daten, aus denen die rassistische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung nur dann zulässig, wenn bestimmte Voraussetzungen vorliegen. Beispielhaft ist dies der Fall bei Vorliegen einer Einwilligung oder Erforderlichkeit der ärztlichen Behandlung. Das deutsche Recht sieht in § 22 BDSG-neu weitere Zulässigkeitsregelungen für sensible Daten vor, beispielsweise bei Erforderlichkeit der Verarbeitung nach dem Recht des Sozialschutzes (SGB). Unter Anführung von Beispielsfällen ist in Abs. 2 dieser Vorschrift zudem geregelt, dass angemessene technische und organisatorische Maßnahmen gemäß dem Stand der Technik zu treffen sind, um die sensiblen Daten besonders zu schützen; auch die §§ 27 und 28 BDSG-neu sind zu beachten.

**Praxistipp:** *Vermeiden Sie – soweit betrieblich möglich – die Verarbeitung sensibler Daten. Hier werden die Aufsichtsbehörden hellhörig und verlangen eine saubere Dokumentation. Falls doch notwendig, stützen Sie die Verarbeitung solcher Daten stets auf die Einwilligung, die allerdings sehr transparent formuliert werden muss.*

### d) Sonderfall: Arbeitnehmerdaten

Der Beschäftigtendatenschutz hat in der DSGVO keine gesonderte Berücksichtigung erfahren. Im BDSG-neu hat der deutsche Gesetzgeber jedoch in § 26 Regelungen getroffen, die auf dem bisherigen § 32 BDSG aufbauen. Zulässig ist die Verarbeitung daher weiterhin bei Erforderlichkeit der Vertragserfüllung sowie zur Aufdeckung von Straftaten. Neu ist die Zulässigkeit bei Erforderlichkeit der Erfüllung von Betriebsvereinbarungen oder Tarifverträgen. Zudem wird die Einwilligung im Arbeitsverhältnis in § 26 Abs. 2 BDSG-neu erstmalig geregelt. Hiernach erfüllt die Einwilligung des Arbeitnehmers grundsätzlich nur dann die notwendige Freiwilligkeit, wenn dieser einen rechtlichen oder wirtschaftlichen Vorteil erhält oder mit dem Arbeitgeber gleichgelagerte Interessen verfolgt werden. Die Einwilligung bedarf grundsätzlich der Schriftform.

**Praxistipp:** *Vermeiden Sie im Arbeitsverhältnis die Einwilligung von Mitarbeitern. Diese kann jederzeit widerrufen werden, soweit sie nicht per Betriebsvereinbarung abgegeben wird. Stützen Sie die Verarbeitung lieber (soweit möglich) auf eine Erforderlichkeit zur Vertragserfüllung oder sorgen Sie für eine wirksame Anonymisierung der betreffenden Mitarbeiterdaten, was den Datenschutz aushebelt.*

### e) Sonderfall: Videoüberwachung

Die Videoüberwachung wird in der DSGVO nicht ausdrücklich geregelt. Es gilt daher für die Rechtmäßigkeit mangels Einwilligung die Generalklausel des Art. 6 Abs. 1 lit. f), also die Verarbeitung auf Grundlage berechtigter Interessen. Vor Installation einer Videoüberwachung ist daher eine dokumentierte Interessenabwägung vorzunehmen und infolge der Risiken für die Betroffenen auch eine – ebenfalls dokumentierte – nach Art. 35 vorgeschriebene Datenschutz-Folgenabschätzung (siehe hierzu Ziffer 5c unten). Die einzelnen Videokameras sind zudem im Verarbeitungsverzeichnis anzuführen. Die Videoüberwachung ist daher datenschutzrechtlich mit einem erheblichen Umsetzungsaufwand verbunden, so dass Aufsichtsbehörden hohe Anforderungen stellen werden. Für den öffentlich zugänglichen Bereich ist § 4 BDSG-neu zu beachten, wonach die Videoüberwachung für Unternehmen nur dann zulässig ist, wenn dies zur Wahrnehmung des Hausrechts oder berechtigter Interessen erforderlich ist, letzteres nur bei positiver Interessenabwägung (siehe hierzu oben Ziffer 3 lit. c). Neu sind auch die erweiterten Informationspflichten: Sowohl die Videoüberwachung selbst, als auch Name und Kontaktdaten des Unternehmen sind an geeigneter Stelle zum frühestmöglichen Zeitpunkt erkennbar zu machen.

