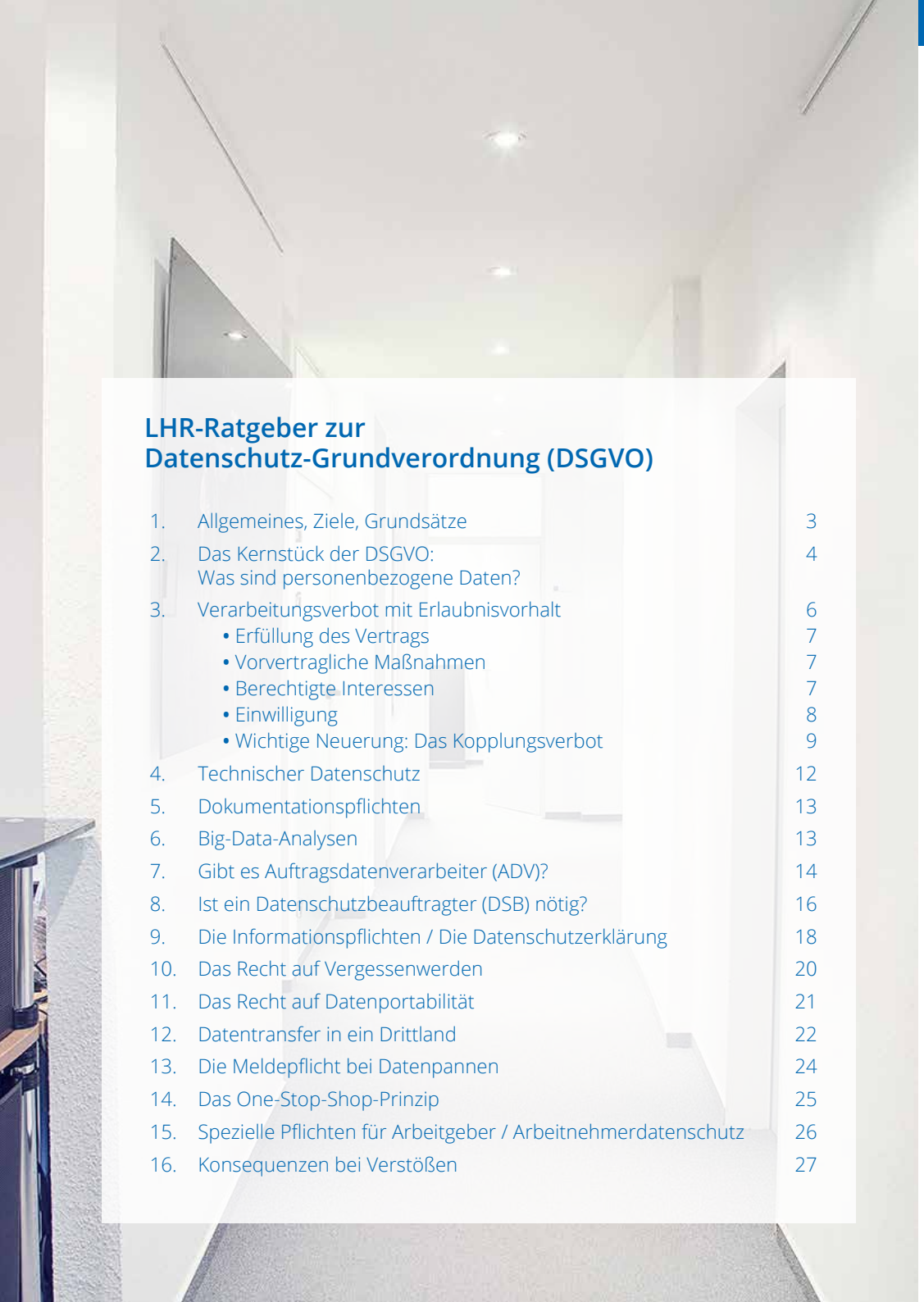
LHR-RATGEBER

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Ab dem **25.05.2018** wird die Datenschutz-Grundverordnung (**DSGVO**) die Verarbeitung von **personenbezogenen Daten** regeln.
Dieser LHR-Ratgeber gibt Ihnen einen Überblick über die **neuen Regelungen** und zeigt Ihnen in **16 Punkten**, was Sie nun zu tun haben.

LHR



LHR-Ratgeber zur Datenschutz-Grundverordnung (DSGVO)

LHR

1. ALLGEMEINES, ZIELE, GRUNDSÄTZE

Die **Ziele** der Verordnung sind

- Schutz der personenbezogenen Daten
- Freier Verkehr personenbezogener Daten

Diese Ziele sollen durch die folgenden **Grundsätze** erreicht werden:

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität & Vertraulichkeit
- Rechenschaftspflicht

Grundsätzlich verarbeiten **Unternehmen** personenbezogene Daten, daher sind von der DSGVO betroffen:

- Unternehmen mit Sitz in der EU
- Unternehmen ohne Niederlassung in der EU, wenn personenbezogene Daten von Personen verarbeitet werden, die sich in der EU befinden

Was Sie nun tun müssen:

Zu Beginn müssen Sie den **Änderungsbedarf** in Ihrem Unternehmen **eruieren**. Hierzu sollten Sie sich zunächst klarmachen, wie die datenschutzrechtlichen Vorgaben bisher umgesetzt wurden (**Status quo**). Im zweiten Schritt sollten Sie sich mit den **neuen Regelungen** auseinandersetzen, hier hilft Ihnen unserer LHR-Ratgeber. Der Abgleich zwischen dem Status quo und den neuen Regelungen ergibt sodann den Änderungsbedarf.

