



Kurzinfo zum Datenschutzrecht

Nr. 1 / 18. Januar 2018

- Rechtsänderungen zum 25. Mai 2018 beachten! -

I.	Einführung	1
1.	Rechtsgrundlagen	1
2.	Wesentliche Änderungen.....	2
II.	Wann gilt die DSGVO?	2
1.	Personenbezogene Daten.....	2
2.	Automatisierung oder Nutzen von Datensystemen	3
3.	Datenverarbeitung	3
4.	Örtlicher Anwendungsbereich	3
III.	Zulässige Datenverarbeitung	4
1.	Erlaubnistatbestände.....	4
2.	Einwilligung.....	5
IV.	Rechte der Betroffenen	5
1.	Informationspflicht (neu)	6
2.	Auskunftspflichten	7
3.	Pflicht zur Berichtigung und Löschung	7
4.	Einschränkung der Verarbeitung	8
5.	Datenübertragbarkeit	8
V.	Technischer Datenschutz	8
VI.	Verarbeitungsverzeichnis	9
VII.	Meldepflichten bei Verstößen	9
VIII.	Auftragsdatenverarbeitung	9
IX.	Sanktionen bei Verstößen	10

I. Einführung

1. Rechtsgrundlagen

Am **25. Mai 2018** werden die Datenschutzgrundverordnung (**DSGVO**) und das neue Bundesdatenschutzgesetz (**BDSG neu**), geändert durch das Datenschutzanpassungs- und Umsetzungsgesetz vom 30. Juni 2017 (BGBl. I, S. 2097 ff.), die bisherigen datenschutzrechtlichen Vorschriften ersetzen.



Zu beachten ist, dass die Vorgaben der DSGVO unmittelbar anzuwenden sind und keiner weiteren Umsetzung in deutsches Recht bedürfen. Soweit die DSGVO dem nationalen Gesetzgeber Umsetzungsspielräume eröffnet hat, hat der deutsche Gesetzgeber hiervon nur teilweise Gebrauch gemacht (BDSG neu). In vielen Fällen verweist das BDSG neu auf den Anwendungsvorrang der DSGVO. Beide Gesetzes sind somit vom Anwender gleichzeitig in den Blick zu nehmen.

2. Wesentliche Änderungen

Mit der DSGVO wird das Datenschutzrecht innerhalb Europas vereinfacht, um dem Einzelnen mehr Kontrolle über seine Daten zu verschaffen.

Achtung! Die wesentlichen Regelungen finden sich jetzt in der DSGVO und nicht mehr im BDSG!

Künftig müssen Nutzer einen leichten Zugang zu ihren Daten haben und jederzeit erfahren können, welche Daten über sie gesammelt werden.

Darüber hinaus sind Nutzer darüber zu informieren, wer die Daten zu welchem Zweck wie und wo verarbeitet. Ebenfalls ist der Nutzer zu informieren, wenn unbefugt Dritte Zugriff auf seine Daten erhalten haben.

Neu eingeführt wird auch das Recht des Nutzers auf Vergessen. So dass die neuen datenschutzrechtlichen Vorgaben auch zusätzliche Pflichten zur Löschung von Daten enthalten.

Das Mindestalter für die Abgabe einer wirksamen Einwilligungserklärung für die Verarbeitung personenbezogener Daten wird von 13 auf 16 Jahre hochgesetzt.

Bei Verstößen drohen Unternehmen nunmehr Höchstsummen in Höhe von 4 % der Jahresumsätze eines Unternehmens, so dass sich die Höhe der Bußgelder im Vergleich zu den bisherigen Vorgaben erheblich erhöht hat.

Wir stellen nachfolgend die aus unserer Sicht wesentlichen Änderungen der datenschutzrechtlichen Vorgaben für unsere Mandanten zusammen.

II. Wann gilt die DSGVO?

Die Datenschutzgrundverordnung (DSGVO) findet Anwendung, wenn von öffentlichen oder nicht-öffentlichen Stellen **personenbezogene Daten** ganz oder teilweise automatisiert verarbeitet werden oder bei einer nichtautomatisierten Verarbeitung eine Speicherung in einem Datensystem erfolgt.

Jedes Unternehmen ist deshalb in der Regel betroffen.

1. Personenbezogene Daten

Der Begriff der **personenbezogenen Daten** ist in Art. 4 Nr. 1 DSGVO legal definiert und umfasst alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.