**Praxistipp:** *Die Videoüberwachung erfordert „Datenschutz für Fortgeschrittene". Lassen Sie hier die Profis ran und sorgen für eine sauber dokumentierte Datenschutz-Folgenabschätzung.*

### f) Sonderfall: Scoring

Das Scoring (Festlegung der Wahrscheinlichkeit für z.B. Kreditausfälle) ist in der DSGVO nicht ausdrücklich geregelt. § 31 BDSG-neu enthält hierzu jedoch nationale Sonderregeln, die als Konkretisierung zur Interessenabwägung (siehe Ziffer 3 lit. c  oben) zu verstehen sind. Insbesondere werden hier Negativ-Merkmale definiert, die ein Scoring unzulässig machen, beispielsweise bei alleiniger Berücksichtigung von Anschriftendaten.

### g) Sonderfall: Werbung

Auch die Verarbeitung personenbezogener Daten zu Werbezwecken ist nicht ausdrücklich geregelt. Es ist daher – soweit keine Einwilligung vorliegt – wiederum eine Interessenabwägung vorzunehmen. Erwägungsgrund 47 der DSGVO erkennt bei der Direktwerbung ein „berechtigtes Interesse" ausdrücklich an, so dass bei der Dokumentation der Interessenabwägung insbesondere auf

die schutzwürdigen Interessen der Betroffenen einzugehen ist. Erneut ist das Widerspruchsrecht der Betroffenen nach Art. 21 (hier Abs. 2) zu beachten, dies gilt auch für die notwendigen Informationspflichten nach den Artikeln 13 und 14 (siehe unten Ziffer 5 lit. b).

**Praxistipp:** *Achten Sie bei der Werbung auch auf § 7 UWG, also das Wettbewerbsrecht. Hier sind die konkreten Vorgaben für Werbemaßnahmen geregelt.*

### h) Sonderfall: Big Data

Die Verarbeitung auf Grundlage berechtigter Interessen muss auch beim Thema „Big Data" herhalten, denn im Regelfall sind personenbezogene Daten, die aufgrund einer Einwilligung oder einer vertraglichen Erforderlichkeit erhoben wurden, der Zweckbindung unterworfen (Art. 5 Abs. 1 lit. b). Sie dürfen daher nicht für „andere Zwecke" verarbeitet werden, soweit hierfür keine Einwilligung vorliegt. Der Einsatz von Big Data erfordert somit eine umfassende, dokumentierte Interessenabwägung; besser wäre eine Anonymisierung oder Pseudonymisierung der betreffenden Daten. Auch das Kopplungsverbot nach Art. 5 Abs. 4 und bei Erhebung via Internet die ePrivacy-Verordnung (Tracking nur noch mit Opt-In) sind zu beachten.

**Praxistipp:** *Die interessanten Big-Data-Auswertungen lassen sich durch das Gesetz zumeist nicht rechtfertigen, auch nicht auf Grundlage von berechtigten Interessen. Sorgen Sie daher bestenfalls dafür, dass die Big-Data-Systeme ausschließlich (zuvor wirksam) anonymisierte Daten verarbeiten.*

## 6. Auftragsverarbeitung unter Berücksichtigung des Cloud-Computing

### a) Allgemeines

Zur Auftragsverarbeitung baut die DSGVO auf denselben Grundlagen auf, wie auch schon das alte BDSG. Typische Fälle der Auftragsverarbeitung sind Cloud-Computing, IT-Outsourcing, die Auslagerung von Daten zu Zwecken der Aktenvernichtung oder die Fernwartung durch IT-Dienstleister mit Zugriff auf interne, personenbezogene Daten. Hinzugekommen sind jedoch u.a. die Anhebung der technischen/organisatorischen Anforderungen auf den Stand der Technik sowie umfassende Mitwirkungspflichten zu Meldepflichten und Datenschutz-Folgeabschätzung.

### b) Pflichten

Die Zulässigkeit der Auftragsverarbeitung ist nun in Art. 28 geregelt. Das Unternehmen hat hiernach zunächst eine Prüfung der Geeignetheit eines Auftragsverarbeiters daraufhin vorzunehmen, ob dieser hinreichend Garantien dafür bietet, dass dieser geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz getroffen hat. Als Beleg hierfür kommt etwa eine genehmigte Verhaltensregel nach Art. 40 oder eine Zertifizierung nach Art. 42 in Betracht. Zudem muss mit dem Auftragsverarbeiter ein Vertrag über die weisungsgebundene Tätigkeit geschlossen werden, der schriftlich oder (und das ist neu) in elektronischer Form zu fassen ist. Die notwendigen Inhalte des Vertrages ergeben sich aus Art. 28 Abs. 3. Subunternehmen darf der Auftragsverarbeiter künftig nur noch dann einsetzen, wenn das Unternehmen hierzu vorher ausdrücklich seine Genehmigung erteilt hat. Der Auftragsverarbeiter haftet jetzt erstmals selbst für Datenschutzverletzungen, wie sich aus Art. 28 Abs. 10 ergibt; dies gilt auch für Bußgelder (Art. 82). Zudem hat der Auftragsverarbeiter nun auch ein Verarbeitungsverzeichnis für alle Kategorien seines Auftrages zu führen, das auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen ist (Art. 30 Abs. 2). Bei Datenpannen hat der Auftragsverarbeiter nach Art. 33 Abs. 2 eigene Meldepflichten gegenüber dem Unternehmen, deren Verstoß zu Bußgeldern führen kann (Art. 83 Abs. 4 ff.).