Wir empfehlen Ihnen, zusätzlich Anwälte oder Datenschutzexperten zu Rate zu ziehen. Diese Fachleute können Ihre bisherigen Prozesse analysieren und mit Ihnen gemeinsam eine Strategie zur Umsetzung der DSGVO erarbeiten.

2. DAS KERNSTÜCK DER DSGVO: WAS SIND PERSONENBEZOGENE DATEN?

Personenbezogene Daten sind gem. Art. 2 Abs. 1 DSGVO Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Die technische Form der personenbezogenen Daten ist irrelevant, so können auch Fotos, Video- oder Tonaufnahmen personenbezogene Daten enthalten.

Bei der Beurteilung, ob ein personenbezogenes Datum vorliegt, ist vor allem der Aspekt der Identifizierbarkeit von besonderer Bedeutung. Kann ein Datum mithilfe von Zusatzwissen einer Person zugeordnet werden, ist die Person identifizierbar und es liegt ein personenbezogenes Datum vor. Ob dieses Zusatzwissen erst mit einem gewissen Aufwand erlangt werden kann, ist nicht von Bedeutung, solange das Zusatzwissen zugänglich und erreichbar ist.

Beispiel: Die IP-Adresse ist für einen Provider grundsätzlich ein personenbezogenes Datum, denn dieser kann die IP-Adresse ohne Weiteres einem Nutzer zuordnen. Für einen Dritten ist die IP-Adresse zunächst kein personenbezogenes Datum, wenn dieser keinen Zugriff auf das Zusatzwissen des Providers hat. Kann die IP-Adresse aber durch frei zugängliche Angaben – beispielsweise im Internet – einer Person zugeordnet werden, so liegt für den Dritten ein personenbezogenes Datum vor. Eine IP-Adresse ist daher auch dann ein personenbezogenes Datum, wenn sie aufgrund von Verknüpfungen mit anderen Daten (Cookies, Nutzerverhalten etc.) zu einer Identifizierung der betroffenen Person führt.

Wichtig zu wissen:

Jegliche Information kann ein personenbezogenes Datum sein.

Insbesondere folgende Daten sind personenbezogen:

- Name
- Geburtsdatum
- Adresse
- E-Mail-Adresse
- Kundendaten (Kundennummer usw.)
- Vertragsbeziehungen
- Freundschaften (bspw. in sozialen Netzwerke)
- Konsum- und Kommunikationsverhalten
- Wahrscheinlichkeitsaussagen
- Arbeitszeiten
- Kontodaten
- IP-Adressen
- Cookies

Was Sie nun tun müssen:

Verdeutlichen Sie sich, **an welchen Stellen** in Ihrem Unternehmen personenbezogene Daten **verarbeitet** und **wo** diese **mit anderen Unternehmen ausgetauscht** werden. Dieses Wissen ist unerlässlich, um Ihren Dokumentationspflichten (hierzu an späterer Stelle mehr) nachzukommen.

Vor allem, wenn Sie im Besitz großer Datensätze sind, empfiehlt sich die Nutzung von **Software zur Identifizierung der personenbezogenen Daten**. Die Software durchsucht Datenbanken nach personenbezogenen Daten, erkennt und katalogisiert sie. Selbst für unstrukturiert vorliegende Daten gibt es entsprechende Software, welche Exchange-Server, ZIP-Dateien, Textdateien oder auch E-Mails samt Anhängen durchforstet.

3. VERARBEITUNGSVERBOT MIT ERLAUBNISVORHALT

Die DSGVO will dem Verlust von Vertrauen in die alten Datenschutzvorschriften Rechnung tragen und bestimmte Vorgänge besonders schützen. Dazu gehören

- Zustimmung
- Kommunikation
- Dokumentation
- Zugang und Übertragbarkeit
- Warnhinweise
- Datenlöschung
- Profilerstellung
- Marketing
- Schutz besonderer Kategorien sowie
- die Übermittlung von Daten nach außerhalb der EU.

Grundsätzlich verbietet die DSGVO die Verarbeitung personenbezogener Daten. Von diesem Verbot wird nur dann eine Ausnahme gemacht, soweit die Verarbeitung der personenbezogenen Daten der **Erfüllung eines Vertrags** oder **vorvertraglicher Maßnahmen**, solange diese auf Anfrage der betroffenen Person erfolgt, dient, oder eine **Einwilligung** vorliegt.

Eine weitere Ausnahme bilden die **berechtigten Interessen**. Allerdings müssen diese Interessen die Grundrechte der betroffenen Personen überwiegen. Eine solche Abwägung ist nicht immer leicht.

• ERFÜLLUNG DES VERTRAGS

Welche Datenverarbeitung für die Erfüllung eines Vertrags notwendig ist, bestimmt sich nach der Natur des betreffenden Vertrags und den sich daraus ergebenden Pflichten. So ist es zum Beispiel unproblematisch zulässig, die Postadresse des Kunden eines Onlinehändlers zur Zustellung der Ware an den Paketdienst weiterzureichen. Die Weitergabe von Daten an ein Unternehmen zur Bonitätsprüfung ist hingegen ohne separate Einwilligung nicht zulässig, da zwar für den Unternehmer zweckmäßig, aber für die Durchführung des Vertrags **nicht zwingend notwendig**.

• VORVERTRAGLICHE MASSNAHMEN

Hierunter versteht man bspw. die **Erstellung von Angeboten** für

- Werkverträge
- Werklieferungsverträge
- Dienstverträge
- Reiseverträge

Kommt der Vertrag nicht zustande, müssen Sie die **Daten löschen**.