Hinweis: Es geht nur um Daten, die sich auf eine **natürliche Person** beziehen. Namen, Anschrift etc. von juristischen Personen (z.B. GmbH, AG, Vereine etc.) sind deshalb nicht betroffen. Anders allerdings z.B. der Name des Geschäftsführers.

Beispiele für personenbezogene Daten sind:

Name, Adresse, Telefonnummer, Autokennzeichen, IP-Adresse, Geburtsdatum, E-Mail-Adresse, Messwerte (insbesondere Lastgänge von Energiekunden)

Ausreichend ist es, wenn die Information einer Person lediglich irgendwie zugeordnet und damit ein **Personenbezug** hergestellt werden kann. Es reicht nach der Rechtsprechung sogar aus, wenn diese Zuordnung nur dadurch möglich ist, dass sich der Anbieter von Online-Mediendiensten insbesondere bei Cyberattacken an die zuständige Ermittlungsbehörde wendet (z.B. dynamische IP-Adresse) (EuGH, Urt. v. 19.10.2016, RS C 582/14; BGH, Urt. v. 16.05.2017, Az. VI ZR 135/13).

2. Automatisierung oder Nutzen von Datensystemen

Eine **automatisierte Verarbeitung** erfolgt üblicherweise über Computer, Smartphones, Kameras, Scanner oder Kopierer. Wenn deshalb z.B. Onlineprodukte angeboten oder über die Homepage des Unternehmens über das Internet vertrieben oder per E-Mail Kontakt mit dem Unternehmen aufgenommen werden kann, führt dies in der Regel zur Anwendbarkeit der Datenschutzgrundverordnung (DSGVO), wenn personenbezogene Daten betroffen sind. Auch Cookies können eine automatisierte Verarbeitung (i.S. einer Speicherung) bewirken. Dies ist bei der Erstellung von Datenschutzbelehrungen zu beachten. Die DSGVO und das BDSG finden aber auch Anwendung, wenn Daten zunächst z.B. im Kundenzentrum handschriftlich aufgenommene personenbezogene Daten geordnet (chronologisch, alphabetisch) abgelegt werden (z.B. Kundenakte, gleiches gilt für Personalakten, Karteikartensysteme).

3. Datenverarbeitung

Unter einer **Datenverarbeitung** versteht man im Sinne des Art. 4 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

4. Örtlicher Anwendungsbereich

In ordentlicher Hinsicht gilt das sog. Markttortprinzip. Das bedeutet, dass sich die verarbeitende Stelle an die Vorgaben der DSGVO halten muss, wenn sie personenbezogene Daten im Zusammenhang mit Angeboten von Waren oder Dienstleistungen in der Europäischen Union verarbeitet.



III. Zulässige Datenverarbeitung

1. Erlaubnistatbestände

Für die Datenverarbeitung gilt weiterhin ein Verbot mit Erlaubnisvorbehalt. Neu ist, dass die zulässige Datenerhebung überwiegend in Art. 6 DSGVO geregelt ist.

Die bisherigen §§ 28 ff. BDSG werden durch Art. 6 DSGVO ersetzt. Danach ist eine Verarbeitung nur erlaubt, wenn sie „**erforderlich**“ ist **und** alternativ folgende Voraussetzungen vorliegen!

- a. **Einwilligung für bestimmte Daten und Zwecke wurde erteilt!**
- b. **Erfüllung einer Vertragspflicht oder zur Vertragsvorbereitung**
- c. **Erfüllung einer sonstigen Rechtspflicht**
- d. **Schutz eines lebenswichtigen Interesses**
- e. **Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt**
- f. **Schutz eines berechtigten Interesses des Verarbeitenden oder eines Dritten (Achtung: Interessenabwägung erforderlich!)**

Sonderregelungen können - soweit sie im Einzelfall engere Zwecke vorsehen – zu beachten sein (z.B. §§ 50, 55MsbG)

Achtung! Die wesentlichen Regelungen finden sich jetzt in der DSGVO und nicht mehr im BDSG!

Art. 6 Abs. 1 f: „Berechtigte Interessen“ ist zukünftig mögliche Erlaubnisnorm z.B. für folgende Zwecke.