---

**Praxistipp:** *Es gibt noch immer viele (auch große) Unternehmen, die beim Thema Auftragsverarbeitung ganz am Anfang stehen und noch nicht einmal schriftliche ADV-Verträge mit ihren Dienstleistern und freien Mitarbeitern geschlossen haben, obwohl diese Systemzugriff haben. Denken Sie daran, dass die Aufsichtsbehörden zuerst beim Thema ADV ansetzen und sehr häufig auch fündig werden. Dieser Punkt gehört ganz oben auf Ihre Prioritätsliste. Beachten Sie, dass ADV nicht nur bedeutet, dass Daten aktiv nach außen gesendet werden (wie beim Cloud-Computing), sondern auch der passive Datenzugriff von außen (z.B. Fernwartung des Softwareherstellers, Remotezugriff des freien Mitarbeiters) einen Datentransfer darstellt, der rechtskonform gestaltet werden muss. Gerade global agierende Konzerne sollten auf ihre Sorgfaltspflichten beim internationalen Datentransfer achten (siehe unten Ziffer 6 lit. c).*

Der Austausch personenbezogener Daten im Konzern ist aus Sicht vieler deutscher Unternehmen privilegiert („Konzernprivileg"), bedarf also keiner besonderer Vorkehrungen. Diese Annahme ist jedoch falsch. Sowohl das alte BDSG, als auch die neue DSGVO sehen eine solche Privilegierung nicht vor. Damit gelten für den Datenaustausch zwischen Konzernunternehmen dieselben, rechtlichen Vorgaben, wie zwischen x-beliebigen Unternehmen. Möchte etwa eine französische Konzernmutter auf Mitarbeiterdaten der deutschen Konzerntochter zugreifen, dann stellt dies eine Übermittlung personenbezogener Daten von deutschen auf französische Server dar und bedarf der Einwilligung der Betroffenen oder aber eine gesetzliche Erlaubnis (siehe hierzu oben Ziffer 3 lit. c). Soweit hierbei auf eine Verarbeitung auf Grundlage berechtigter Interessen zurückgegriffen wird, kann allerdings Erwägungsgrund 48 helfen, wonach der Konzerntransfer grundsätzlich als „berechtigtes Interesse" anerkannt wird.

**Praxistipp:** *Es gibt bislang nur wenig Konzerne, die es beim Thema Datentransfer zur Compliance geschafft haben, gerade im internationalen Bereich. Überprüfen Sie daher alle Datentransfers im Konzern und schaffen (z.B. durch Standardvertragsklauseln, siehe nachfolgender Punkt) die rechtlichen Grundlagen für die Datenübermittlung.*

### c) Datenübermittlung in Drittländer

Auch nach der neuen DSGVO bedarf es zur Datenübermittlung an Stellen außerhalb der EU eines dort bestehenden, angemessenen Datenschutzniveaus (Art. 44 ff.). Unternehmen dürfen daher keine Cloud-Provider mit Serverstandort außerhalb der EU beauftragen, soweit nicht besondere Voraussetzungen vorliegen. Hier kommt einerseits eine **Angemessenheitsentscheidung** der EU-Kommission in Betracht, die heute für die Länder Andorra, Argentinien, Kanada, Schweiz, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay gilt. In diese Länder darf ein Datentransfer daher ohne weiteres stattfinden, soweit das Verbot mit Erlaubnisvorbehalt beachtet wird (siehe oben Ziffer 3 lit.a). Darüber hinaus kann ein angemessenes Datenschutzniveau im EU-Ausland durch sog. **Standardvertragsklauseln** erreicht werden, die von der Kommission (oder erstmals auch von Aufsichtsbehörden) freigegeben und vom Datenempfänger unterzeichnet werden. Möglich ist die Erreichung eines angemessenen Datenschutzniveaus konzernweit auch durch interne Datenschutzvorschriften (Art. 47), sog. **Binding Corporate Rules**. Hierbei werden alle Konzernunternehmen datenschutzrechtlich auf den Stand der DSGVO-Vorgaben gebracht und das Gesamt-Richtlinienwerk von der zuständigen Aufsichtsbehörde anschließend überprüft. Sind aus deren Sicht die Anforderungen erfüllt, genehmigt diese das Richtlinienwerk, was für das notwendige, angemessene Datenschutzniveau beim Konzernunternehmen im Drittland sorgt. Neu sind dagegen sog. **Verhaltensregeln** (Codes of Conducts) und **Zertifizierungen** (Art. 46 Abs. 2 lit. e/f), welche die Aufsichtsbehörden genehmigen können und die fortan als Rechtsgrundlage für die Schaffung des notwendigen, angemessenen Datenschutzniveaus dienen.