• BERECHTIGTE INTERESSEN

Ob Ihre **berechtigten Interessen** überwiegen, kann nicht pauschal beantwortet werden. **Anhaltspunkte zur Orientierung** sind die folgenden:

- Je eher die Datenverarbeitungstätigkeit **üblich oder bekannt** ist, desto eher wird sie rechtmäßig sein (Stichpunkt: Web- bzw. Reichweitenanalyse wie Google Analytics oder Piwik).
- Sie sollten mit dem **Opt-Out-Prinzip** arbeiten.
- **Informieren** Sie die betroffenen Personen **verständlich und umfassend**.
- **Pseudonymisieren** Sie die Daten schnellstmöglich!
- Seien Sie bei der Datenverarbeitung von **Minderjährigen** besonders zurückhaltend.

• EINWILLIGUNG

Eine weitere Ausnahme zum grundsätzlichen Verbot stellt die **nachweisliche Einwilligung** dar. Daher sind zum Beispiel Cookie-Banner, wie „Sollten Sie weiterhin diese Webseite besuchen, gehen wir davon aus, dass Sie mit dem Setzen von Cookies einverstanden sind.“, nicht mehr ausreichend.

Was Sie nun tun müssen:

Beachten Sie **unbedingt** die folgenden Punkte:

- Im Zweifel sollte eine Einwilligung eingeholt werden. Darauf, dass ein Gericht oder die Datenschutzbehörde ein überwiegendes berechtigtes Interesse annimmt, sollten Sie **nicht vertrauen**.
- Die Einwilligung muss **nachweislich** sein. Nutzen Sie das **Opt-In-Prinzip**.
- **Zweckbindung**: Einwilligungen müssen zweckgebunden erfolgen. Geben Sie immer die Zwecke der Datenverarbeitung an.
- Geben Sie den Nutzern eine **einfache Widerrufsmöglichkeit**.
- Es wird ein **Mindestalter für Einwilligungen** geben. Mit sechzehn Jahren kann eine wirksame Einwilligung erteilt werden. Minderjährige unter dreizehn Jahre können keine wirksame Einwilligung abgeben, diese sind erst mit dem Einverständnis der Eltern wirksam. Ob Minderjährige zwischen dreizehn und sechzehn Jahren eine wirksame Einwilligung erteilen können, lässt die DSGVO offen und überlässt diese Entscheidung den nationalen Gesetzgebern.

Wichtig zu wissen:

Alte Einwilligungen bestehen fort, sofern sie den bisherigen Anforderungen des Bundesdatenschutzgesetzes (BDSG) und des Telemediengesetzes (TMG) genügen und Sie die Einholung der Einwilligungen via Opt-In-Prinzip nachweisen können.

• WICHTIGE NEUERUNG: DAS KOPPLUNGSVERBOT

Die Einwilligung muss **freiwillig** erfolgen. Deshalb beinhaltet die DSGVO das so genannte **Kopplungsverbot**. Dieses ist in Art. 7 Abs. 4 DSGVO normiert:

> „Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“

Es handelt sich dabei um eine missglückte Formulierung, deren Sinngehalt sich nicht beim ersten Lesen offenbart. Das Kopplungsverbot betrifft einen Fall wie den Folgenden:

> Sie möchten die E-Mail-Adresse des Kunden nicht nur zur Kommunikation hinsichtlich der Bestellung nutzen. Sie möchten sie vielmehr einem anderen Unternehmen für dessen Werbezwecke weitergeben. Sie weisen den Kunden hierauf hin und lassen sich dessen Einverständnis erteilen.

Ob in diesem Fall das Kopplungsverbot eingreift, lässt sich allein anhand des Art. 7 Abs. 4 DSGVO nicht eindeutig beantworten. Gegen eine Freiwilligkeit der Einwilligung spricht der Umstand, dass Sie die Einwilligung in den Bestellprozess haben einfließen lassen. Der Vertragsschluss ist von der Einwilligung in die Verarbeitung der personenbezogenen Daten abhängig gemacht worden. Für die Freiwilligkeit der Einwilligung spricht wiederum, dass Sie den Kunden auf die Folgen seines Einverständnisses aufmerksam gemacht haben.

Zieht man den Erwägungsgrund 43 Satz 2 DSGVO zu Rate, kommt man zu einem anderen Ergebnis:

> „Die Einwilligung gilt nicht als freiwillig erteilt, [...]| wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, **von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist**.“

Die Einwilligung ist in unserem kleinen Fall nicht für die Abwicklung des Kaufvertrags erforderlich. Nach dem Erwägungsgrund gilt die Einwilligung als nicht freiwillig erteilt und ist damit unwirksam. Hier offenbart sich eine **Diskrepanz zwischen der Vorschrift und ihrem Erwägungsgrund**, die zu einer Rechtsunsicherheit in der Praxis führen wird. Während Aufsichtsbehörden und Verbraucherschützer eine strenge Auslegung des Kopplungsverbots vornehmen werden, werden Berater von Unternehmen auf die Möglichkeiten aufmerksam machen, die Art. 7 Abs. 4 DSGVO losgelöst von seinem Erwägungsgrund eröffnet.