- Direktwerbung und andere Formen des Marketing (bisher § 28 BDSG – u.a. sog. Listenprivileg)
- Gewinnerzielung, arbeitsteilige Datenverarbeitung innerhalb von Unternehmensgruppen (z.B. Adresshandel, Auskunfteien, kleines Konzernprivileg)
- Durchsetzung von Rechtsansprüchen über außergerichtliche Verfahren (z.B. Inkasso)
- Verteidigung des eigenen Vermögens, Verhütung von Betrug, Leistungsmisbrauch oder Geldwäsche (z.B. Bonitätsprüfung)
- Persönliche Sicherheit, IT- und Netzsicherheit (z.B. IP-Adresse speichern)

Berechtigt ist das Interesse im Rahmen einer Güterabwägung mit den Interessen des Betroffenen immer nur dann,

- wenn es mit dem Datenschutzrecht und dem sonstigen Recht in Einklang steht!
- Hinreichend klar bestimmt ist (damit eine Interessenabwägung überhaupt stattfinden kann)
- Tatsächlich und gegenwärtig ist (nicht spekulativ)
- **Die berechtigten Interessen im Rahmen einer Interessenabwägung überwiegen! Die Interessenabwägung ist zu dokumentieren**



Fehlt es an einem überwiegenden berechtigten Interesse, dann ist eine Einwilligung des Betroffenen erforderlich!

Bei Zweckänderung, d.h. bei einer Verarbeitung, die von dem Zweck abweicht, zu dem die Daten ursprünglich erhoben wurden, ist immer dann eine Einwilligung erforderlich, wenn keine Fälle des Art. 6 Abs. 4 a) bis e) vorliegen.

Zu beachten ist ferner, dass auch berechnigte Interessen **Dritter** bei Art. 6 Abs. 1 f) DSGVO geprüft werden. Dies spielt in der Regel bei der Frage eine Rolle, ob Daten in zulässiger Weise an Dritte **übermittelt** werden dürfen. Vorschriften zur Daten**übermittlung** – wie bisher in § 28 a (Auskunfteien) und § 29 BDSG (Adresshandel) gibt es so nicht mehr!

2. Einwilligung

Immer dann, wenn keine andere erlaubte Datenverarbeitung vorliegt, ist eine Einwilligung erforderlich. Zusätzlich ist eine Einwilligung **weiterhin** u.a. in Fällen des § 7 Abs. 2 Nr. 2 und Nr. 3 UWG, MsbG, § 13 TMG, Art. 9 DSGVO erforderlich.

Besondere Beachtung sollte finden, dass die Anforderungen an eine Einwilligung in die Verarbeitung personenbezogener Daten durch den Betroffenen durch die Datenschutzgrundverordnung **höheren Anforderungen** genügen muss. Während bisher z.B. nach dem Bundesdatenschutzgesetz und der Rechtsprechung des BGH bei Einwilligungserklärungen auch eine sog. Opt-Out-Klausel zulässig war, ist dies nach den Erwägungsgründen der Datenschutzgrundverordnung zu Art. 7 DSGVO nicht mehr ausreichend. D.h., es werden zukünftig lediglich sog. **Opt-In**-Klauseln zulässig sein, bei denen der Betroffene ausdrücklich seine Einwilligung erklären muss und vorgefertigte bereits angekreuzte Kästchen (Opt-Out) nicht mehr verwendet werden. Dies wird in der Praxis zu erheblichen Umstellungen bei der Vertragsgestaltung führen. Die wichtigsten Anforderungen an eine rechtsgültige Einwilligung sind nach wie vor, dass

- eine freie Entscheidung des Betroffenen vorliegen muss,
- der Betroffene vor Abgabe der Einwilligungserklärung über den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten im Einzelnen informiert werden muss,
- nach Art. 7 DSGVO nachgewiesen werden kann, dass eine Einwilligung erteilt wurde. Deshalb sollte die Einwilligung mindestens in Textform oder in elektronischer Form (dann am besten als sog. double-opt-in) erfolgen.

Ferner muss sichergestellt sein, dass der Betroffene über die Widerruflichkeit der Einwilligungserklärung belehrt wird.