**Praxistipp:** *Zu diesem Thema gehört auch das sog. EU-US-Privacy-Shield. Die EU-Kommission hat hierdurch alle beigetretenen US-Unternehmen quasi mit einem angemessenen Datenschutzniveau ausgestattet. Denken Sie jedoch daran, dass sich (Stand August 2017) sowohl das Privacy Shield, als auch die Standardvertragsklauseln derzeit in der gerichtlichen Prüfung befinden und insbesondere letztere möglicherweise in 2017 oder 2018 für ungültig erklärt werden könnten, was dann für akuten Handlungsbedarf sorgt, soweit Sie personenbezogene Daten in den USA oder anderen Drittstaaten speichern.*

## 7. Organisatorische Maßnahmen

### a) Dokumentationspflichten

Unternehmen haben durch die neue DSGVO umfangreiche Dokumentationspflichten auferlegt bekommen. So ist beispielsweise nach Art. 30 ein (zumindest elektronisches) **Verarbeitungsverzeichnis** zu führen, wo u.a. Kontaktdaten des Unternehmen, Zweck der jeweiligen Verarbeitung, Beschreibung der Kategorien von Betroffenen und Daten, Übermittlungen in Drittländer oder internationale Organisationen, Löschungsfristen oder eine Beschreibung technischer sowie organisatorischer Maßnahmen aufgeführt werden. Im Falle der Videoüberwachung ist diese in jedem Fall aufzunehmen (§ 4 BDSG-neu). Unternehmen ohne regelmäßige Verarbeitung von personenbezogenen Daten mit weniger als 250 Mitarbeitern sind allerdings nach Art. 30 Abs. 5 von der Pflicht zur Führung des Verzeichnisses ausgenommen. Diese Ausnahme dürfte allerdings nur wenige deutsche Unternehmen betreffen, da eine regelmäßige Verarbeitung personenbezogener Daten heute Standard geworden ist (z.B. bei eigener Kunden- oder Mitarbeiterdatenbank). Zudem trifft Unternehmen nach Art. 5 Abs. 2 eine sog. **Rechenschaftspflicht** („Accountability"). Im Gegensatz zur bisherigen Regelung im BDSG haben Unternehmen nun die Pflicht, die Einhaltung der DSGVO-Grundsätze in Art. 5 Abs. 1 gegenüber den Aufsichtsbehörden nachzuweisen, insbesondere die „Rechtmäßigkeit der Verarbeitung", was faktisch einer Beweislastumkehr gleichkommt.

**Praxistipp:** *Zu diesem Thema gehört auch das sog. EU-US-Privacy-Shield. Die EU-Kommission hat hierdurch alle beigetretenen US-Unternehmen quasi mit einem angemessenen Datenschutzniveau ausgestattet. Denken Sie jedoch daran, dass sich (Stand August 2017) sowohl das Privacy Shield, als auch die Standardvertragsklauseln derzeit in der gerichtlichen Prüfung befinden und insbesondere letztere möglicherweise in 2017 oder 2018 für ungültig erklärt werden könnten, was dann für akuten Handlungsbedarf sorgt, soweit Sie personenbezogene Daten in den USA oder anderen Drittstaaten speichern.*