Das Kopplungsverbot ist besonders relevant für das Geschäftsmodell „**Service gegen Daten**“. Hierunter fallen unter anderem:

- **„Kostenfreie“ Gewinnspiele** im Internet: Solche Gewinnspiele finanzieren sich in aller Regel über Werbung, in die der Teilnehmer vorher einwilligt. Die Verarbeitung personenbezogener Daten zu Werbezwecken ist allerdings für die Durchführung des Gewinnspiels nicht von Nöten.
- **„Kostenloser“ E-Mail-Account**: Dieser E-Mail-Account finanziert sich häufig durch die Zusendung von Newslettern, die dem Bewerben bestimmter Produkte dienen. Auch in diesem Beispiel ist die Verarbeitung von personenbezogenen Daten zu Werbezwecken für die Bereitstellung des E-Mail-Accounts nicht notwendig.

Was Sie nun tun müssen:

Das Geschäftsmodell „Service gegen Daten“ könnte künftig unzulässig sein. Sie müssten Ihr Geschäftsmodell entsprechend anpassen, um sicher zu gehen. Es sind **drei verschiedene gangbare Lösungswege** denkbar (Beispielsfall „Kostenloser E-Mail-Account“):

- **Entkoppeln**: Trennen Sie den Abschluss des Dienstvertrags von der Einwilligung in die Verarbeitung personenbezogener Daten zum Zwecke von Werbung. Sie laufen bei dieser Lösung allerdings Gefahr, dass die Nutzer nach Abschluss des Dienstvertrags nicht mehr in die Verarbeitung der personenbezogenen Daten einwilligen: Ihre Refinanzierung durch Werbung ist gefährdet.
- **Integrieren**: Sie können die Verarbeitung der personenbezogenen Daten zum integralen Bestandteil Ihres Vertrags machen. Ihre Leistung ist demnach das Bereitstellen des E-Mail-Accounts, die Gegenleistung des Kunden hingegen ist das Bereitstellen der personenbezogenen Daten zum Zwecke der Werbung. Dies müssen Sie dann aber auch deutlich nach außen kommunizieren. Die pauschale Darstellung, der E-Mail-Account sei kostenlos, verbietet sich dann.
- **Eine Alternative schaffen**: Die für Sie sicherste Lösung ist, eine Alternative anzubieten. Zusätzlich zu dem Angebot „E-Mail-Account gegen Daten“ können Sie optional die Bereitstellung des E-Mail-Accounts gegen Bezahlung mit Geld anbieten. Bei der Bezahlvariante dürfen Sie die personenbezogenen Daten natürlich nicht zu weiteren Werbezwecken nutzen.

4. TECHNISCHER DATENSCHUTZ

Nach Art. 24 DSGVO haben Sie den **Datenschutz durch technische und organisatorische Maßnahmen sicherzustellen**. Dabei sind die folgenden Grundsätze zu beachten:

- privacy by design - Datenschutz durch Technik
- privacy by default - datenschutzfreundliche Voreinstellungen

Wollen Sie neue, automatisierte oder groß angelegte Techniken für die Verarbeitung der personenbezogenen Daten einführen, müssen Sie eine **Datenschutz-Folgen-abschätzung** vornehmen. Bei einem negativen Ergebnis ist die Aufsichtsbehörde zu kontaktieren.

Was Sie nun tun müssen:

Auf die Frage, welche Maßnahmen Sie genau zu treffen haben, gibt die DSGVO keine konkrete Antwort. Denkbar sind aber folgende Maßnahmen:

- Maßnahmen, die die Datenverarbeitung minimieren
- Maßnahmen, die die Datenverarbeitung schnellstmöglich pseudonymisieren
- Möglichkeiten für die betroffenen Personen, die Verarbeitung ihrer Daten zu überwachen

5. DOKUMENTATIONSPFLICHTEN

Sie müssen fortan all Ihre Datenverarbeitungstätigkeiten dokumentieren. Gegebenenfalls kann von Ihnen verlangt werden, nachzuweisen, dass Sie sich an die Vorgaben der DSGVO gehalten haben **(Rechenschaftspflicht)**.

Konkret fordert Art. 30 DSGVO **die Führung eines Verzeichnisses Ihrer Datenverarbeitungstätigkeiten**. In diesem Verzeichnis müssen bspw. die Zwecke der Verarbeitung sowie die Kategorien der personenbezogenen Daten angegeben werden.

Was Sie nun tun müssen:

Werden Sie sich der Zwecke bewusst, für die Sie die personenbezogenen Daten verarbeiten und beginnen Sie schon jetzt, ein Verzeichnis Ihrer Datenverarbeitungstätigkeiten anzulegen. Je mehr Daten Sie verarbeiten, desto eher bietet es sich an, auf eine Software-Lösung zurückzugreifen.

6. BIG-DATA-ANALYSEN

Big-Data-Analysen sind für gewisse Unternehmen ein wichtiger Teil ihrer Geschäftstätigkeit. Es sollen Unternehmensabläufe optimiert und Vorteile gegenüber Mitbewerbern erzielt werden. Ein Beispiel ist die häufig auf Verkaufsplattformen zu findende Kaufanregung „andere Kunden kauften auch“. Verarbeiten Sie dabei personenbezogene Daten, benötigen Sie die **Einwilligung** der betroffenen Personen falls Ihre berechtigten Interessen die Grundrechte der Betroffenen nicht überwiegen, was im Regelfall nicht der Fall sein wird.

Was Sie nun tun müssen:

Da die DSGVO nur auf personenbezogene Daten anwendbar ist, bedeutet das im Umkehrschluss: **Anonymisieren** Sie die Daten, so findet die DSGVO keine Anwendung und Sie benötigen keine Einwilligung der Betroffenen für Big-Data-Analysen.

7. GIBT ES AUFTRAGSDATENVERARBEITER (ADV)?

Auftragsdatenverarbeiter (ADV) hafteten auch schon vor der DSGVO für eine unbefugte Datenverarbeitung. Neu ist, dass die DSGVO bereits gewisse **inhaltliche Anforderungen an den Vertrag zwischen Ihnen und einem etwaigen ADV vorschreibt**.