IV. Rechte der Betroffenen

Die Rechte der Betroffenen werden durch die Datenschutzgrundverordnung (DSGVO) erheblich gestärkt. Die Datenschutzgrundverordnung sieht insbesondere folgende Rechte vor:

- Informationsrecht
- Auskunfts- und Widerspruchsrecht
- Recht auf Berichtigung, Löschung und Einschränkung



- Recht auf Datenübertragbarkeit

1. Informationspflicht (neu)

Neu und für Unternehmen von besonderer Bedeutung ist die Informationspflicht nach Art. 13 DSGVO. Danach muss das Unternehmen den Betroffenen zum Zeitpunkt der Erhebung der Daten wie folgt zu informieren:

Informationsblatt
<ul style="list-style-type: none">• Name und Kontaktdaten des Verantwortlichen (ggf. auch des Vertreters) Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)• Zweck und Rechtsgrundlage der Verarbeitung• Berechtigte Interessen (bei Verarbeitung nach Art. 6 DSGVO)• Empfänger bzw. Kategorien von Empfängern• Übermittlung in Drittland oder an internationale Organisationen (soweit erfolgt)• Dauer der Speicherung• Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit• Bestehen eines Rechts auf Widerspruch der Einwilligung• Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde• Informationen, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich und mögliche Folgen der Nichtbereitstellung• Bestehen einer automatisierten Entscheidungsfindung einschließlich etwaiges Profiling• Informationen über eine mögliche Zweckänderung der Datenverarbeitung

Hinweis:

Sie sollten deshalb Ihre bisherige Vertragsabwicklung überprüfen und zumindest ein Informationsblatt vorsehen, welche die vorgenannten Informationen enthält. **Wir unterstützen Sie gerne bei der Gestaltung.**

Eine **weitere Information** ist durchzuführen, wenn die Daten nicht beim Betroffenen, sondern bei einem Dritten erhoben werden. Insoweit gilt Art. 14 DSGVO. **Anwendungsfall** ist hier z.B. die Abfrage der Kreditwürdigkeit des Betroffenen bei einer Auskunft. Insoweit müssen gem. Art. 14 DSGVO zusätzliche Informationen darüber angegeben werden, aus welcher Quelle die Daten stammen und ob sie ggf. aus öffentlichen Quellen stammen.

Relevant kann dies z.B. zur Prüfung der Kreditwürdigkeit des Betroffenen sein, wenn Sie Daten von einer Auskunft erhalten. Es kann auch sein, dass Sie personenbezogene Daten von Dritten anlässlich des Vertragsschlusses erhalten (z.B. zu Familienmitgliedern, Mitarbeitern von Geschäftspartnern).

Auf eine Information kann nur in sehr engen Grenzen verzichtet werden.



2. Auskunftspflichten

Nach Art. 15 DSGVO kann der Betroffene Auskunft über folgende Informationen verlangen:

- Zwecke der Datenverarbeitung
- Kategorien der Daten
- Empfänger oder Kategorien von Empfängern
- Dauer der Speicherung
- Recht auf Berichtigung, Löschung und Widerspruch
- Beschwerderecht bei einer Aufsichtsbehörde
- Herkunft der Daten (wenn nicht beim Betroffenen erhoben)
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- Übermittlung in Drittland oder an internationale Organisationen

Der Betroffene ist durch eine **Kopie aller personenbezogenen Daten** auf gängigem elektronischen Wege zu informieren. Dies erfordert von dem Unternehmen, dass es in der Lage ist, die bei ihm gespeicherten personenbezogenen Daten in einem elektronisch üblichen Format an den Betroffenen herauszugeben.

3. Pflicht zur Berichtigung und Löschung

Neben den Auskunftsrechten besteht nach Art. 16 DSGVO das Recht auf Berichtigung und nach Art. 17 DSGVO das Recht auf Löschung von Daten.

Hinweis:

Sie sollten prüfen, in welcher Weise bei Ihnen die Daten gespeichert sind und wie Sie sicherstellen können, dass die Rechte auf Auskunftserteilung, Berichtigung und Löschung angemessen erfüllt werden können.

Für die praktische Umsetzung ist zu beachten, dass unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen zu treffen sind, um die Verantwortlichen, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat.

Das Recht auf Löschung von Daten besteht allerdings nur dann, wenn die Speicherung der Daten nicht mehr notwendig ist, wenn der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat, wenn die Daten unrechtmäßig verarbeitet wurden oder wenn eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht. Hier sind insbesondere auch Aufbewahrungspflichten aus anderen Rechtsnormen (z.B. Abgabenordnung) zu berücksichtigen.

Das Recht auf Vergessen wird gem. Art. 17 DSGVO bei bestimmten Anwendungsfällen begrenzt.