## b) Informationspflichten

Betroffene müssen nach Art. 13 bei Erhebung von personenbezogenen Daten umfassend über die geplante Verwendung **informiert** werden, insbesondere über Kontaktdaten des Unternehmens, Zweck bzw. Rechtsgrundlage der Verarbeitung, ggf. unter Darlegung des „berechtigten Interesses", eine mögliche Weiterleitung der Daten in Drittländer mit Rechtsgrundlage der Übermittlung, die Dauer der Speicherung bzw. die Kriterien der Festlegung oder das Bestehen von Betroffenenrechten. Werden die Daten nicht beim Betroffenen direkt erhoben, so ist nach Art. 14 zusätzlich noch anzugeben, aus welcher Quelle die Daten kommen und welche Kategorien von personenbezogenen Daten betroffen sind. Obige Informationspflichten bestehen u.a. dann nicht, wenn der Betroffene bereits hierüber verfügt oder bei direkter Erhebung eine Informierung unmöglich wäre bzw. einen unverhältnismäßigen Aufwand erfordert. Weitere Ausnahmetatbestände sind in §§ 32 und 33 BDSG-neu geregelt. **Formell** ist bei den Informationspflichten zu beachten, dass die Informationen präzise, leicht zugänglich sowie in klarer und einfacher Sprache abgefasst sind (siehe Art. 12). Bei der Zielgruppe Kinder muss die Information in kindgerechter Sprache erfolgen. Grundsätzlich ist die Schriftform zu wählen, im Internet ist auch elektronische Form zulässig; nur im Ausnahmefall darf mündlich informiert werden. Belehrungen auf bestehende Widerspruchsrechte sind nach Art. 21 Abs. 4 allerdings gesondert aufzuführen. Zeitlich muss die Information, soweit möglich, nach Art. 14 Abs. 3 direkt bei der Erhebung erfolgen, andernfalls innerhalb angemessener Frist (max. 1 Monat) nach Erhebung.

---

**Praxistipp:** *Alle datenschutzrechtlichen Belehrungstexte müssen überarbeitet werden, denn die neuen Artikel 13 und 14 sehen neue Anforderungen vor. Denken Sie daran, dass der Datenschutzbeauftragte nach Art. 39 nur zur „Überwachung, Unterrichtung und Beratung" verpflichtet ist, nicht jedoch zur Ausfertigung der datenschutzrelevanten Dokumente. Dies ist Sache der Geschäftsführung, die ggf. an die Rechtsabteilung delegieren kann.*

## c) Datenschutz-Folgenabschätzung

Art. 35 der DSGVO sieht eine Pflicht zur Datenschutz-Folgenabschätzung vor für den Fall, dass eine konkret durchgeführte Verarbeitungstätigkeit ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringt. Ein solches hohes Risiko ist nach Erwägungsgrund 75 etwa anzunehmen bei Diskriminierung, Identitätsdiebstahl, finanziellem Verlust, Rufschädigung oder Profilbildung mit Standortdaten. Die Aufsichtsbehörden werden hierzu eine Liste von Verarbeitungstätigkeiten vorlegen, bei denen eine Abschätzung im Regelfall stattzufinden hat (Blacklist). Eine Datenschutz-Folgenabschätzung (vormals „Vorabkontrolle") muss neben einer systematischen Beschreibung der Verarbeitungsvorgänge auch die Zwecke der Verarbeitung umfassen. Auf dieser Grundlage sind dann die Interessen des Unternehmens an der jeweiligen Verarbeitung (z.B. Einführung

von Videoüberwachung) abgewogen werden mit den Interessen der betroffenen Person an einem Unterlassen dieser Verarbeitung. Diese Abwägung ist zu dokumentieren.

**Praxistipp:** *Lesen Sie zur konkreten Vorgehensweise der Datenschutz-Folgenabschätzung die praktischen Hinweise der Aufsichtsbehörden, z.B. in Bayern oder Baden-Württemberg. Diese enthalten häufige gute Praxishilfen.*

### d) Meldepflichten bei Datenpannen

Datenpannen sind jederzeit möglich. Sicherheitslücken von Webanwendungen werden ausgenutzt, um einen Vollzugriff auf Unternehmenssysteme zu ermöglichen oder Festplatten werden aus dem Serverraum gestohlen. Während heute nach § 42a BDSG nur sensible Daten von der Meldepflicht betroffen sind, müssen Unternehmen nach Art. 33 und 34 nun auch bei regulären, personenbezogenen Daten die Meldepflichten beachten. Eine solche Meldung an die zuständige Aufsichtsbehörde hat hiernach bei **jedem Datenschutzverstoß** zu erfolgen, es sei denn, die Datenpanne führt „voraussichtlich" nicht zu einem Risiko für den Betroffenen. Besteht allerdings ein „hohes Risiko" für dessen Rechte und Freiheiten, ist auch der Betroffene selbst zu informieren. Dies gilt nicht, wenn geeignete technische und organisatorische Maßnahmen getroffen wurden, um zukünftige, gleichartige Datenschutzverstöße zu verhindern oder wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden und diese das hohe Risiko eliminiert haben. **Zuständige Aufsichtsbehörde** ist gemäß dem neuen Prinzip **One-Stop-Shop** (Art. 56) diejenige am Sitz der „Hauptniederlassung" des Unternehmens, die dann grundsätzlich für alle datenschutzrechtlichen Konzernbelange Ansprechpartner ist. Die Meldung hat unverzüglich, spätestens innerhalb von 72 Stunden zu erfolgen und muss gewisse Angaben wie Art der Datenpanne, Kategorien von betroffenen Daten, Anzahl der Betroffenen und der Datensätze enthalten.