Was ist ein Auftragsdatenverarbeiter (ADV)?

Nach Art. 4 Nr. 8 DSGVO versteht man hierunter

> „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet."

Gemeint sind hiermit bspw. externe Kundencenter, externe Marketing-Agenturen, externe Rechenzentren oder externe Newsletter-Anbieter.

Was Sie nun tun müssen:

Eruieren Sie zunächst, mit welchen ADV Sie zusammenarbeiten. Sodann müssen Sie alle **bestehenden Verträge oder Vertragsvorlagen anhand der Anforderungen des § 28 Abs. 3 DSGVO überprüfen**. Bedenken Sie, dass Sie aufgrund von Verträgen, die diesen **Anforderungen nicht gerecht werden, haftbar** gemacht werden können.

Nach Art. 28 Abs. 3 DSGVO muss der Vertrag mit Ihrem ADV insbesondere vorsehen, dass dieser

- die personenbezogenen Daten nur auf **dokumentierte Weisung** von Ihnen verarbeitet;
- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen **zur Vertraulichkeit verpflichtet** haben oder einer angemessenen gesetzlichen **Verschwiegenheitspflicht** unterliegen;
- den **technischen Datenschutz gewährleistet**;
- für die **Inanspruchnahme der Dienste eines weiteren ADV** eine vorherige gesonderte oder allgemeine schriftliche Genehmigung von Ihnen einholt und dieselben Anforderungen an den Vertrag mit dem weiteren ADV einhält, die er für den Vertrag mit Ihnen einhalten muss;
- angesichts der Art der Verarbeitung Sie nach Möglichkeit **mit geeigneten technischen und organisatorischen Maßnahmen** dabei **unterstützt**, Ihrer Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen;
- unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen Sie bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützt;
- nach Abschluss der Erbringung der Verarbeitungsleistungen **alle personenbezogenen Daten** entsprechend Ihrer Wahl entweder **löscht oder zurückgibt**, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
- Ihnen alle erforderlichen **Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt** und Überprüfungen – einschließlich **Inspektionen** –, die von Ihnen oder einem anderen von Ihnen beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

8. IST EIN DATENSCHUTZ-BEAUFTRAGTER (DSB) NÖTIG?

Bisher musste bereits unter bestimmten Voraussetzungen ein **Datenschutzbeauftragter (DSB)** bestellt werden. Hierbei wurde an die Zahl der Mitarbeiter angeknüpft, die mit der Verarbeitung personenbezogener Daten ständig beschäftigt sind.

Die Voraussetzungen der Bestellpflicht eines DSB ändern sich nun durch die DSGVO. **Ein DSB** ist zum einem **zu bestellen, wenn**

- die Art, der Umfang und/oder die Zwecke der Datenverarbeitung (insbes. **Scoring** oder **Profiling** Maßnahmen) eine umfangreiche regelmäßige und systematische Überwachung erforderlich machen

und zum anderen, **wenn**

- Ihre Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten (rassische & ethische Herkunft, politische Meinungen, religiöse & weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische & biometrische bzw. Gesundheitsdaten) liegt.

Der DSB genießt **Weisungsfreiheit** und darf aufgrund seiner Tätigkeit **weder benachteiligt noch abberufen** werden.

Die Anforderungen an den DSB

- berufliche Qualifikation
- Fachwissen, auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis
- Fähigkeiten zur Erfüllung seiner Aufgaben

Die Aufgaben des DSB

- Unterrichtung & Beratung des Verantwortlichen oder Auftragsdatenverarbeiters
- Überwachung der Einhaltung der DSGVO
- Beratung und Überwachung der Datenschutz-Folgenabschätzung
- Zusammenarbeit und Anlaufstelle für die Aufsichtsbehörde

Muss ich einen externen Datenschutzbeauftragten bestellen oder kann ich mich eines Mitarbeiters bedienen?

Auf diese Frage gibt Art. 36 Abs. 6 DSGVO eine Antwort. Sie **können** einen externen Datenschutzbeauftragten benennen, **müssen** dies aber **nicht** tun. Es genügt, wenn Sie einen Ihrer Beschäftigten bestellen.

Was Sie nun tun müssen:

Vergewissern Sie sich, ob Sie einen DSB benötigen! Es droht Ihnen ein **Bußgeld von bis zu 10 Millionen Euro oder** im Fall eines Unternehmens **von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres.

9. DIE INFORMATIONSPFLICHTEN / DIE DATENSCHUTZERKLÄRUNG

Nach der derzeitigen Fassung des Bundesdatenschutzgesetzes (BDSG) müssen Sie die von der Datenverarbeitung betroffenen Personen informieren. Mit der DSGVO werden die Informationspflichten erweitert.

Über was muss ich die Betroffenen informieren?