4. Einschränkung der Verarbeitung

Nach Art. 18 DSGVO kann vom Betroffenen die Einschränkung der Verarbeitung der personenbezogenen Daten dann verlangt werden,

- wenn die Richtigkeit der Daten bestritten ist, die Verarbeitung unrechtmäßig war, sich der Zweck der Verarbeitung erledigt hat, die Daten aber zu Geltendmachung von Rechtsansprüchen des Betroffenen notwendig sind,
- wenn ein Widerspruch des Betroffenen vorliegt.

Nach Art. 19 DSGVO ist der Verantwortliche verpflichtet, den Empfängern, an die Daten weitergegeben wurden, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen, es sei denn dies ist unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden. Auch dies erfordert von den Verwendern der Daten eine Kenntnis darüber, an wen die Daten weitergegeben wurden und dass organisatorisch eine Weitergabe der Informationen nach Art. 19 DSGVO überhaupt möglich ist.

Hinweis:

Die Dokumentation der Datenempfänger ist wichtig, da diesen unverzüglich eine berechtigte Bitte auf Berichtigung, Löschung oder Einschränkung von Daten weitergegeben werden muss.

5. Datenübertragbarkeit

Das neu eingefügte Recht auf Datenübertragbarkeit nach Art. 20 DSGVO soll sicherstellen, dass Betroffene von einem Anbieter, z.B. sozialer Netzwerke, zu einem anderen wechseln können, ohne den Verlust ihrer Daten befürchten zu müssen.

V. Technischer Datenschutz

Für Unternehmen ist besonders zu berücksichtigen, dass es Vorgaben zum technischen Datenschutz auch nach der DSGVO gibt. Nach Art. 24 DSGVO sind Unternehmen verpflichtet, unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen zu installieren. Hierzu haben sich die Unternehmen unterschiedlicher technischer Maßnahmen zu bedienen. Die Verordnung unterscheidet einmal zwischen dem Grundsatz des Datenschutzes durch Technik (data protection by design) und datenschutzfreundlichen Voreinstellung (data protection by default). Solche Maßnahmen können u.a. darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktion und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Datenverarbeitung zu überwachen und der für die Verarbeitung Verantwortlichen in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern (Erwägungsgrund 61 DSGVO).

Hinweis:

Die bestehenden technischen und organisatorischen Maßnahmen sind vor diesem Hintergrund zu überprüfen (z.B. Verschlüsselung, Anonymisierung etc.).



VI. Verarbeitungsverzeichnis

Schon bisher waren Unternehmen verpflichtet, geeignete technische und organisatorische Maßnahmen im Rahmen eines Verzeichnisses von Verarbeitungstätigkeiten vorzuhalten. Daran ändert sich auch nach der DSGVO nichts. Auch **weiterhin** ist ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO vorzuhalten, was folgende Informationen enthalten muss:

- Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen (ggf. auch Vertreter und Datenschutzbeauftragter)
- Zwecke der Verarbeitung
- Kategorien von betroffenen Personen und personenbezogenen Daten
- Kategorien von Empfängern, an die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden (auch in Drittländer)
- Übermittlung von Daten an ein Drittland oder an eine internationale Organisation
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Anhand dieses Verzeichnisses von Verarbeitungstätigkeiten soll auch dokumentiert werden, dass das Unternehmen die datenschutzrechtlichen Vorgaben ordnungsgemäß beachtet.

Es kann hier zwischen einem externen und einem internen Verarbeitungsverzeichnis unterschieden werden. Das externe Verarbeitungsverzeichnis muss auch den Aufsichtsbehörden vorgelegt werden können. Das interne Verarbeitungsverzeichnis dient der internen Dokumentation.

VII. Meldepflichten bei Verstößen

In dem Zusammenhang ist auch zu beachten, dass nach Art. 33 DSGVO der Verantwortliche verpflichtet ist, Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde zu melden. Die Meldung hat unverzüglich und ohne unangemessene Verzögerung zu erfolgen, möglichst binnen höchstens 72 Stunden, nachdem die Verletzung bekannt wurde. Gleichzeitig muss auch der Betroffene nach Art. 34 DSGVO von der Datenschutzverletzung benachrichtigt werden. Die Benachrichtigungspflicht gilt nur dann nicht, wenn technische oder organisatorische Maßnahmen wie z.B. eine Verschlüsselung die Kenntnisnahme von personenbezogenen Daten verhindert oder sichergestellt ist, dass kein hohes Risiko besteht.