**Praxistipp:** *Erstellen Sie ein Merkblatt mit Prozessbeschreibung für Ihre Mitarbeiter, damit diese bei Datenpannen sofort wissen, was zu tun ist.*

## 8. Technische Maßnahmen

### a) Technische Anforderungen

Der technische Datenschutz ist in Art. 32 geregelt. Vorrangig geht es hier um die klassischen Schutzziele der IT-Sicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit, die bereits im alten BDSG Berücksichtigung fanden. Neu ist das Schutzziel der sog. „Belastbarkeit der Systeme"; diese müssen so widerstandsfähig sein, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gewährleistet ist, auch bei Cyberangriffen von außen. Umzusetzen sind nach Art. 32 geeignete technische und organisatorische Maßnahmen zur Erfüllung der datenschutzrechtlichen Vorgaben unter Berücksichtigung u.a. des Standes des Technik und der Implementierungskosten.

---

**Praxistipp:** *Bis die Aufsichtsbehörden konkrete Vorgaben zur praktischen Umsetzung von Art. 32 veröffentlicht haben, können sich Unternehmen derweil an der VDS-Richtlinie VdS 3473 orientieren, die auf 38 Seiten eine gute Übersicht der notwendigen Maßnahmen gibt.*

### b) Zertifizierung

Bei den technischen Anforderungen stellt sich die Frage, wie Unternehmen deren Erfüllung nachweisen können, insbesondere bei Berücksichtigung der Rechenschaftspflicht nach Art. 5 Abs. 2. Art. 32 Abs. 3 gibt hier Hilfestellung. Hiernach können etwa genehmigte Verhaltensregeln oder Zertifizierungsverfahren als Faktor herangezogen werden, um die Erfüllung nachzuweisen. Derartige Verhaltensregeln oder Zertifizierungsverfahren gibt es heute (Stand August 2017) noch nicht. Es ist jedoch davon auszugehen, dass diese alsbald nach Wirksamwerden der DSGVO entwickelt und von den Aufsichtsbehörden genehmigt werden, so dass in Zukunft ein Konstrukt zum Nachweis der Anforderungen aus Art. 32 zur Verfügung steht. Die Zulassungsanforderungen an Zertifizierungsstellen sind in § 39 BDSG-neu geregelt.

---

**Praxistipp:** *Beobachten Sie die Geschehnisse der kommenden Monate. Es ist davon auszugehen, dass vielleicht noch in 2017 erste Zertifizierungsverfahren zur DSGVO angeboten werden. Eine aktuelle Übersicht zu Zertifikaten nach BDSG finden Sie auf der Website der Stiftung Datenschutz.*

### c) Datenübertragbarkeit

Den Betroffenen steht nach Art. 20 das neue Recht der Datenübertragbarkeit zu. Sie können daher die sie betreffenden, personenbezogenen Daten vom Unternehmen in einem strukturierten, gängigen und maschinenlesbaren Format herausverlangen. Zudem haben sie das Recht, diese Daten direkt an den neuen Anbieter übermitteln zu lassen. Die technischen Anforderungen an dieses Format sind noch nicht eindeutig festgelegt; es ist jedoch damit zu rechnen,

dass die Aufsichtsbehörden rechtzeitig vor Mai 2018 entsprechende Vorgaben veröffentlichen werden.