Werden die Daten direkt beim Betroffenen erhoben, richten sich die Informationspflichten nach § 13 DSGVO. Es müssen die folgenden Angaben zum **Zeitpunkt der Erhebung** gemacht werden:

- **Name & Kontaktdaten** des **Verantwortlichen**
- **Kontaktdaten** des **Datenschutzbeauftragten**
- die **Zwecke** sowie die **Rechtsgrundlage** der Datenverarbeitung
- die **berechtigten Interessen**, sofern die Verarbeitung auf diese gestützt wird
- gegebenenfalls die **Empfänger**
- gegebenenfalls die **Absicht**, dass die Daten an ein **Drittland** oder an eine **internationale Organisation** übermittelt werden

Um eine faire und transparente Datenverarbeitung zu gewährleisten, sind zusätzlich **zum Zeitpunkt der Erhebung** die folgenden Angaben zu machen:

- **die Dauer** der Datenspeicherung
- das Bestehen eines Rechts auf **Auskunft** sowie auf **Berichtigung** oder auf **Löschung** oder auf Einschränkung der Verarbeitung oder auf Widerruf sowie des Rechts auf **Datenübertragbarkeit**
- wenn die Verarbeitung auf einer Einwilligung beruht, das Bestehen eines Rechts, die **Einwilligung jederzeit zu widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird

- das Bestehen eines **Beschwerderechts** bei einer **Aufsichtsbehörde**
- ob die Bereitstellung der personenbezogenen Daten **gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist**, ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte
- das Bestehen einer **automatischen Entscheidungsfindung** einschließlich Profiling

Was bedeutet „zum Zeitpunkt der Erhebung“?

Gemeint ist hiermit der Beginn der Nutzung. Werden Daten bei dem „Betreten“ einer Webseite erhoben, so müssen Sie dem Betroffenen zeitgleich die Möglichkeit geben, von der Datenschutzerklärung Kenntnis zu nehmen.

Wie steht es um meine Informationspflichten, wenn ich die Daten nicht direkt beim Betroffenen erhebe?

Auch in diesem Fall müssen Sie den Betroffenen informieren. Die Informationspflichten richten sich hier nach § 14 DSGVO, welche denen des § 13 DSGVO ähneln. Die Informationen müssen spätestens einen Monat nach Erlangung der Daten bereitgestellt werden. Sollten Sie die Daten vorher zur Kommunikation mit der betroffenen Person verwenden, so muss der Betroffene zum Zeitpunkt der ersten Mitteilung informiert werden.

Was Sie nun tun müssen:

Gleichen Sie unbedingt Ihre bisherige Datenschutzerklärung mit den neuen Vorgaben der DSGVO ab. Hinsichtlich der **Form der Datenschutzerklärung** müssen Sie die folgenden Aspekte beachten:

- Die **Sprache** muss **klar** und **einfach** sein. Vermeiden Sie technische oder juristische Fachausdrücke.
- Die Datenschutzerklärung muss **präzise** (inhaltliche Richtigkeit & Vollständigkeit), **transparent** und **verständlich** (Sortierung in Abschnitten mit Überschriften versehen) sein.
- Die Datenschutzerklärung muss **leicht zugänglich** sein. Sie muss mit allen gängigen Softwareprogrammen aufrufbar sein. Die Informationen dürfen **nicht versteckt** werden und müssen für die betroffene Person **sofort erkennbar** sein.
- Die Datenschutzerklärung soll in schriftlicher Form erfolgen. Sie kann aber auch die elektronische Form aufweisen.

10. DAS RECHT AUF VERGESSENWERDEN

Das Recht auf Vergessenwerden ist eine Neuheit der DSGVO. Unter bestimmten Voraussetzungen müssen sämtliche Daten der betroffenen Person gelöscht werden. Wurden die Daten bereits veröffentlicht, müssen Sie die Dritten, die durch Sie in den Besitz der Daten gelangt sind, informieren, dass ein Löschungsverlangen vorliegt.

Wann muss ich die Daten löschen?

Liegt eine der folgenden Voraussetzungen vor, müssen Sie die Daten unverzüglich, d.h. ohne schuldhaftes Zögern, löschen:

- die Daten sind für die Zwecke **nicht mehr notwendig**
- **Widerruf** der Einwilligung bei gleichzeitigem Fehlen einer anderweitigen Rechtsgrundlage
- **Widerspruch** gegen die Verarbeitung bei Nichtvorliegen von berechtigten Interessen
- unrechtmäßige Verarbeitung der personenbezogenen Daten
- Die **Löschung** der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten **erforderlich**, dem der **Verantwortliche** unterliegt.
- die Daten wurde in Bezug auf angebotene Dienste der Informationsgesellschaft **gem. Art. 8 Abs. 1 DSGVO erhoben**

Gibt es Ausnahmen?

Ja, die gibt es tatsächlich, sofern die Verarbeitung

- zur Ausübung des **Rechts auf freie Meinungsäußerung und Information**;
- zur **Erfüllung einer rechtlichen Verpflichtung**, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus **Gründen des öffentlichen Interesses** im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 lit. h), i) DSGVO sowie Art. 9 Abs. 3 DSGVO;
- für im öffentlichen Interesse liegende **Archivzwecke, wissenschaftliche oder historische Forschungszwecke** oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen**

erforderlich ist.

Um den gesetzlichen Pflichten nachzukommen, kann auch an dieser Stelle auf entsprechende Software zurückgegriffen werden. So kann in mancher Software ein „Verfallsdatum“ der Daten festgelegt werden, nach welchem die Daten automatisch gelöscht werden.

Zumeist verlangt eine Löschungsanfrage bei Ihnen aber mehrere Tätigkeiten. All diese Tätigkeiten können Sie mithilfe von Programmen organisieren lassen. Gleichzeitig werden hierüber Protokolle zu Nachweiszwecken erstellt.

11. DAS RECHT AUF DATENPORTABILITÄT

Eine weitere Neuerung ist das in Art. 20 DSGVO normierte Recht auf Datenportabilität. Nutzer können also ihre Daten von Ihrem Unternehmen bei einem Wechsel zu einem anderen Unternehmen mitnehmen.