VIII. Auftragsdatenverarbeitung

Besonderes Augenmerk sollten die Unternehmen auch auf die Fragen der Auftragsdatenverarbeitung legen. Zwar ist schon jetzt grundsätzlich nach § 11 BDSG der Abschluss einer Auftragsdatenverarbeitungsvereinbarung notwendig, wenn Dritte bei der Datenverarbeitung nach Weisung einbezogen sind. Nunmehr sind allerdings Pflichtenverstöße gegen diese Vorgabe mit erheblichen Bußgeldern bewährt, so dass die Unternehmen eingehend



prüfen sollten, ob derzeit überhaupt eine Auftragsdatenverarbeitung mit Dienstleistern bestehen und ob diese Auftragsdatenverarbeitungsvereinbarungen den Anforderungen des Art. 28 DSGVO genügen.

Eine Auftragsdatenverarbeitungsvereinbarung muss folgende Inhalte nach Art. 28 Abs. 3 DSGVO enthalten:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten und Kategorien von betroffenen Personen
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen und organisatorischen Maßnahmen
- Hinzuziehung von Subunternehmern
- Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitungsvereinbarung
- Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

Anders als bisher nach dem Bundesdatenschutzgesetz enthält Art. 82 DSGVO schärfere Haftungsregelungen für die Auftragsverarbeiter. Auch der Auftragsverarbeiter kann vom Betroffenen wegen Schadensersatz in Anspruch genommen werden. Dies galt nach dem Bundesdatenschutzgesetz so nicht. Grundsätzlich gilt, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter gegenüber dem Betroffenen gemeinsam als Gesamtschuldner haften und im Innenverhältnis ein Innenausgleich erfolgen muss.

Neu ist, dass auch Auftragsverarbeiter nach Art. 30 Abs. 2 DSGVO ein Verzeichnis über die Verarbeitungstätigkeiten führen müssen. Die Inhalte sind jedoch etwas geringer als nach Art. 28 Abs. 3.

Häufig wird vergessen, dass eine Auftragsdatenverarbeitung auch dann vorliegen kann, wenn Dienstleister lediglich mit der Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen beauftragt werden und dabei den Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

IX. Sanktionen bei Verstößen

Bei Verstößen gegen die Verpflichtungen der Art. 28 DSGVO drohen den für die Verarbeitung Verantwortlichen und den Auftragsdatenverarbeitern nach Art. 83 DSGVO Geldbußen in Höhe von bis zu 10 Mio. EUR oder 2 % des gesamten weltweit erzielten Jahresumsatzes, je nach dem welcher Betrag höher ist.

**Hinweis:**

Die Unternehmen sollten bestehende Prozesse und Verträge zur Datenverarbeitung im Auftrag überprüfen und erforderliche Änderungen umgehend vornehmen. Neu abzuschließende Verträge sollten die bereits künftige Rechtslage berücksichtigen.

gez.
Wibke Reimann
Rechtsanwältin

Ansprechpartner:**Rechtsanwältin Wibke Reimann**

Tel.: 030 / 89 04 92 – 12

E-Mail: reimann@brs-rechtsanwaelte.de

**Rechtsanwalt Glenn Dammann**

Tel.: 030 / 89 04 92 – 15

E-Mail: dammann@brs-rechtsanwaelte.de



Redaktion: Rechtsanwältin Wibke Reimann
Herausgeber: Bethge.Reimann.Stari Rechtsanwälte Partnerschaft mbB, Berlin
Sekretariat: Katja Schäbsdat, Tel: 030 – 890492-12, Fax: 030 – 890492-10

Recht aktuell wird nach sorgfältig ausgewählten Unterlagen erstellt. Diese Veröffentlichung verfolgt ausschließlich den Zweck, bestimmte Themen anzusprechen und erhebt keinen Anspruch auf Vollständigkeit. Für die Anwendung im konkreten Fall kann eine Haftung nicht übernommen werden. Sollten Sie weitere Fragen zu den angesprochenen Themen haben, so wenden Sie sich bitte an unsere Ansprechpartner. Der Nachdruck - auch auszugsweise - ist nur mit Quellenangabe gestattet.

Wenn Sie die Publikation nicht mehr erhalten wollen, teilen Sie uns dies bitte per E-Mail mit.