**Praxistipp:** *An dieser Stelle müssen Sie Ihre IT-Systeme anpassen. Personenbezogene Kunden- oder Mitarbeiterprofile müssen ab Mai 2018 technisch so gestaltet sein, dass sie sehr kurzfristig herausgegeben werden können. Bei Inanspruchnahme von Providern sollten Sie hier Lock-In-Effekte vermeiden und das Recht zur Datenübertragbarkeit ausdrücklich mit in die Verträge einbeziehen.*

### d) Privacy by Design, Privacy by Default

Zukünftig müssen Unternehmen bereits im Stadium der Produktentwicklung datenschutzrechtliche Vorgaben beachten. Art. 25 sieht vor, dass schon „zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung", also im Entwicklungsstadium, notwendige technische und organisatorische Maßnahmen zur Einhaltung des Datenschutzes getroffen werden („Privacy by Design"). Gibt es im Produkt Einstellungsmöglichkeiten, so ist diejenige Voreinstellung zu wählen, die für die Erfüllung des jeweiligen Verarbeitungszwecks erforderlich ist („Privacy by Default"). Hier ist das Prinzip der Datensparsamkeit zu berücksichtigen. Sowohl Privacy by Design als auch Privacy by Default wurden in der DSGVO (und das ist neu) bußgeldbewährt ausgestaltet, was ihre Bedeutung aus Sicht der EU-Kommission unterstreicht.

**Praxistipp:** *Schulen Sie Ihre Entwicklungsabteilung und stellen dieser eine enge Verbindung zur Datenschutzabteilung zur Verfügung. Die Aufsichtsbehörden werden zukünftig genau prüfen, ob Sie schon im Entwicklungs- und Produktionsprozess datenschutzrechtliche Grundsätze implementiert haben oder nicht.*

## 9. Rechte der Betroffenen

Die Betroffenenrechte werden durch die DSGVO gestärkt. Diese erhalten nicht nur jederzeit Einblick in ihre Daten, sondern können auch aktiv Einfluss auf diese Daten nehmen. So besteht nach Art. 13 und 14 für Unternehmen die Pflicht, die Betroffenen vor Erhebung der Daten umfassend darüber aufzuklären, was genau mit diesen Daten geschehen wird (Informationspflicht, siehe hierzu oben Ziffer 5 lit. b). Sind die Daten des Betroffenen bereits beim Unternehmen erhoben, so steht ersterem ein unentgeltliches Auskunftsrecht nach Art. 15 (siehe Ausnahmen nach § 34 BDSG-neu) sowie ein Recht auf Berichtigung von unrichtigen Daten nach Art. 16 zu. Ist die Speicherung der betreffenden Daten nicht mehr notwendig, wurde eine Einwilligung widerrufen oder erfolgt die Verarbeitung unrechtmäßig, so kann der Betroffene nach Art. 17 auch die Löschung verlangen (siehe hierzu die Ergänzungen nach § 35 BDSG-neu).

Das Unternehmen hat dann grundsätzlich auch diejenigen anderen Unternehmen hierüber zu informieren, an die er die betreffenden Daten zuvor weitergegeben hat (Recht auf Vergessen, Art. 17 Abs. 2). Statt der Löschung kommt auch eine Sperrung nach Art. 18 in Betracht, etwa wenn die betreffenden Daten aus gesetzlichen Aufbewahrungsgründen noch aufbewahrt werden müssen. Schließlich besteht zugunsten des Betroffenen auch das Widerspruchsrecht nach Art. 21, etwa wenn die Datenverarbeitung auf Grundlage berechtigter Interessen erfolgt. Die obigen Rechte sind gemäß Art. 12 Abs. 3 grundsätzlich innerhalb von einem Monat nach Eingang der jeweiligen Anfrage zu erfüllen.

**Praxistipp:** *Die Betroffenen erhalten umfassende Rechte und dürfen sogar eine Antwort des betreffenden Unternehmens innerhalb von einem Monat erwarten. Schaffen Sie daher intern Systeme, die ermöglichen, dass Anfragen von Betroffenen zum Thema Datenschutz sehr kurzfristig und mit wenig Personalaufwand beantwortet werden können. Bei Inanspruchnahme von Providern ist auch hier vertraglich sicherzustellen, dass die Mitwirkungspflichten bei Anfragen von Betroffenen umgesetzt werden.*

## 10. Datenschutzbeauftragter

Die DSGVO sieht nur im Ausnahmefall die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten („DSB“) vor und zwar u.a. für den Fall, dass die umfangreiche oder systematische Überwachung von Personen zur Kerntätigkeit des Unternehmens gehört. Allerdings hat der deutsche Gesetzgeber hier zulässigerweise eine eigene Regelung getroffen und in § 38 BDSG-neu festgelegt, dass alle Unternehmen mit mindestens 10 Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (z.B. weil sie einem eigenen E-Mail-Account arbeiten), einen DSB bestellen müssen. Der DSB ist auf Grundlage seiner beruflichen Qualifikation und seines Fachwissens auf dem Gebiet des Datenschutzrechtes sowie seiner Fähigkeit, die gesetzlichen Aufgaben zu erfüllen, zu bestellen. Hierbei sind (und dies ist neu) seine Kontaktdaten zu veröffentlichen und auch der Aufsichtsbehörde mitzuteilen. Der DSB untersteht direkt der höchsten Managementebene und darf aufgrund seiner Position nicht abberufen oder benachteiligt werden.