Denkbar wäre eine Ausübung dieses Rechts, wenn der Nutzer in ein anderes soziales Netzwerk wechselt oder aber der Arbeitgeber gewechselt wird. Sie müssen dann die Daten in einem **„strukturierten, gängigen und maschinenlesbaren Format“** dem Nutzer übermitteln.

Was Sie nun tun müssen:

Warten Sie nicht erst ab, bis irgendjemand bei Ihnen von diesem Recht Gebrauch machen wird. Da die Nichtbeachtung des Rechts auf Datenportabilität mit **hohen Bußgeldern** bedacht ist und **hohe Schadensersatzforderungen** drohen, sollten Sie sich rechtzeitig um die technischen Voraussetzungen in Ihrem Unternehmen kümmern.

12. DATENTRANSFER IN EIN DRITTLAND

Auch hinsichtlich der grenzüberschreitenden Datenübermittlung in ein Drittland gibt es einige Punkte zu beachten. Relevant ist dies vor allem, wenn Sie bestimmte Unternehmensprozesse in ein Drittland verlagern. Denken Sie bspw. an

- die Lohnbuchhaltung
- die Wartung Ihrer IT-Systeme
- die Nutzung von Cloudlösungen (Dropbox etc.)

Was ist ein Drittland?

Drittländer sind solche Länder, die weder der Europäischen Union, noch dem Europäischen Wirtschaftsraum (Island, Norwegen, Liechtenstein) angehören. Drittländer sind bspw. Russland, China oder die USA.

Wann darf ich Daten an ein Drittland übermitteln?

Daten dürfen an ein Drittland übermittelt werden, wenn die Europäische Kommission festgestellt hat, dass das Drittland ein angemessenes Schutzniveau bietet.

Welchen Drittländern wurde ein angemessenes Schutzniveau attestiert?

- Andorra
- Argentinien
- Kanada
- Schweiz
- Färöer Inseln
- Isle of Man
- Jersey
- Neuseeland
- Uruguay
- Guernsey

Was ist mit den USA?

Die USA gewährleisten grundsätzlich kein der EU angemessenes Datenschutzniveau. Dennoch ist es möglich, Daten rechtskonform in die USA zu übermitteln. Zwischen der EU und den USA wurde das Abkommen **„EU-US Privacy Shield“** geschlossen. Amerikanische Unternehmen müssen sich in eine entsprechende Liste eintragen lassen und sich zertifizieren lassen. Wenn Sie Daten an ein amerikanisches Unternehmen übermitteln wollen, müssen Sie darauf achten, dass das Unternehmen zertifiziert ist und das Zertifikat noch nicht abgelaufen ist.

Was Sie nun tun müssen:

Zunächst müssen Sie klären, **ob** Sie **Daten in ein Drittland übermitteln**. Sodann haben Sie zu recherchieren, ob das Drittland ein **angemessenes Datenschutzniveau** aufweist.

Darüber hinaus handelt es sich bei dem Datenempfänger zumeist um einen **Auftragsdatenverarbeiter**, sodass Sie die entsprechenden **vertraglichen Anforderungen** einhalten müssen. Weiterhin müssen Sie sicherstellen, dass Sie die **Datentransfers ordnungsgemäß dokumentieren**. Des Weiteren müssen Sie in Ihrer **Datenschutzerklärung** über Ihre Absicht aufklären, dass die personenbezogenen Daten an ein Drittland übermittelt werden sollen.

© wk1003mike / Shutterstock.com

13. DIE MELDEPFLICHT BEI DATENPANNEN

Bisher waren lediglich sog. „Risikodaten“ von einer Meldepflicht umfasst. Den Begriff der „Risikodaten“ kennt die DSGVO nicht mehr. **Jedwede Verletzung des Schutzes der personenbezogenen Daten** muss binnen einer Frist von 72 Stunden bei der Aufsichtsbehörde gemeldet werden. Unter Umständen muss auch der Betroffene informiert werden. Dies ist der Fall, wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht.

Was ist eine Datenpanne?

Hierunter versteht man eine Verletzung der Sicherheit, die

- zur Vernichtung
- zum Verlust
- zur Veränderung
- zur unbefugten Offenlegung
- oder unbefugten Zugang

von personenbezogenen Daten führt. Der Hintergrund der Datenpanne spielt keine Rolle. Es werden

- **unbeabsichtigte** (nicht ordnungsgemäße Entsorgen von Unterlagen oder **Liegenlassen von Datenträgern**) und
- beabsichtigte (Weitergabe an Unbefugte, Hacking oder Pishing) Handlungen als Datenpanne eingeordnet.

Des Weiteren bestehen auch hier Dokumentationspflichten. So müssen die Verletzung sowie jegliche weitere Fakten dokumentiert werden.

Einzige Ausnahme: Die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

Was muss ich bei einer solchen Meldung angeben?

- **Art der Verletzung** des Schutzes personenbezogener Daten
- **Name und Kontaktdaten des Datenschutzbeauftragten**
- wahrscheinliche **Folgen** der Verletzung
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen **Maßnahmen zur Behebung** der Verletzung

Was Sie nun tun müssen:

Bereiten Sie schon jetzt die organisatorischen Abläufe für den Fall einer Datenpanne vor. Kommt es zu einer solchen Panne, müssen Sie Ihre Aufsichtsbehörde innerhalb von 72 Stunden entsprechend den Mindestangaben informieren.

14. DAS ONE-STOP-SHOP-PRINZIP

Kommt es in Ihrem Unternehmen zu einer grenzüberschreitenden Datenverarbeitung, müssen Sie sich nicht mehr mit mehreren Datenschutzbehörden auseinandersetzen. Dank dem One-Stop-Shop-Prinzip ist **nur noch die federführende Aufsichtsbehörde Ihr Ansprechpartner**.

Wichtig zu wissen:

Haben Sie lediglich eine Niederlassung, Ihre Datenverarbeitung hat allerdings erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedsstaat, so liegt eine grenzüberschreitende Datenverarbeitung vor.

Was ist die federführende Aufsichtsbehörde?

Nach Art. 56 Abs. 1 DSGVO ist die federführende Aufsichtsbehörde die Aufsichtsbehörde Ihrer Hauptniederlassung. Ihre Hauptniederlassung ist wiederum die Niederlassung, in welcher die datenschutzrechtlichen Entscheidungen getroffen werden.

Unsere Empfehlung:

Für den Fall, dass Sie in verschiedenen Mitgliedsstaaten eine Niederlassung haben, sollten Sie die datenschutzrechtlichen Entscheidungen auf die Niederlassung verlagern, welche der Ihnen günstigsten Aufsichtsbehörde untersteht.

15. SPEZIELLE PFLICHTEN FÜR ARBEITGEBER / ARBEITNEHMERDATENSCHUTZ

Die DSGVO beinhaltet im Hinblick auf den Arbeitnehmerdatenschutz eine Öffnungsklausel, welche es den Mitgliedsstaaten erlaubt, eine eigene gesetzliche Regelung zu schaffen. Hiervon hat die Bundesrepublik Deutschland Gebrauch gemacht. Zeitgleich mit der DSGVO tritt die Neufassung des Bundesdatenschutzgesetzes (BDSG neu) in Kraft.

Wann darf ich personenbezogene Daten von meinen Beschäftigten verarbeiten?

Dies ist nur zum Zwecke des Beschäftigungsverhältnisses möglich, wenn

- dies für die **Entscheidung über die Begründung eines Beschäftigungsverhältnisses** oder
- dies für dessen **Durchführung** oder
- dies für dessen **Beendigung** oder
- dies zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten

erforderlich ist.

Sie können natürlich auch eine **Einwilligung** der Betroffenen einholen. Die Einwilligung muss freiwillig erfolgen, was aufgrund des Abhängigkeitsverhältnisses des Arbeitnehmers problematisch sein kann. Die Einwilligung bedarf der **Schriftform**, sie muss also unterschrieben sein. Weiterhin müssen Sie den Betroffenen über den **Zweck der Datenverarbeitung** und sein **Widerrufsrecht** aufklären. Der Arbeitnehmerbegriff umfasst nach der Neufassung des Bundesdatenschutzgesetzes auch **Leiharbeiter** und **Freiwillige** des Jugend- sowie des Bundesfreiwilligendienstes.

Was Sie nun tun müssen:

Überprüfen Sie unbedingt, welche Daten Ihnen bisher vorliegen und ob diese von Ihnen überhaupt verarbeitet werden dürfen.

Vorsicht: Auch wenn der deutsche Gesetzgeber aktiv geworden ist, müssen Sie die **Grundsätze der DSGVO** einhalten.

16. KONSEQUENZEN BEI VERSTÖSSEN

Verstoßen Sie in irgendeiner Weise drohen Ihnen empfindliche Sanktionen. Bisher waren Bußgelder im Einzelfall bis zu 300.000 € möglich, diese werden nun mit der DSGVO hinsichtlich der Höhe verschärft.

Was für Sanktionen drohen bei einem Verstoß gegen die DSGVO?

- **Bußgelder von bis zu 20.000.000 € oder** im Falle eines Unternehmens **von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahr verhängt werden, je nachdem, welcher der Beträge höher ist.
- **Maßnahmen** der Aufsichtsbehörden, wie Verwarnungen, Anweisungen oder aber das Verhängen eines Verbots zur Verarbeitung personenbezogener Daten, treffen.
- **Schadensersatz** sowohl für **materielle**, als auch für **immaterielle** Schäden
- **Abmahnungen und Unterlassungklagen** von Verbraucherverbänden und Mitbewerbern
- **strafrechtliche** Konsequenzen

Denken Sie daran: **Ein Datenschutzverstoß kommt selten allein**. Häufig liegt der Fehler im System, sodass Sie sich schnell mehreren Schadensersatzansprüchen ausgesetzt sehen. Des Weiteren haben Sie die **Beweislast** zu stemmen. Sie müssen im Zweifel beweisen können, dass Sie die DSGVO eingehalten haben.

Was Sie nun tun müssen:

Um sich effektiv gegen eine etwaige Haftung zu wappnen, ist die Einhaltung der DSGVO unerlässlich. Achten Sie insbesondere auf die **Einhaltung Ihrer Dokumentationspflichten**. Nur aufgrund Ihrer Dokumentationen können Sie die entsprechenden **Beweise** antreten.

LHR

LHR – Zweifach ausgezeichnet als **Top-Wirtschaftskanzlei 2017.** FOCUS-SPEZIAL **Deutschlands Top-Anwälte.**

Impressum
Rechtsanwälte Lampmann,
Haberkamm & Rosenbaum
Partnerschaft

Partnerschaftsregister Amtsgericht
Essen, Nr. PR 1861

USt-IDNr.: DE237233654

vertreten durch die Gesellschafter:
Arno Lampmann, Niklas Haberkamm
und Birgit Rosenbaum

Stadtwaldgürtel 81-83
50935 Köln

Kontakt
Telefon: 0221 / 2716733-0
Telefax: 0221 / 2716733-33
E-Mail: info@lhr-law.de
Internet: www.lhr-law.de