**Praxistipp:** *Der Datenschutzbeauftragte muss nicht zwingend aus dem eigenen Unternehmen kommen. Es kann auch ein Beratungsunternehmen oder eine Rechtsanwaltskanzlei als sog. „externer Datenschutzbeauftragter“ bestellt werden. Sie lagern damit auch die Haftung für die Bereiche „Überwachung, Unterrichtung und Beratung“ auf den Dienstleister aus, was eigene Risiken reduziert.*

## 11. Sanktionen

Den Aufsichtsbehörden stellt die DSGVO eine breite Palette an Sanktionsmöglichen zur Verfügung. Im Gegensatz zum alten BDSG sind die Aufsichtsbehörden grundsätzlich angehalten, bei Verstoß gegen Datenschutzvorgaben auch Sanktionen zu erlassen (Erwägungsgrund 148), es sei denn, es handelt sich lediglich um geringfügige Verstöße. Bußgelder können **bis zu einer Höhe von EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes (ggf. auch konzernweit)** festgesetzt werden und zwar sowohl gegen das betreffende Unternehmen als auch gegen einen ggf. beauftragten IT-Dienstleister (Auftragsverarbeiter), soweit dieser für den Datenschutzverstoß verantwortlich ist. Bußgelderhöhend wirken sich einschlägige frühere Datenschutzverstöße aus sowie eine fehlende Kooperationsbereitschaft des Unternehmens mit der Aufsichtsbehörde. Für den Bereich der Verbraucherkredite regelt § 43 BDSG-neu eigene Sanktionen bei fehlerhafter Erfüllung von Auskunfts- und Informationspflichten. Strafrechtlich ist § 42 BDSG-neu zu beachten, wonach insbesondere gewerbliches, verbotenes Handeln sowie Handeln in Bereicherungs- und Schädigungsabsicht unter Strafe gestellt werden.

---

**Praxistipp:** *Die Aufsichtsbehörden werden wohl nicht gleich Bußgelder in Millionenhöhe festsetzen, bei üblichen Verstoßen im Mittelstand wie fehlerhafter Auftragsverarbeitung eher in vier- bis fünfstelliger Höhe. Schlimmer sind jedoch die Reputationsfolgen von Datenpannen, denn hierauf stürzt sich die Presse besonders gern. Unternehmen sollten zudem berücksichtigen, dass ein ordnungsgemäß eingerichtetes Datenschutzsystem eine optimale Grundlage für die gerade stattfindende Digitalisierung bietet, denn eine transparente, aufgeräumte Datenverwaltung ermöglicht es, schnell und effektiv digitale Werkzeuge wie Predictive Analytics oder künstliche Intelligenz einzusetzen.*

## 12. Ausblick

Die DSGVO sowie das BDSG-neu werden am 25.05.2018 wirksam. Die Aufsichtsbehörden haben bereits bekannt gegeben, dass sie keine „Grace-Period" (sanktionsfreie Übergangsfrist zur Umsetzung) gewähren werden. Auch beachten sollten Unternehmen die kommende E-Privacy-Verordnung, die ebenfalls am 25.05.2018 in Kraft treten wird. Sie soll die bestehende E-Privacy-Richtlinie 2002/58 sowie Cookie-Richtlinie 2009/136 ersetzen und führt im Wesentlichen die Pflicht ein, für die Verwendung von Cookies auf Webseiten die sog. Opt-In-Lösung zu verwenden, also stets eine ausdrückliche Einwilligung einzuholen, was allerdings auch durch vordefinierte Browsereinstellungen geschehen kann.

## Herausgeber

1&1 IONOS Cloud GmbH
Greifswalder Straße 207
10405 Berlin, Germany

## Ansprechpartner:

**Mark Neufurth**
Senior Content Marketing Manager
E-Mail: mark.neufurth@cloud.ionos.com

## Copyright

RA Dr. Hans M. Wulf
SKW Schwarz Rechtsanwälte



1&1 IONOS Cloud GmbH
Greifswalder Straße 207
10405 Berlin, Germany

Tel: +49 30 57700-850
Fax: +49 30 57700-8598
E-Mail: enterprise-cloud@ionos.de

Geschäftsführung:
Christoph Steffens,
Matthias Steinberg, Achim Weiß

Registergericht Berlin Charlottenburg, Germany
Registernummer: HRB 125506 B
USt-ID: DE 270700052